aws

Guida per l'utente

AWS Organizations

AWS Organizations: Guida per l'utente

Table of Contents

Cos'è AWS Organizations?

AWS Organizations è un servizio di gestione degli account che consente di consolidare più account Account AWS in un'organizzazione che crei e gestisci centralmente. AWS Organizations include funzionalità di gestione degli account e di fatturazione consolidata che consentono di soddisfare al meglio le esigenze di budget, sicurezza e conformità dell'azienda. In qualità di amministratore di un'organizzazione, è possibile creare account nell'organizzazione e invitare account esistenti a far parte dell'organizzazione.

Questa guida definisce i concetti fondamentali per AWS Organizations, fornisce tutorial e spiega come creare e gestire un'organizzazione.

Argomenti

Caratteristiche di AWS Organizations

AWS Organizations offre le seguenti funzionalità:

Gestione centralizzata di tutti gli Account AWS

> 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.

Fatturazione consolidata per tutti gli account membri

> La fatturazione consolidata è una funzionalità di AWS Organizations. È possibile utilizzare l'account di gestione dell'organizzazione per consolidare e pagare le spese di tutti gli account membri. Nella fatturazione consolidata, gli account di gestione possono anche accedere alle informazioni di fatturazione, alle informazioni sull'account e all'attività dell'account degli account membri nell'organizzazione. Queste informazioni possono essere utilizzate per servizi come Cost Explorer, che consentono agli account di gestione di migliorare le prestazioni dei costi dell'organizzazione.

Raggruppamento gerarchico degli account per soddisfare le esigenze di budget, sicurezza o conformità

È possibile raggruppare gli account in unità organizzative (UO) e collegare diverse policy di accesso a ogni UO. Ad esempio, se disponi di account che devono accedere solo ai servizi AWS che soddisfano determinati requisiti normativi, è possibile collocare tali account in un'unica UO. È quindi possibile collegare una policy a quella UO che blocca l'accesso ai servizi che non sono in grado di soddisfare tali requisiti normativi. È possibile nidificare UO all'interno di altre UO a una profondità di cinque livelli, in modo da fornire flessibilità nel modo in cui si strutturano i gruppi di account.

Policy per centralizzare il controllo sulle operazione API e sui servizi AWS a cui ogni account può accedere

In qualità di amministratore dell'account di gestione di un'organizzazione, è possibile utilizzare le policy di controllo dei servizi (SCP) per specificare le autorizzazioni massime per gli account membri dell'organizzazione. Nelle SCP, è possibile limitare a quali operazioni API singole, risorse e serviziAWS gli utenti e i ruoli in ciascun account membro possono accedere. È inoltre possibile definire le condizioni per limitare l'accesso alle operazioni API, risorse e servizi AWS. Queste restrizioni prevalgono anche sugli amministratori degli account membri nell'organizzazione. Quando AWS Organizations blocca l'accesso a un'operazione del servizio, della risorsa o dell'API per un account membro, un utente o un ruolo dell'account non può accedervi. Questo blocco rimane attivo anche se l'amministratore di un account membro concede esplicitamente le autorizzazioni in una policy IAM.

Per ulteriori informazioni, consultare Policy di controllo dei servizi (Service Control Policies, SCP).

Policy per semplificare la standardizzazione dei tag tra le risorse degli account dell'organizzazione

Puoi utilizzare le policy di tag per mantenere i tag coerenti, incluso il trattamento lettere maiuscole o minuscole preferito delle chiavi e dei valori di tag.

Per ulteriori informazioni, consulta Policy di tag

Policy per controllare come i servizi di intelligenza artificiale (IA) e di machine learning di AWS possono raccogliere e archiviare i dati.

È possibile utilizzare le policy di rifiuto dei servizi di IA per disattivare la raccolta e l'archiviazione dei dati per uno qualsiasi dei servizi di IA di AWS che non desideri utilizzare.

Per ulteriori informazioni, consulta Policy di rifiuto dei servizi di IA

Policy che configurano i backup automatici per le risorse negli account dell'organizzazione

È possibile utilizzare le policy di backup per configurare e applicare automaticamente i piani AWS Backup alle risorse di tutti gli account dell'organizzazione.

Per ulteriori informazioni, consulta Policy di backup

Integrazione e supporto per AWS Identity and Access Management (IAM)

IAM fornisce un controllo granulare su utenti e ruoli nei singoli account. AWS Organizations espande tale controllo a livello di account offrendo il controllo sulle operazioni che gli utenti e i ruoli in un account o un gruppo di account possono eseguire. Le autorizzazioni risultanti sono l'intersezione logica delle operazioni consentite da AWS Organizations a livello di account e delle autorizzazioni concesse in modo esplicito da IAM a livello di utente o ruolo in tale account. In altre parole, l'utente può accedere solo a ciò che è consentito sia dalle policy AWS Organizations sia da quelle IAM. Se una delle policy blocca un'operazione, l'utente non può accedere a tale operazione.

Integrazione con altri servizi AWS

È possibile sfruttare i servizi di gestione multi-account disponibili in AWS Organizations con servizi AWS selezionati per eseguire attività su tutti gli account membri di un'organizzazione. Per un elenco dei servizi e i vantaggi dell'uso di ciascun servizio a livello dell'intera organizzazione, consulta AWS servizi che puoi utilizzare con AWS Organizations.

Quando abiliti un servizio AWS per eseguire attività per tuo conto negli account membri dell'organizzazione, AWS Organizations crea un account membro del ruolo collegato ai servizi IAM per tale servizio in ogni account membro. Il ruolo collegato ai servizi dispone di autorizzazioni IAM predefinite che consentono all'altro servizio AWS di eseguire attività specifiche nell'organizzazione e nei suoi account. Per poter funzionare, tutti gli account di un'organizzazione hanno automaticamente un ruolo collegato al servizio. Questo ruolo consente al servizio AWS Organizations di creare i ruoli collegati al servizio richiesti dai servizi AWS per i quali si abilita l'accesso attendibile. Questi ruoli collegati ai servizi aggiuntivi vengono forniti con policy di autorizzazione IAM che consentono al servizio specificato di eseguire solo quelle attività richieste dalle opzioni di configurazione. Per ulteriori informazioni, consultare Uso di AWS Organizations con altri servizi AWS.

Accesso globale

AWS Organizations è un servizio globale con un singolo endpoint che funziona da tutte le Regioni AWS. Non è necessario selezionare esplicitamente una Regione in cui operare.

Replica dei dati che è consistente finale

AWS Organizations, come molti altri servizi AWS, è consistente finale. AWS Organizations raggiunge elevata disponibilità per la replica dei dati su più server all'interno di data center AWS nella sua regione. Se una richiesta per modificare alcuni dati ha successo, la modifica viene completata e memorizzata in maniera sicura. Tuttavia, la modifica deve poi essere replicata su più server. Per ulteriori informazioni, consultare Le modifiche apportate non sono sempre immediatamente visibili.

Utilizzo gratis

AWS Organizations è una funzionalità dell'Account AWS offerta senza costi aggiuntivi. Ti vengono addebitati costi solo quando accedi ad altri servizi AWS dagli account nell'organizzazione. Per informazioni sui prezzi degli altri prodotti AWS, consulta la Pagina dei prezzi di Amazon Web Services.

Prezzi di AWS Organizations

AWS Organizations è disponibile senza alcun costo aggiuntivo. Il costo viene calcolato solo per le risorse AWS utilizzate dagli utenti e dai ruoli negli account membri. Ad esempio, ti verrà addebitata la tariffa standard per le istanze Amazon EC2 utilizzate da utenti o ruoli negli account membri. Per informazioni sui prezzi degli altri servizi AWS, consulta Prezzi AWS.

Accesso a AWS Organizations

Puoi lavorare con AWS Organizations nei modi descritti di seguito:

AWS Management Console

La console AWS Organizations è un'interfaccia basata su browser che è possibile utilizzare per gestire l'organizzazione e le risorse AWS. È possibile eseguire qualsiasi attività nell'organizzazione utilizzando la console.

AWS Strumenti a riga di comando

Con gli strumenti a riga di comando AWS puoi inviare comandi alla riga di comando del tuo sistema per eseguire attività AWS Organizations e AWS. L'utilizzo della riga di comando può essere più veloce e semplice rispetto all'uso della console. Gli strumenti a riga di comando sono inoltre utili per creare script che eseguono le attività di AWS.

AWS offre due gruppi di strumenti a riga di comando:

- AWS Command Line Interface (AWS CLI). Per istruzioni su come installare e utilizzare la AWS CLI, consulta la Guida per l'utente di AWS Command Line Interface.
- AWS Tools for Windows PowerShell. Per informazioni sull'installazione e sull'utilizzo di Tools for Windows PowerShell, consulta la Guida per l'utente di AWS Tools for Windows PowerShell.

SDK AWS

Gli SDK AWS sono costituiti da librerie e codice di esempio per diversi linguaggi di programmazione e piattaforme (ad esempio, Java, Python, Ruby, .NET, iOS e Android). Gli SDK si occupano di attività quali la firma crittografica delle richieste, la gestione degli errori e la ripetizione automatica delle richieste. Per ulteriori informazioni sugli SDK AWS, inclusi i dettagli su come scaricarli e installarli, consulta la pagina relativa agli strumenti per Amazon Web Services.

API Query HTTPSAWS Organizations

L'API query HTTPS AWS Organizations offre l'accesso sistematico ad AWS Organizations 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 Chiamata dell'API tramite richieste di query HTTP e la documentazione di riferimento delle API di AWS Organizations.

Supporto e feedback per AWS Organizations

Apprezziamo il tuo feedback. Puoi inviare i tuoi commenti all'indirizzo feedback-awsorganizations@amazon.com. Puoi anche pubblicare il tuo feedback e le tue domande sul forum di supporto di AWS Organizations. Per ulteriori informazioni sui forum di supporto di AWS consulta la guida dei forum.

Altre risorse AWS

- Formazione e corsi AWS - Collegamenti a corsi basati su ruoli e di specializzazione nonché a corsi gestiti dall'utente per affinare le proprie competenze AWS e acquisire esperienza pratica.
- Strumenti di sviluppo AWS - Collegamenti a strumenti e risorse per sviluppatori che forniscono documentazione, esempi di codici, note di rilascio e altre informazioni utili per creare applicazioni innovative con AWS.

- Centro AWS Support - L'hub per la creazione e la gestione dei casi di AWS Support. Include anche i collegamenti ad altre risorse utili, come forum, domande frequenti di carattere tecnico, stato di integrità dei servizi e AWS Trusted Advisor.
- AWS Support - La pagina Web principale che include le informazioni su AWS Support, un canale di assistenza rapida individuale che aiuta a creare ed eseguire applicazioni nel cloud.
- Contatti - Un punto di contatto centrale per richieste relative a fatturazione, account, eventi, uso illecito e altre questioni relative ad AWS.
- AWS Termini di utilizzo del sito: informazioni dettagliate sul copyright e i marchi, l'account, la licenza, l'accesso al sito e altri argomenti.

Nozioni di base su AWS Organizations

I seguenti argomenti forniscono informazioni per aiutarti a iniziare ad apprendere e a utilizzare AWS Organizations.

Ulteriori informazioni su...

[AWS Organizations Concetti e terminologia]

Informazioni sulla terminologia e sui concetti fondamentali necessari per comprendere AWS Organizations. Questa sezione descrive tutti i componenti di un'organizzazione e le nozioni di base di come funzionano insieme per fornire un nuovo livello di controllo su ciò che gli utenti in tali account possono fare.

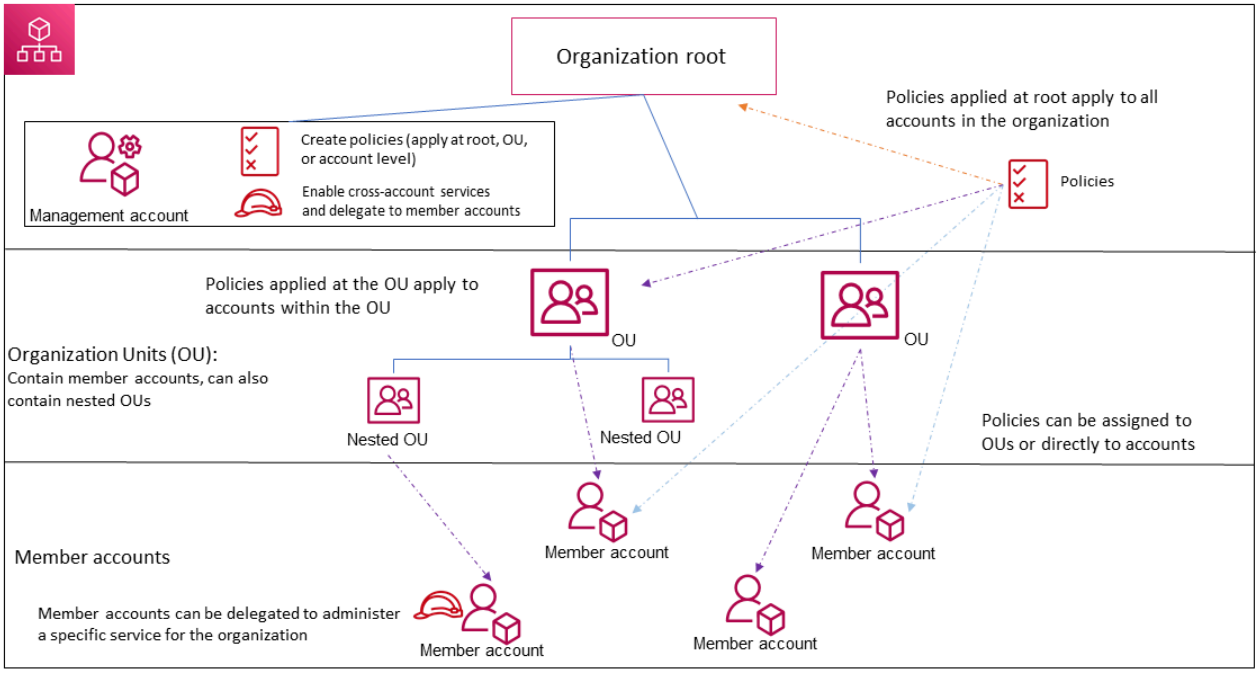
[Fatturazione consolidata per le organizzazioni]

Una delle principali caratteristiche su AWS Organizations è il consolidamento della fatturazione di tutti gli account della tua organizzazione. Ulteriori informazioni su come viene gestita la fatturazione in un'organizzazione e su come funzionano diversi sconti se condivisi su più account. Questo contenuto si trova nella Guida per l'utente di AWS Billing.

AWS Organizations Concetti e terminologia

Per aiutarti a iniziare a utilizzare AWS Organizations, questo argomento spiega alcuni dei concetti chiave.

Il seguente diagramma mostra un'organizzazione di base costituita da cinque account strutturati in quattro unità organizzative (UO) a partire dal root. L'organizzazione, inoltre, offre diverse policy collegate ad alcune delle UO o direttamente agli account. Per una descrizione di ciascuna di queste voci, fare riferimento alle definizioni in questo argomento.



Organizzazione

Un'entità che hai creato per consolidare i tuoi account AWS in modo da poterle amministrare come un'unità singola. È possibile utilizzare la AWS Organizations console per visualizzare e gestire centralmente tutti gli account all'interno della propria organizzazione. Un'organizzazione ha un account di gestione insieme a zero o più account membri. È possibile organizzare gli account in una struttura gerarchica ad albero con una radice nella parte superiore e unità organizzative sotto la radice. Ogni account può trovarsi direttamente nella radice o essere inserito in una delle UO nella gerarchia. Un'organizzazione ha la funzionalità determinata dall'insieme di caratteristiche che si abilita.

Root

Il container genitore per tutti gli account dell'organizzazione. Se si applica una policy alla radice, si applica a tutte le unità organizzative (UO) e agli account nell'organizzazione.

> **Note**
>
> Attualmente, è possibile avere una sola radice. AWS Organizations la crea automaticamente nel momento stesso in cui si crea un'organizzazione.

Unità organizzativa (UO)

Un container per gli account all'interno di una radice. Una UO, inoltre, è in grado di contenere altre unità organizzative, consentendo di creare una gerarchia simile a un albero capovolto, con una radice nella parte superiore e rami di UO che si estendono verso il basso, terminando con le foglie dell'albero, rappresentate dagli account. Quando si collega una policy a uno dei nodi della gerarchia, questo scorre verso il basso, interessando tutti i rami (UO) e le foglie (account) sottostanti. Una UO può avere esattamente un genitore e attualmente ogni account può essere membro di una sola UO.

Account

Un account in Organizations è un Account AWS standard che contiene le tue risorse AWS e le identità che possono accedere a tali risorse.

> **Tip**
>
> Un account AWS non coincide con un account utente. Un utente AWS è un'identità che crei utilizzando AWS Identity and Access Management (IAM) e assume la forma di un utente IAM con credenziali a lungo termine o un ruolo IAM con credenziali a breve termine. Un singolo account AWS può contenere, e in genere contiene, molti utenti e ruoli.

Esistono due tipi di account in un'organizzazione: un singolo account designato come account di gestione e gli account membri.

- L'account di gestione è l'account utilizzato per creare l'organizzazione. Dall'account di gestione dell'organizzazione puoi eseguire le seguenti operazioni:
  - Creare account nell'organizzazione
  - Invitare altri account esistenti nell'organizzazione
  - Rimuovere account dall'organizzazione
  - Designa account amministratore delegato
  - Gestire gli inviti
  - Applicare policy a entità (root, UO o account) all'interno dell'organizzazione
  - Abilitare l'integrazione con i servizi AWS supportati per fornire funzionalità di servizio in tutti gli account dell'organizzazione.

L'account di gestione ha le responsabilità di un account di pagamento ed è responsabile del pagamento di tutte le spese sostenute dagli account membri. Non è possibile modificare l'account di gestione di un'organizzazione.

- Gli account membri costituiscono tutti gli altri account in un'organizzazione. Un account può essere membro di una sola organizzazione alla volta. È possibile collegare una policy a un account per applicare controlli solo a quell'account.

> **Note**
>
> Puoi designare alcuni account membro come account amministratore delegato. Consulta Amministratore delegato, di seguito.

Amministratore delegato

Consigliamo di utilizzare l'account di gestione Organizations e i relativi utenti e ruoli solo per le attività che possono essere eseguite esclusivamente da tale account. Consigliamo di archiviare tutte le risorse AWS in altri account membro nell'organizzazione ed escluderle dall'account di gestione. Questo perché le funzionalità di sicurezza come le policy di controllo dei servizi (SCP) di Organizations non limitano nessun utente o ruolo nell'account di gestione. Inoltre, la separazione delle risorse dall'account di gestione può aiutare a comprendere gli addebiti sulle fatture. Dall'account di gestione dell'organizzazione, puoi designare uno o più account membro come account amministratore delegato per aiutarti a implementare questo suggerimento. Esistono due tipi di amministratori delegati:

- Amministratore delegato per Organizations: da questo account, puoi gestire le policy dell'organizzazione e collegarle alle entità (root, unità organizzative o account) all'interno dell'organizzazione. L'account di gestione può controllare le autorizzazioni di delega a livelli granulari. Per ulteriori informazioni, consulta Amministratore delegato per AWS Organizations.
- Amministratore delegato per un servizio AWS: da questo account, puoi gestire servizi AWS che si integrano con Organizations. L'account di gestione può registrare diversi account membro come amministratori delegati per diversi servizi, a seconda delle necessità. Questi account dispongono delle autorizzazioni amministrative per un servizio specifico, nonché delle autorizzazioni per le operazioni di sola lettura per Organizations. Per ulteriori informazioni, consulta Amministratore delegato per i servizi AWS che funzionano con Organizations.

Invito

Il processo di chiedere a un altro account di unirsi alla propria organizzazione. Un invito può essere inviato solo dall'account di gestione dell'organizzazione. L'invito viene esteso all'ID dell'account o all'indirizzo e-mail associato all'account invitato. Dopo che l'account invitato accetta un invito, diventa un account membro nell'organizzazione. Gli inviti possono anche essere inviati a tutti gli account membri attuali quando l'organizzazione ha bisogno che tutti i membri approvino la modifica dal solo supporto delle caratteristiche di fatturazione consolidata per supportare tutte le funzionalità dell'organizzazione. Gli inviti funzionano attraverso le strette di mano tra gli account. Gli handshake potrebbero non essere visibili quando utilizzi la console AWS Organizations. Ma se usi l'AWS CLI o l'API AWS Organizations, devi lavorare direttamente con gli handshake.

Handshake

Un processo in più fasi di scambio di informazioni tra due parti. Uno dei suoi principali usi nelle AWS Organizations è quello di fungere da implementazione sottostante per gli inviti. L'invio e la risposta dei messaggi di handshake avviene tra l'iniziatore dell'handshake e il destinatario. I messaggi vengono passati in un modo che contribuisce a garantire che entrambe le parti sappiano sempre qual è lo stato corrente. Gli handshake vengono utilizzati anche quando si modifica l'organizzazione dal solo supporto delle caratteristiche di fatturazione consolidata per supportare tutte le caratteristiche che AWS Organizations offre. In genere, è necessario interagire direttamente con gli handshake solo se si utilizza l'API di AWS Organizations o si utilizzano gli strumenti a riga di comando, ad esempio il AWS CLI.

Set di caratteristiche disponibili

- Tutte le caratteristiche - Il set completo delle caratteristiche disponibile per AWS Organizations. Include tutte le funzionalità di fatturazione consolidata, oltre a caratteristiche avanzate che offrono maggiore controllo sull'account nella propria organizzazione. Ad esempio, quando tutte le caratteristiche sono abilitate, l'account di gestione dell'organizzazione ha il controllo completo su ciò che gli account membri possono fare. L'account di gestione può applicare le policy di controllo dei servizi per limitare i servizi e le operazioni a cui gli utenti (incluso l'utente root) e i ruoli di un account possono accedere. L'account di gestione può anche impedire agli account membri di lasciare l'organizzazione. Puoi inoltre consentire l'integrazione con i servizi AWS supportati per consentire a tali servizi di fornire funzionalità a tutti gli account della tua organizzazione.

  È possibile creare un'organizzazione con tutte le caratteristiche già abilitate oppure è possibile abilitare tutte le caratteristiche di un'organizzazione che inizialmente supportava solo le

caratteristiche di fatturazione consolidata. Per abilitare tutte le caratteristiche, tutti gli account membri invitati devono approvare la modifica accettando l'invito inviato quando l'account di gestione avvia il processo.

- Fatturazione consolidata - Questo set di caratteristiche fornisce la funzionalità di fatturazione condivisa, ma non include le caratteristiche avanzate di AWS Organizations. Ad esempio, non è possibile abilitare altri servizi AWS da integrare nell'organizzazione che funzionino in tutti i suoi account oppure utilizzare policy per limitare le operazioni di utenti e ruoli in account diversi. Per utilizzare le caratteristiche avanzate di AWS Organizations, è necessario abilitare tutte le caratteristiche nella propria organizzazione.

Policy di controllo dei servizi (SCP)

Una policy che specifica i servizi e le operazioni che gli utenti e i ruoli possono utilizzare negli account interessati dalla SCP. Le SCP sono simili alle policy di autorizzazione di IAM, tranne per il fatto che non concedono autorizzazioni. Al contrario, le SCP specificano le autorizzazioni massime per un'organizzazione, unità organizzativa (UO) o account. Quando si collega una SCP alla root dell'organizzazione o a una UO, la SCP limita le autorizzazioni per le entità negli account membri.

Elenchi consentiti rispetto agli elenchi di rifiuto

Gli elenchi degli elementi consentiti e gli elenchi degli elementi non consentiti sono strategie che puoi usare per applicare le SCP per filtrare le autorizzazioni disponibili per gli account.

- Strategia dell'elenco consentiti - Specifichi in modo esplicito l'accesso che è consentito. Tutti gli altri accessi sono implicitamente bloccati. Per impostazione predefinita, AWS Organizations collega una AWS policy gestita denominata `FullAWSAccess` a tutte le radici, alle UO e agli account. Ciò aiuta a garantire che, durante la creazione di un'organizzazione, nulla venga bloccato fino a quando lo si desidera. In altre parole, per impostazione predefinita sono ammesse tutte le autorizzazioni. Quando si desidera limitare le autorizzazioni, sostituire la `FullAWSAccess` policy con una che consente solo il set di autorizzazioni più limitato desiderato. Gli utenti e i ruoli negli account interessati possono quindi esercitare solo tale livello di accesso, anche se le loro policy IAM consentono tutte le operazioni. Se si sostituisce la policy predefinita nella radice, tutti gli account nell'organizzazione vengono interessati dalle restrizioni. Non è possibile aggiungere le autorizzazioni a un livello inferiore nella gerarchia, in quanto una SCP non concede mai le autorizzazioni; le filtra soltanto.
-

Strategia dell'elenco non consentiti - Specifichi in modo esplicito l'accesso che non è consentito. Tutti gli altri accessi sono consentiti. In questo scenario, tutte le autorizzazioni sono consentite, a meno che non siano esplicitamente bloccate. Questo è il comportamento predefinito di AWS Organizations. Per impostazione predefinita, AWS Organizations collega una AWS policy gestita denominata `FullAWSAccess` a tutte le radici, alle UO e agli account. Ciò consente a qualsiasi account di accedere a qualsiasi operazione o servizio senza le restrizioni imposte da AWS Organizations. A differenza della tecnica degli elenchi degli elementi consentiti descritta in precedenza, quando si utilizzano gli elenchi degli elementi non consentiti, in genere lasci la policy `FullAWSAccess` predefinita (che consente "tutto"). Quindi colleghi le policy aggiuntive che rifiutano esplicitamente l'accesso ai servizi e alle operazioni indesiderate. Proprio come con le policy di autorizzazione di IAM, un rifiuto esplicito di un'operazione ha la precedenza su qualsiasi permesso di quell'operazione.

Policy di rifiuto dei servizi di intelligenza artificiale (IA)

Un tipo di policy che consente di standardizzare le impostazioni di disattivazione dei servizi di IA di AWS in tutti gli account dell'organizzazione. Alcuni servizi di IA di AWS possono archiviare e utilizzare i contenuti dei clienti elaborati da tali servizi per lo sviluppo e il miglioramento continuo dei servizi e delle tecnologie di IA di Amazon. Come cliente AWS, puoi utilizzare le policy di rifiuto dei servizi di IA per opporti all'archiviazione e all'utilizzo dei tuoi contenuti per migliorare il servizio.

Policy di backup

Un tipo di policy che consente di standardizzare e implementare una strategia di backup per le risorse in tutti gli account dell'organizzazione. In una policy di backup, è possibile configurare e distribuire piani di backup per le risorse.

Policy di tag

Un tipo di policy che semplifica la standardizzazione dei tag tra le risorse in tutti gli account dell'organizzazione. In una policy di tag puoi specificare le regole di tag per risorse specifiche.

Tutorial di AWS Organizations

Utilizza i tutorial di questa sezione per ulteriori informazioni su come eseguire operazioni utilizzando AWS Organizations.

Tutorial: creazione e configurazione di un'organizzazione

Diventa operativo subito grazie a istruzioni dettagliate che ti consentiranno di creare la tua organizzazione, invitare i tuoi primi account membri, creare una gerarchia dell'unità organizzativa (UO) contenente i tuoi account e applicare alcune policy di controllo dei servizi (SCP).

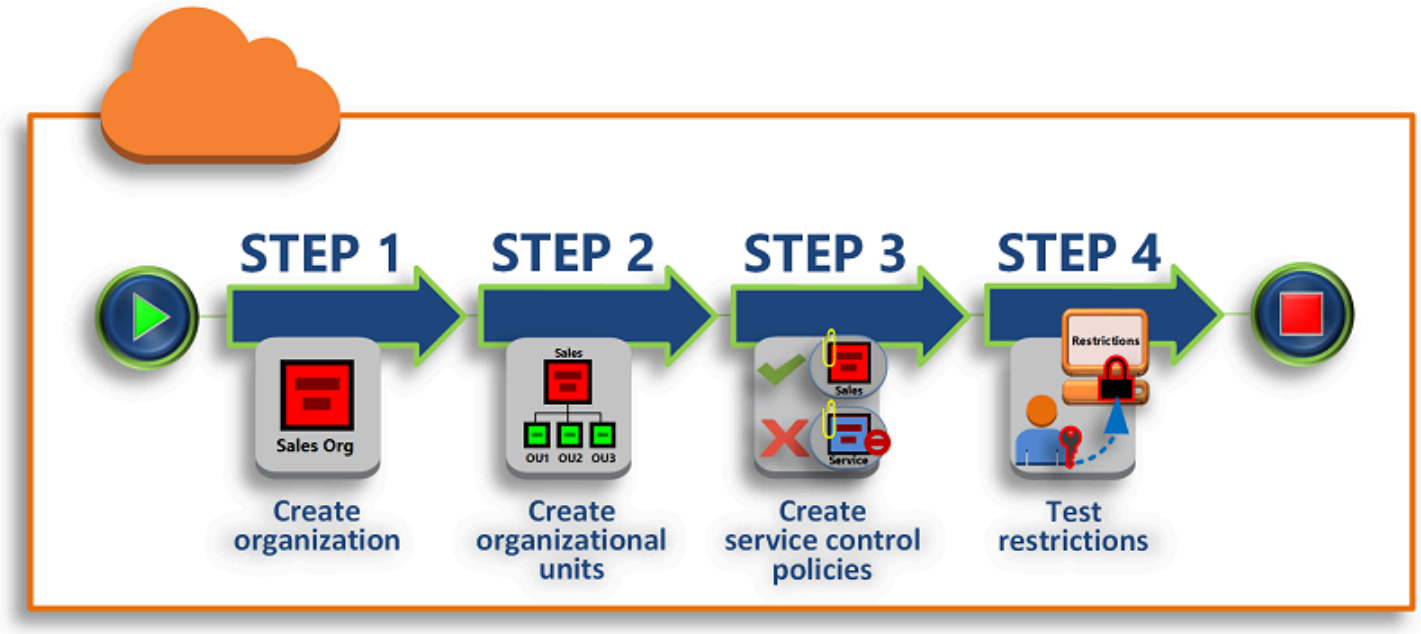
Tutorial: Monitoraggio delle modifiche importanti all'organizzazione con Amazon EventBridge

Controlla le modifiche chiave relative alla tua organizzazione configurando Amazon EventBridge affinché attivi un allarme sotto forma di e-mail, messaggio di testo SMS o voce di log quando nella tua organizzazione vengono eseguite le operazioni che hai indicato. Ad esempio, molte organizzazioni vogliono sapere quando viene creato un nuovo account o quando un account tenta di lasciare l'organizzazione.

Tutorial: creazione e configurazione di un'organizzazione

Questo tutorial illustrerà come creare un'organizzazione e come configurarla con due account membri di AWS. Creando uno degli account membri nell'organizzazione, sarà possibile invitare altri account a far parte dell'organizzazione. Sarà quindi possibile utilizzare la tecnica dell'elenco consentiti per specificare che solo gli amministratori dell'account potranno delegare operazioni e servizi esplicitamente elencati. Questa operazione consente agli amministratori di convalidare qualsiasi nuovo servizio introdotto da AWS prima che venga autorizzato il suo impiego per gli altri utenti dell'azienda. In questo modo, se AWS introduce un nuovo servizio, finché un amministratore non aggiunge il servizio all'elenco consentiti nella policy appropriata non sarà possibile accedervi. Il tutorial, inoltre, illustra come utilizzare la tecnica di elenco di rifiuto per assicurarsi che nessun utente di un account membro possa modificare la configurazione dei log di audit creati da AWS CloudTrail.

La figura seguente mostra le fasi principali del tutorial.



Fase 1: creazione dell'organizzazione

In questa fase è possibile creare un'organizzazione con l'attuale Account AWS come account di gestione. Inoltre, è possibile invitare un Account AWS a entrare a far parte dell'organizzazione e creare un secondo account come account membro.

Fase 2: creazione delle unità organizzative (UO)

Successivamente, è necessario creare due unità organizzative nella tua organizzazione e posizionare i nuovi account dei membri in quelle unità organizzative.

Fase 3: creazione delle policy di controllo dei servizi

È possibile applicare delle restrizioni per le operazioni che possono essere delegate a utenti e ruoli negli account membri utilizzando le policy di controllo dei servizi. In questa fase è necessario creare due policy di controllo dell'organizzazione e collegarle alle unità organizzative nella tua organizzazione.

Fase 4: Test delle policy dell'organizzazione

È possibile effettuare l'accesso come utente da ogni account di test e visualizzare gli effetti che le SCP hanno sugli account.

Per nessuna delle fasi descritte in questo tutorial verrà addebitato un costo nella fattura AWS. AWS Organizations è un servizio gratuito.

Prerequisiti

Questo tutorial presuppone che si possa accedere a due Account AWS esistenti (è necessario crearne un terzo come parte di questo tutorial) e che sia possibile effettuare l'accesso come amministratore per ogni account.

Il tutorial si riferisce ad account come:

- `111111111111` - L'account utilizzato per creare l'organizzazione. Questo account diventa l'account di gestione. Il proprietario di questo account dispone di un indirizzo e-mail di `OrgAccount111@example.com`.
- `222222222222` - Un account invitato a far parte dell'organizzazione come account membro. Il proprietario di questo account dispone di un indirizzo e-mail di `member222@example.com`.
- `333333333333` - Un account creato come membro dell'organizzazione. Il proprietario di questo account dispone di un indirizzo e-mail di `member333@example.com`.

Sostituire i valori in alto con i valori associati agli account di test. Per questo tutorial consigliamo di non utilizzare account di produzione.

Fase 1: creazione dell'organizzazione

In questa fase si accede come amministratore per l'account 111111111111, si crea un'organizzazione che abbia quell'account come account di gestione e si invita un account esistente (222222222222) a far parte dell'organizzazione.

AWS Management Console

1. Accedi a AWS come amministratore dell'account 111111111111 e apri la console AWS Organizations.
2. Nella pagina introduttiva scegli Create an organization (Crea un'organizzazione).
3. Nella finestra di dialogo di conferma, scegli Create organization (Crea organizzazione).

> **Note**
>
> Per impostazione predefinita, l'organizzazione viene creata con tutte le caratteristiche abilitate. È inoltre possibile creare l'organizzazione solo con le caratteristiche di fatturazione consolidata abilitate.

AWS crea l'organizzazione e ti mostra la pagina Account AWS. Se ti trovi su una pagina diversa, scegli Account AWS nel pannello di navigazione sinistro.

Se l'indirizzo e-mail dell'account che utilizzi non è mai stato verificato da AWS, verrà inviata automaticamente un'e-mail di verifica all'indirizzo associato al tuo account di gestione. Potrebbe verificarsi un ritardo prima di ricevere l'e-mail di verifica.

4. Verificare l'indirizzo e-mail entro 24 ore. Per ulteriori informazioni, consulta Verifica dell'indirizzo e-mail.

Ora hai un'organizzazione che ha come unico membro il tuo account. Questo è l'account di gestione dell'organizzazione.

Invitare un account esistente a far parte dell'organizzazione

Ora che disponi di un'organizzazione puoi iniziare a popolarla con gli account. Nelle fasi descritte in questa sezione, è possibile invitare un account esistente a diventare membro dell'organizzazione.

AWS Management Console

Per invitare un account esistente a far parte della tua organizzazione

1. Vai alla pagina Account AWS e scegli Add an Account AWS (Aggiungi un Account AWS).
2. Nella pagina Aggiungi un Account AWS, scegli Invita un Account AWS esistente.
3. Nella casella Email address or account ID of an Account AWS to invite (Indirizzo e-mail o ID dell'Account AWS da invitare), inserisci l'indirizzo e-mail del proprietario dell'account a cui mandare l'invito, simile al seguente: **`member222@example.com`**. In alternativa, se conosci il numero ID dell'Account AWS puoi inserirlo qui.
4. Digita il testo desiderato nella casella Message to include in the invitation email message (Messaggio da includere nel messaggio e-mail di invito). Questo testo verrà incluso nell'e-mail inviata al proprietario dell'account.
5. Scegli Send invitation (Manda invito). AWS Organizations manderà l'invito al proprietario dell'account.

> **Important**
>
> Espandi il messaggio di errore, se indicato. Se l'errore indica che hai superato i limiti di account per l'organizzazione o che non è possibile aggiungere un account perché la tua organizzazione è ancora in fase di inizializzazione, attendi un'ora dalla creazione dell'organizzazione e riprova. Se l'errore persiste, contattare AWS Support.

6. Ai fini di questo tutorial, è ora necessario accettare l'invito. Eseguire una delle operazioni descritte di seguito per arrivare alla pagina Invitations (Inviti) nella console:

   - Apri l'e-mail che AWS ha inviato dall'account di gestione e seleziona il link per accettare l'invito. Quando verrà richiesto, accedere come amministratore dall'account membro invitato.
   - Apri la console AWS Organizations e vai alla pagina Invitations (Inviti).

7. Nella pagina Account AWS, scegli Accept (Accetta), quindi Confirm (Conferma).

> **Tip**
>
> La ricezione dell'invito potrebbe subire ritardi e potrebbe essere necessario attendere prima di poter accettare l'invito.

8. Disconnetti l'account membro e accedi nuovamente come amministratore dall'account di gestione.

Creazione di un account membro

Nelle fasi descritte in questa sezione, è possibile creare un Account AWS che diventerà automaticamente membro dell'organizzazione. Nel tutorial ci si riferisce a questo account come 333333333333..

AWS Management Console

Per creare un account membro

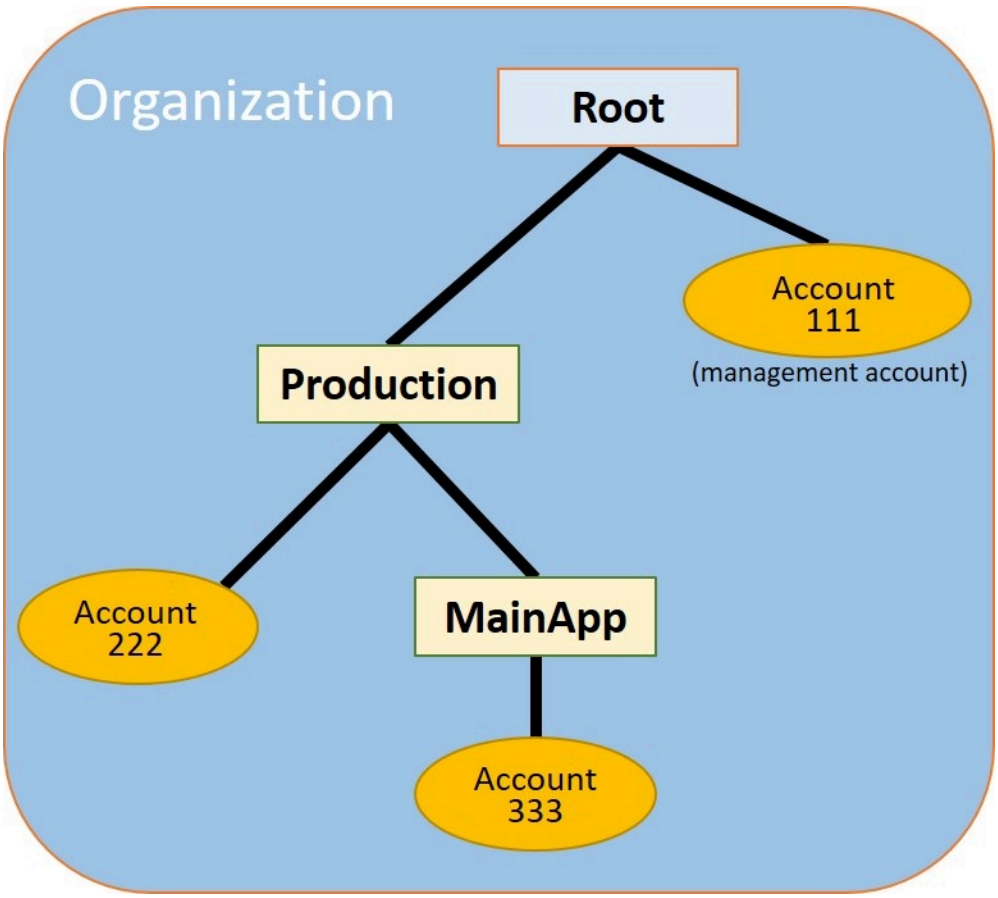
1. Nella console AWS Organizations, alla pagina Account AWS, scegli Add Account AWS (Aggiungi Account AWS).

2. Nella pagina Add an Account AWS (Aggiungi un Account AWS), scegli Create an Account AWS (Crea un Account AWS).
3. Per Account AWS name (Nome dell'Account AWS), inserisci un nome per l'account, ad esempio **`MainApp Account`**.
4. Per Email address of the account's root user (Indirizzo e-mail dell'utente root dell'account), inserisci l'indirizzo e-mail della persona che riceverà le comunicazioni per conto dell'account. Questo valore deve essere univoco a livello globale. I due account non possono avere lo stesso indirizzo e-mail. Ad esempio, è possibile utilizzare un indirizzo simile a **`mainapp@example.com`**.
5. Per IAM role name (Nome del ruolo IAM), è possibile scegliere un nome o lasciare vuoto questo campo per utilizzare automaticamente il nome del ruolo predefinito di `OrganizationAccountAccessRole`. Questo ruolo consente di accedere al nuovo account membro quando si accede come utente IAM dall'account di gestione. Per questo tutorial, lasciare vuoto il campo per indicare ad AWS Organizations di creare il ruolo con il nome predefinito.
6. Scegli Create (Crea) Account AWS. Per visualizzare il nuovo account nella pagina Account AWS è necessario attendere e aggiornare la pagina.

> **Important**
>
> Se ricevi un messaggio di errore che indica che hai superato il limite del numero di account per l'organizzazione o che non è possibile aggiungere un account perché la tua organizzazione è ancora in corso di inizializzazione, attendi un'ora dalla creazione dell'organizzazione e riprova. Se l'errore persiste, contattare AWS Support.

Fase 2: creazione delle unità organizzative (UO)

Nelle fasi di questa sezione, crei delle unità organizzative e vi posizioni gli account membri. Al termine, la gerarchia si presenterà come illustrato di seguito. L'account di gestione rimane nel root. Un account membro viene trasferito nell'UO Production e l'altro account membro viene trasferito nell'UO MainApp, elemento figlio di Production.



AWS Management Console

Per creare e popolare le unità organizzative

> **Note**
>
> Nei passaggi seguenti, interagisci con gli oggetti per i quali è possibile scegliere il nome dell'oggetto stesso o il pulsante di opzione accanto all'oggetto.
>
> - Se scegli il nome dell'oggetto, si apre una nuova pagina in cui vengono visualizzati i dettagli dell'oggetto.
> - Se scegli il pulsante di opzione accanto all'oggetto, stai identificando l'oggetto su cui deve essere eseguita un'altra operazione, ad esempio la scelta di un'opzione di menu.
>
> I passaggi che seguono prevedono che tu scelga il pulsante di opzione in modo da poter agire sull'oggetto associato attraverso scelte di menu.

1. Nella console AWS Organizations, vai alla pagina Account AWS.
2. Seleziona la casella di controllo
   
   accanto al container Root.
3. Nella scheda Children (Figli), scegli Actions (Operazioni) e quindi in Organizational unit (Unità organizzativa) scegli Create new (Crea nuova).
4. Nella pagina Create organizational unit in Root (Crea unità organizzativa in root), per Organizational unit name (Nome unità organizzativa) inserisci **`Production`** e quindi scegli Create organizational unit (Crea unità organizzativa).
5. Seleziona la casella di controllo
   
   accanto alla nuova UO Production.
6. Scegli Actions (Operazioni) e quindi in Organizational unit (Unità organizzativa) scegli Create new (Crea nuova).
7. Nella pagina Create organizational unit in Production (Crea unità organizzativa in produzione), per il nome della seconda UO inserisci **`MainApp`** e quindi scegli Create organizational unit (Crea unità organizzativa).

   Ora puoi trasferire gli account membri in queste UO.
8. Torna alla pagina Account AWS ed espandi la struttura sotto l'UO Production (Produzione) scegliendo il triangolo
   
   accanto ad essa. In questo modo viene visualizzata l'UO MainApp come figlia di Production.
9. Vicino a 333333333333, seleziona la casella di controllo
   
   (non il nome), scegli Operazioni) e quindi sotto a Account AWS scegli Sposta.
10. Nella pagina Sposta Account AWS "333333333333", scegli il triangolo accanto a Produzione per espanderlo. Vicino a MainApp, scegi il pulsante radio
    
    (non il nome), quindi scegli Sposta Account AWS.
11. Vicino a 222222222222, seleziona la casella di controllo
    
    (non il nome), scegli Operazioni) e quindi sotto a Account AWS scegli Sposta.

12. Nella pagina Sposta Account AWS "222222222222", accanto a Produzione, scegli il pulsante radio (non il nome), quindi scegli Sposta Account AWS.

Fase 3: creazione delle policy di controllo dei servizi

Nelle fasi descritte in questa sezione, verranno create tre policy di controllo dei servizi (SCP) e collegate alla root e alle UO, al fine di limitare le operazioni che ciascun utente può eseguire negli account dell'organizzazione. La prima SCP impedisce a qualsiasi account membro di creare o modificare i log di AWS CloudTrail configurati. L'account principale non viene influenzato da alcuna SCP, quindi dopo aver applicato la SCP di CloudTrail è necessario creare i log dall'account di gestione.

Abilitare il tipo di policy di controllo dei servizi per l'organizzazione

Prima di poter collegare una policy di qualsiasi tipo a un root o a una o più UO all'interno di un root, è necessario abilitare il tipo di policy per l'organizzazione. I tipi di policy non sono abilitati per impostazione predefinita. Le fasi descritte in questa sezione mostrano come abilitare il tipo di policy di controllo dei servizi (SCP) per l'organizzazione.

AWS Management Console

Per abilitare le policy di controllo dei servizi per l'organizzazione

1. Vai alla pagina Policy, quindi scegli Policy di controllo dei servizi.
2. Nella pagina Service Control Policies (Policy di controllo dei servizi), scegli Enable service control policies (Abilita le policy di controllo dei servizi).

   Viene visualizzato un banner verde per informarti che ora puoi creare SCP nella tua organizzazione.

Crea le SCP

Ora che le policy di controllo dei servizi sono abilitate nell'organizzazione, puoi creare le tre policy che ti occorrono per questo tutorial.

AWS Management Console

Per creare la prima SCP che blocca le operazioni di configurazione di CloudTrail

1. Vai alla pagina Policy, quindi scegli Policy di controllo dei servizi.
2. Nella pagina Service control policies (Policy di controllo dei servizi), scegli Create policy (Crea policy).
3. In Policy name (Nome policy), inserisci **`Block CloudTrail Configuration Actions`**.
4. Nella sezione Policy, nell'elenco dei servizi a destra, seleziona CloudTrail per il servizio. Quindi scegliere le seguenti operazioni: AddTags, CreateTrail, DeleteTrail, RemoveTags, StartLogging, StopLogging e UpdateTrail.
5. Sempre nel riquadro di destra, scegli Aggiungi risorsa e specifica CloudTrail e Tutte le risorse. Scegliere Add resource (Aggiungi risorsa).

   L'istruzione di policy sulla sinistra diventa simile alla seguente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1234567890123",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:AddTags",
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:RemoveTags",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. Scegli Crea policy.

La seconda policy definisce un elenco consentiti di tutti i servizi e le operazioni che si desiderano abilitare per utenti e ruoli nella UO Production. Al termine, gli utenti nella UO Production potranno accedere solo ai servizi e alle operazioni elencati.

AWS Management Console

Per creare la seconda policy che consente agli utenti di utilizzare i servizi approvati per la UO Production

1. Nella pagina Service control policies (Policy di controllo dei servizi), scegli Create policy (Crea policy).
2. In Policy name (Nome policy), inserisci **`Allow List for All Approved Services`**.
3. Posizionare il cursore nel riquadro destro della sezione Policy e incollare una policy simile alla seguente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1111111111111",
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "elasticloadbalancing:*",
                "codecommit:*",
                "cloudtrail:*",
                "codedeploy:*"
              ],
            "Resource": [ "*" ]
        }
    ]
}
```

4. Scegli Crea policy.

La policy finale fornisce un elenco di rifiuto dei servizi che non possono essere utilizzati nella UO MainApp. Per questo tutorial, l'accesso ad Amazon DynamoDB viene bloccato per tutti gli account che si trovano nell'UO MainApp.

AWS Management Console

Per creare la terza policy che nega l'accesso a servizi che non possono essere utilizzati nella UO MainApp

1. Nella pagina Service control policies (Policy di controllo dei servizi), scegli Create policy (Crea policy).
2. In Policy name (Nome policy), inserisci **`Deny List for MainApp Prohibited Services`**.
3. Nella sezione Policy a sinistra, seleziona Amazon DynamoDB come servizio. Per l'operazione, scegliere All actions (Tutte le operazioni).
4. Sempre nel riquadro di sinistra, scegli Add resource (Aggiungi risorsa) e specifica DynamoDB e All Resources (Tutte le risorse). Scegliere Add resource (Aggiungi risorsa).

   L'istruzione di policy sulla destra si aggiorna e diventa simile alla seguente.

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

5. Scegliere Create policy (Crea policy) per salvare la SCP.

Collegare le SCP alle UO

Ora che le SCP esistono e sono abilitate per la root, è possibile collegarle alla root e alle UO.

AWS Management Console

Per collegare le policy alla root e alle UO

1. Accedi alla pagina Account AWS.
2. Nella pagina Account AWS, scegli Root (il nome, non il pulsante di opzione) per andare alla relativa pagina dei dettagli.

3. Nella pagina dei dettagli del Root, scegli la scheda Policies (Policy) e quindi in Service Control Policies (Policy di controllo dei servizi) scegli Attach (Collega).
4. Nella pagina Attach a service control policy (Collega una policy di controllo dei servizi), scegli il pulsante di opzione accanto alla SCP denominata `Block CloudTrail Configuration Actions` e quindi Attach (Collega). In questo tutorial, la policy viene collegata al root affinché venga applicata a tutti gli account membri per impedire che chiunque possa modificare la configurazione di CloudTrail.

   Nella pagina dei dettagli Root, la scheda Policies (Policy) mostra ora due SCP collegate al root: quella appena creata e la SCP `FullAWSAccess` predefinita.
5. Torna a Account AWS e seleziona la casella di controllo dell'UO Production (Produzione) (il nome, non il pulsante di opzione) per passare alla rispettiva pagina dei dettagli.
6. Nella pagina dei dettagli dell'UO Production, scegli la scheda Policies (Policy).
7. Sotto Service Control Policies (Policy di controllo dei servizi), scegli Attach (Collega).
8. Nella pagina Attach a service control policy (Collega una policy di controllo dei servizi), scegli il pulsante di opzione accanto a `Allow List for All Approved Services` e quindi Attach (Collega). In questo modo, gli utenti o i ruoli negli account membri nell'UO Production possono accedere ai servizi approvati.
9. Seleziona di nuovo la scheda Policies per verificare che due SCP siano collegate all'UO: quella appena creata e la SCP `FullAWSAccess` predefinita. Tuttavia, poiché l'SCP `FullAWSAccess` è anche un elenco consentiti che consente l'accesso a tutti i servizi e le operazioni, ora è necessario scollegare questa SCP per far sì che vengano consentiti solo i servizi approvati.
10. Per rimuovere la policy predefinita dall'UO Produzione, scegli il pulsante di opzione per FullAWSAccess, scegli Detach (Scollega) e quindi, nella finestra di dialogo di conferma, scegli Detach policy (Scollega policy).

    Dopo avere rimosso questa policy predefinita, tutti gli account membri nell'UO Production perderanno immediatamente la possibilità di accedere a tutte le operazioni e ai servizi che non si trovano nell'SCP dell'elenco consentiti collegata nella fase precedente. Qualsiasi richiesta di utilizzo di operazioni non incluse nell'SCP Allow List for All Approved Services (Elenco consentiti per tutti i servizi approvati) viene negata. Ciò vale anche se un amministratore in un account concede l'accesso a un altro servizio collegando una policy di autorizzazione IAM a un utente in uno degli account membri.

11. Ora è possibile collegare l'SCP denominata `Deny List for MainApp Prohibited services` per evitare che qualsiasi account nell'UO MainApp possa utilizzare uno dei servizi limitati.

    A tale scopo, vai alla pagina Account AWS, scegli l'icona del triangolo per espandere il ramo Production (Produzione) dell'unità organizzativa, quindi scegli l'UO MainApp (il nome, non il pulsante di opzione) per passare ai suoi contenuti.
12. Nella pagina dei dettagli MainApp, scegli la scheda Policies (Policy.
13. Sotto Service Control Policies (Policy di controllo dei servizi), scegli Attach (Collega), quindi nell'elenco delle policy disponibili scegli il pulsante di opzione accanto a Deny List for MainApp Prohibited Services (Elenco non consentiti per servizi vietati MainApp) e quindi Attach policy (Collega policy).

Fase 4: Test delle policy dell'organizzazione

Adesso puoi accedere come utente in qualsiasi account membro e provare a eseguire diverse operazioni AWS:

- Se si accede come utente nell'account di gestione, è possibile eseguire qualsiasi operazione consentita dalle policy di autorizzazione IAM. Le SCP non hanno alcun effetto su utenti o ruoli nell'account di gestione, indipendentemente dal root o dall'UO in cui si trova l'account.
- Se si accede come utente nell'account 222222222222, è possibile eseguire tutte le operazioni consentite dall'elenco consentiti. AWS Organizations nega qualsiasi tentativo di eseguire un'operazione in qualsiasi servizio che non si trovi nell'elenco consentiti. Inoltre, AWS Organizations rifiuta qualsiasi tentativo di eseguire una delle operazioni relative alla configurazione di CloudTrail.
- Se si accede come utente nell'account 333333333333, è possibile eseguire tutte le operazioni consentite dall'elenco consentiti e non bloccate dall'elenco non consentiti. AWS Organizations rifiuta qualsiasi tentativo di eseguire un'operazione che non è nella policy dell'elenco consentiti e qualsiasi operazione che si trova nella policy dell'elenco non consentiti. Inoltre, AWS Organizations rifiuta qualsiasi tentativo di eseguire una delle operazioni relative alla configurazione di CloudTrail.

Tutorial: Monitoraggio delle modifiche importanti all'organizzazione con Amazon EventBridge

Questo tutorial mostra come configurare Amazon EventBridge, precedentemente Eventi Amazon CloudWatch per monitorare le modifiche nella tua organizzazione. Per iniziare, è necessario configurare una regola che si attiva quando gli utenti invocano operazioni specifiche di AWS Organizations. Successivamente, configura Amazon EventBridge per eseguire una funzione AWS Lambda nel momento in cui la regola viene attivata. Inoltre, configura Amazon SNS per inviare un'e-mail con i dettagli dell'evento.

La figura seguente mostra le fasi principali del tutorial.

[Fase 1: configurazione di un trail e un selettore di eventi](#)

Creare un log denominato trail su AWS CloudTrail. e configuralo in modo da acquisire tutte le chiamate API.

[Fase 2: configurazione di una funzione Lambda](#)

Crea una funzione AWS Lambda che registra i dettagli dell'evento in un bucket S3.

[Fase 3: creazione di un argomento Amazon SNS che invia e-mail ai sottoscrittori](#)

Crea un argomento Amazon SNS che invia e-mail ai sottoscrittori, quindi esegui la sottoscrizione all'argomento.

[Fase 4: Creazione di una regola Amazon EventBridge](#)

Crea una regola che indichi a Amazon EventBridge di passare i dettagli delle specifiche chiamate API alla funzione Lambda e ai sottoscrittori dell'argomento di SNS.

[Fase 5: Test della regola di Amazon EventBridge](#)

Testa la nuova regola eseguendo una delle operazioni monitorate. In questo tutorial, l'operazione monitorata consiste nella creazione di un'unità organizzativa. Puoi visualizzare la voce di log creata dalla funzione Lambda e l'e-mail inviata da Amazon SNS ai sottoscrittori.

> **Suggerimento**
>
> È inoltre possibile utilizzare questo tutorial come guida per la configurazione di operazioni simili, ad esempio l'invio di notifiche e-mail al completamento della creazione dell'account. Poiché la creazione dell'account è un'operazione asincrona, come impostazione predefinita non viene inviata alcuna notifica al completamento. Per ulteriori informazioni sull'utilizzo di AWS CloudTrail e Amazon EventBridge con AWS Organizations, consulta Registrazione e monitoraggio in AWS Organizations.

Prerequisiti

Questo tutorial presuppone quanto segue:

- È possibile accedere alla AWS Management Console come utente IAM dall'account di gestione nell'organizzazione. L'utente IAM deve disporre delle autorizzazioni per creare e configurare un log in CloudTrail, una funzione in Lambda, un argomento in Amazon SNS e una regola in Amazon EventBridge. Per ulteriori informazioni sulla concessione delle autorizzazioni, consulta Gestione dell'accesso nella Guida per l'utente di IAM o nella guida del servizio per cui desideri configurare l'accesso.
- Hai accesso a un Amazon Simple Storage Service (Amazon S3) Bucket esistente (oppure disponi dell'autorizzazione per creare un bucket) per ricevere il log CloudTrail configurato nella prima fase.

> **Important**
>
> Al momento AWS Organizations è ospitato solo nella Regione Stati Uniti orientali (Virginia settentrionale), sebbene sia disponibile in tutto il mondo. Per eseguire tutte le fasi in questo tutorial, dovrai configurare la AWS Management Console per l'utilizzo di questa regione.

Fase 1: configurazione di un trail e un selettore di eventi

In questa fase accederai all'account di gestione e configurerai un log (denominato trail) su AWS CloudTrail. Configura inoltre un selettore di eventi nel trail per acquisire tutte le chiamate API di lettura/scrittura, in modo che Amazon EventBridge disponga di chiamate da attivare.

Per creare un trail

1. Accedi ad AWS come amministratore dell'account di gestione dell'organizzazione, quindi apri la console CloudTrail su https://console.aws.amazon.com/cloudtrail/.
2. Nella barra di navigazione nell'angolo in alto a destra della console, scegli la Regione Stati Uniti orientali (Virginia settentrionale). Se scegli una regione differente, AWS Organizations non sarà disponibile come opzione nelle impostazioni di configurazione di Amazon EventBridge e CloudTrail non acquisirà le informazioni relative ad AWS Organizations.
3. Nel riquadro di navigazione selezionare Trails (Percorso).
4. Scegliere Create trail (Creare trail).
5. In Trail name (Nome trail), immettere **`My-Test-Trail`**.
6. Effettua una delle seguenti opzioni per specificare la posizione di recapito dei log da parte di CloudTrail:

   - Se devi creare un bucket, scegli Create new S3 bucket (Crea nuovo bucket S3) e quindi, per Trail log bucket and folder (Bucket e cartella del log del trail), immetti un nome per il nuovo bucket.

     > **Note**
     >
     > I nomi di bucket S3 devono essere univoci a livello globale.

   - Se hai già un bucket, scegli Use existing S3 bucket (Utilizza bucket S3 esistente), quindi scegli il nome del bucket dall'elenco S3 bucket (Bucket S3).
7. Seleziona Successivo.
8. Nella pagina Choose log events (Scegli eventi di log), nella sezione Management events (Eventi di gestione), scegli Read (Lettura) e Write (Scrittura).
9. Seleziona Successivo.
10. Rivedi le selezioni effettuate, quindi scegli Create trail (Crea trail).

Amazon EventBridge ti consente di scegliere tra diversi modi per inviare avvisi quando un regola di avviso corrisponde a una chiamata API in entrata. Questo tutorial illustra due metodi: la chiamata di una funzione Lambda che può registrare la chiamata API e l'invio di informazioni a un argomento di Amazon SNS che invia un'e-mail o un messaggio di testo ai sottoscrittori dell'argomento. Nelle prossime due fasi verranno creati i componenti necessari: la funzione Lambda e l'argomento di Amazon SNS.

Fase 2: configurazione di una funzione Lambda

In questa fase verrà creata una funzione Lambda che registra l'attività dell'API inviata dalla regola Amazon EventBridge che verrà configurata in seguito.

Creazione di una funzione Lambda che registra gli eventi Amazon EventBridge

1. Apri la console AWS Lambda all'indirizzo https://console.aws.amazon.com/lambda/.
2. Se non hai esperienza con Lambda, scegli Get Started Now (Inizia ora) sulla pagina di benvenuto. Altrimenti scegli Create function (Crea funzione).
3. Nella pagina Create function (Crea funzione) scegliere Use a blueprint (Usa un piano).
4. Dal riquadro di ricerca Blueprint, immettere **`hello`** per il filtro e scegliere la blueprint hello-world.
5. Scegliere Configure (Configura).
6. Nella pagina Basic information (Informazioni di base), procedere come segue:
   a. Per il nome della funzione Lambda, inserisci **`LogOrganizationEvents`** nella casella di testo Name (Nome).
   b. In Role (Ruolo), scegliere Create a new role with basic Lambda permissions (Crea un nuovo ruolo con le autorizzazioni Lambda di base). Questo ruolo concede alla tua funzione Lambda le autorizzazioni per accedere ai dati necessari e per scriverli nel log di output.
7. Modifica il codice per la funzione Lambda, come mostrato nell'esempio seguente.

```
console.log('Loading function');

exports.handler = async (event, context) => {
    console.log('LogOrganizationsEvents');
    console.log('Received event:', JSON.stringify(event, null, 2));
    return event.key1;  // Echo back the first key value
    // throw new Error('Something went wrong');
};
```

Questo codice di esempio registra l'evento con una stringa di contrassegno **`LogOrganizationEvents`** seguita dalla stringa JSON che costituisce l'evento.

8. Scegli Create function (Crea funzione).

Fase 3: creazione di un argomento Amazon SNS che invia e-mail ai sottoscrittori

In questa fase, creerai un argomento Amazon SNS che invia informazioni tramite e-mail ai sottoscrittori. Imposterai questo argomento come "destinazione" della regola Amazon EventBridge che creerai più tardi.

Per creare un argomento Amazon SNS che invia un'e-mail ai sottoscrittori

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/.
2. Nel pannello di navigazione, scegli Topics (Argomenti).
3. Scegli Create new topic (Crea nuovo argomento).
   a. Per Topic name (Nome argomento), immettere **`OrganizationsCloudWatchTopic`**.
   b. Per Display name (Nome visualizzato), inserire **`OrgsCWEvnt`**.
   c. Scegli Create topic (Crea argomento).
4. Puoi ora creare una sottoscrizione per l'argomento. Scegli l'ARN per l'argomento che hai appena creato.
5. Scegliere Create Subscription (Crea iscrizione).
   a. Nella pagina Create subscription (Crea sottoscrizione) scegli Email (E-mail) in Protocol (Protocollo).
   b. Per Endpoint, immettere il proprio indirizzo e-mail.
   c. Scegliere Create subscription (Crea abbonamento). AWS invia un'e-mail all'indirizzo e-mail specificato nella fase precedente. Attendere l'arrivo dell'e-mail, quindi scegliere il link Confirm subscription (Conferma abbonamento) nell'e-mail per verificare l'avvenuta ricezione dell'e-mail.
   d. Torna alla console e aggiorna la pagina. Il messaggio Pending confirmation (Conferma in sospeso) non verrà più visualizzato e verrà sostituito dall'ID di sottoscrizione attualmente valido.

Fase 4: Creazione di una regola Amazon EventBridge

Ora che la funzione Lambda richiesta è presente nel tuo account, crea una regola Amazon EventBridge in grado di invocarla quando sono soddisfatti i criteri nella regola.

Per creare una regola EventBridge

1. Apri la console Amazon EventBridge su https://console.aws.amazon.com/events/.
2. Imposta la console sulla regione Stati Uniti orientali (Virginia settentrionale), altrimenti le informazioni su Organizations non saranno disponibili. Nella barra di navigazione nell'angolo in alto a destra della console, scegli la Regione Stati Uniti orientali (Virginia settentrionale).
3. Per ulteriori informazioni sulla creazione di regole, consulta Nozioni di base di Amazon EventBridge nella Guida per l'utente di Amazon EventBridge.

Fase 5: Test della regola di Amazon EventBridge

In questa fase, verrà creata un'unità organizzativa (UO) e verrà osservata la regola Amazon EventBridge, verrà generata una voce di log e sarà inviata un'e-mail a sé stessi con i dettagli dell'evento.

AWS Management Console

Per creare un'unità organizzativa

1. Apri la console AWS Organizations alla pagina Account AWS.
2. Seleziona la casella di controllo dell'UO

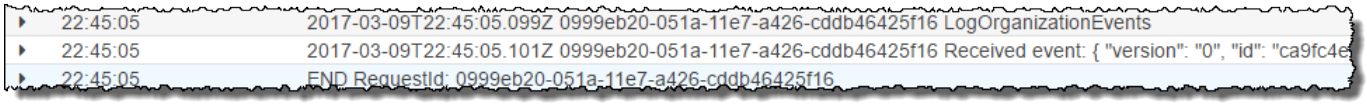
   ☑

   Root, scegli Actions (Operazioni) e quindi in Organizational unit (Unità organizzativa) scegli Create new (Crea nuova).
3. Come nome della UO, inserire **`TestCWEOU`** e scegliere Create organizational unit (Crea unità organizzativa).

Visualizzazione della voce di log di EventBridge

1. Apri la console CloudWatch all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nella pagina di navigazione scegli Logs (Log).

3. In Gruppi di log, scegli il gruppo associato alla funzione Lambda: /aws/lambda/LogOrganizationEvents.
4. Ogni gruppo contiene uno o più flussi e per il giorno odierno dovrebbe esserci un gruppo. Sceglilo.
5. Visualizza il log. Dovresti vedere righe simili alla seguente:



6. Seleziona la riga centrale della voce per visualizzare il testo JSON completo dell'evento ricevuto. Puoi visualizzare tutti i dettagli della richiesta API nelle parti `requestParameters` e `responseElements` dell'output.

```
2017-03-09T22:45:05.101Z 0999eb20-051a-11e7-a426-cddb46425f16 Received event:
{
    "version": "0",
    "id": "123456-EXAMPLE-GUID-123456",
    "detail-type": "AWS API Call via CloudTrail",
    "source": "aws.organizations",
    "account": "123456789012",
    "time": "2017-03-09T22:44:26Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventVersion": "1.04",
        "userIdentity": {
            ...
        },
        "eventTime": "2017-03-09T22:44:26Z",
        "eventSource": "organizations.amazonaws.com",
        "eventName": "CreateOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.168.0.1",
        "userAgent": "AWS Organizations Console, aws-internal/3",
        "requestParameters": {
            "parentId": "r-exampleRootId",
            "name": "TestCWEOU"
        },
        "responseElements": {
            "organizationalUnit": {
                "name": "TestCWEOU",
                "id": "ou-exampleRootId-exampleOUId",
```

```
                "arn": "arn:aws:organizations::1234567789012:ou/o-exampleOrgId/ou-
exampleRootId-exampeOUId"
            }
        },
        "requestID": "123456-EXAMPLE-GUID-123456",
        "eventID": "123456-EXAMPLE-GUID-123456",
        "eventType": "AwsApiCall"
    }
}
```

7. Controlla nell'account e-mail la presenza di un messaggio da OrgsCWEvnt (il nome visualizzato dell'argomento Amazon SNS). Il corpo dell'e-mail contiene lo stesso output del testo JSON della voce di log visualizzata nella fase precedente.

Pulizia: rimozione delle risorse non necessarie

Per non incorrere in costi aggiuntivi, è necessario eliminare qualsiasi risorsa di AWS creata come parte di questo tutorial che non si desidera mantenere.

Per pulire il tuo ambiente AWS

1. Utilizza la console CloudTrail per eliminare il trail denominato **`My-Test-Trail`** creato nella fase 1.
2. Se nella fase 1 hai creato un bucket Amazon S3, utilizza la console Amazon S3 per eliminarlo.
3. Utilizza la console Lambda per eliminare la funzione denominata **`LogOrganizationEvents`** creata nella fase 2.
4. Utilizza la console Amazon SNS per eliminare l'argomento Amazon SNS denominato **`OrganizationsCloudWatchTopic`** creato nella fase 3.
5. Utilizza la console CloudWatch per eliminare la regola EventBridge denominata **`OrgsMonitorRule`** creata nella fase 4.
6. Utilizza la console Organizations per eliminare l'unità organizzativa denominata **`TestCWEOU`** creata alla fase 5.

Sono state completate tutte le operazioni. In questo tutorial hai configurato EventBridge per monitorare la tua organizzazione per eventuali modifiche. Hai configurato una regola che viene attivata quando gli utenti invocano operazioni specifiche di AWS Organizations. La regola eseguiva una funzione Lambda che registrava l'evento e inviava un'e-mail contenente i dettagli dell'evento.

Best practice per la gestione di più account

Segui questi consigli per aiutarti a configurare e gestire un ambiente multi-account in AWS Organizations.

Argomenti

Gestione degli account all'interno di un'unica organizzazione

Consigliamo di creare un'unica organizzazione e di gestire tutti gli account all'interno di quest'ultima. Un'organizzazione è un limite di sicurezza che consente di mantenere la coerenza tra gli account nel tuo ambiente. Puoi applicare centralmente le policy o le configurazioni dei livelli di servizio tra gli account all'interno di un'organizzazione. Se desideri abilitare policy coerenti, visibilità centralizzata e controlli programmatici in tutto il tuo ambiente multi-account, è consigliato farlo all'interno di una singola organizzazione.

Utilizzo di una password complessa per l'utente root

Consigliamo di utilizzare una password complessa e univoca. Numerosi gestori di password e algoritmi e strumenti di generazione di password complesse possono aiutarti a raggiungere questi obiettivi. Per ulteriori informazioni, consulta la pagina Changing the password for the Utente root dell'account AWS. Utilizza le policy di sicurezza delle informazioni aziendali per gestire l'archiviazione a lungo termine e l'accesso alle password dell'utente root. Consigliamo di archiviare la password in un sistema di gestione delle password o equivalente che soddisfi i requisiti di sicurezza dell'organizzazione. Per evitare di creare una dipendenza circolare, non memorizzare la password dell'utente root con strumenti che dipendono da servizi AWS a cui si accede con l'account protetto. Qualunque metodo tu scelga, consigliamo di dare priorità alla resilienza e di valutare la possibilità di richiedere a più attori di autorizzare l'accesso a questo vault per una protezione avanzata. Qualsiasi accesso alla password o alla sua posizione di archiviazione deve essere registrato e monitorato. Per ulteriori consigli sulle password degli utenti root, consulta la pagina Root user best practices for your Account AWS.

Documenta i processi per l'utilizzo delle credenziali dell'utente root

Documenta le esecuzioni di processi importanti man mano che vengono eseguiti per assicurarti di disporre di un record delle persone coinvolte in ogni fase. Per gestire la password, consigliamo di utilizzare un gestore di password crittografato sicuro. Inoltre, è importante documentare eventuali eccezioni ed eventi imprevisti che potrebbero verificarsi. Per ulteriori informazioni, consulta Risoluzione dei problemi di accesso a AWS Management Console nella Guida per l'utente per l'accesso a AWS e Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Testa e verifica di continuare ad avere accesso all'utente root e che il numero di contatto sia operativo a cadenza perlomeno trimestrale. Questa operazione consente all'azienda di assicurarsi che il processo funzioni e di mantenere l'accesso all'utente root. Inoltre, dimostra che le persone responsabili dell'accesso root comprendono i passaggi che devono eseguire affinché il processo abbia esito positivo. Per aumentare i tempi di risposta e il successo, è importante assicurarsi che tutto il personale coinvolto in un processo comprenda esattamente cosa deve fare nel caso in cui sia necessario l'accesso.

Abilitazione dell'MFA per le credenziali di utente root

Consigliamo di abilitare più dispositivi con autenticazione a più fattori (MFA) per l'utente root dell'Account AWS e per gli utenti IAM degli Account AWS. Ciò consente di aumentare la sicurezza degli Account AWS e semplificare la gestione dell'accesso agli utenti con privilegi elevati, come l'utente root dell'Account AWS. Per soddisfare le diverse esigenze dei clienti, AWS supporta tre tipi di dispositivi MFA per IAM, tra cui chiavi di sicurezza FIDO, applicazioni di autenticazione virtuale e token hardware con password monouso.

Ogni tipo di autenticatore ha proprietà fisiche e di sicurezza leggermente diverse che si adattano maggiormente a diversi casi d'uso. Le chiavi di sicurezza FIDO2 offrono il massimo livello di sicurezza e sono resistenti al phishing. Qualsiasi forma di autenticazione a più fattori offre un livello di sicurezza più solido rispetto all'autenticazione con sola password e consigliamo vivamente di aggiungere qualche forma di MFA al tuo account. Seleziona il tipo di dispositivo che meglio si adatta ai requisiti operativi e di sicurezza.

Se scegli un dispositivo alimentato a batteria come autenticatore principale, ad esempio un token hardware con password monouso, valuta anche la possibilità di registrare un autenticatore non basato su batteria come meccanismo di backup. Inoltre, controllare regolarmente la funzionalità del dispositivo e sostituirlo prima della data di scadenza è essenziale per mantenere un accesso continuativo. Indipendentemente dal tipo di dispositivo scelto, consigliamo di registrare almeno due dispositivi (IAM supporta fino a otto dispositivi MFA per utente) per aumentare la resilienza in caso di perdita o guasto del dispositivo.

Segui la policy di sicurezza delle informazioni dell'organizzazione per l'archiviazione del dispositivo MFA. Consigliamo di archiviare il dispositivo MFA separatamente dalla password associata. Ciò garantisce che l'accesso alla password e al dispositivo MFA richieda risorse diverse (persone, dati e strumenti). Questa separazione aggiunge un ulteriore livello di protezione dagli accessi non autorizzati. Inoltre, consigliamo di registrare e monitorare qualsiasi accesso al dispositivo MFA o alla relativa posizione di archiviazione. Ciò aiuta a rilevare e rispondere a qualsiasi accesso non autorizzato.

Per ulteriori informazioni, consulta la pagina Secure your root user sign-in with multi-factor authentication (MFA) nella Guida per l'utente di IAM. Per istruzioni sull'abilitazione della MFA, consulta Utilizzo dell'autenticazione a più fattori (MFA) in AWS e Abilitazione dei dispositivi MFA per gli utenti in AWS.

Applica controlli per monitorare l'accesso alle credenziali utente root

L'accesso alle credenziali utente root dovrebbe essere un evento raro. Crea avvisi utilizzando strumenti come Amazon EventBridge per annunciare l'accesso e l'utilizzo delle credenziali utente root dell'account di gestione. Questo avviso dovrebbe includere, ma non esclusivamente, l'indirizzo e-mail utilizzato per l'utente root stesso. Questo avviso dovrebbe essere significativo e difficile da ignorare. Per un esempio, consulta Monitoraggio e notifiche sull'attività dell'utente root Account AWS. Verifica che il personale che riceve un avviso di questo tipo comprenda come convalidare che è previsto l'accesso utente root e come sottoporre la questione ai livelli gerarchici superiori se ritiene che sia in corso un incidente di sicurezza. Per ulteriori informazioni, consulta Segnala e-mail sospette o Segnalazione di vulnerabilità. In alternativa, puoi contattare AWS per ricevere assistenza e indicazioni aggiuntive.

Mantieni aggiornato il numero di telefono di contatto

Per recuperare l'accesso all'Account AWS, è fondamentale disporre di un numero di telefono di contatto valido e attivo che consenta di ricevere messaggi di testo o chiamate. Consigliamo di utilizzare un numero di telefono dedicato per assicurarti che AWS possa contattarti per l'assistenza e il ripristino dell'account. Puoi visualizzare e gestire facilmente i numeri di telefono dell'account tramite la AWS Management Console o le API di gestione degli account.

Esistono vari modi per ottenere un numero di telefono dedicato che garantisca ad AWS di contattarti. Consigliamo vivamente di procurarti una scheda SIM dedicata e un telefono fisico. Conserva in modo sicuro il telefono e la SIM a lungo termine per garantire che il numero di telefono rimanga disponibile per il ripristino dell'account. Assicurati inoltre che il team responsabile della fattura del dispositivo mobile comprenda l'importanza di questo numero, anche se rimane inattivo per periodi prolungati. È essenziale mantenere riservato questo numero di telefono all'interno dell'organizzazione per una protezione aggiuntiva.

Documenta il numero di telefono nella pagina della console Informazioni di contatto di AWS e condividine i dettagli con i team specifici che ne devono essere a conoscenza nell'organizzazione. Questo approccio consente di ridurre al minimo il rischio associato al trasferimento del numero di telefono su una SIM diversa. Custodisci il telefono in base alle policy di sicurezza delle informazioni esistenti. Tuttavia, non custodire il telefono nella stessa posizione delle altre informazioni relative alle credenziali. Qualsiasi accesso al telefono o alla sua posizione di deposito deve essere registrato

e monitorato. Se il numero di telefono associato a un account cambia, implementa i processi per aggiornare il numero di telefono nella documentazione esistente.

Utilizzo di un indirizzo e-mail per account root

Utilizza un indirizzo e-mail gestito dalla tua azienda. Utilizza un indirizzo e-mail che inoltra i messaggi ricevuti direttamente a un gruppo di utenti. Nel caso in cui AWS debba contattare il proprietario dell'account, ad esempio per confermare l'accesso, il messaggio e-mail viene distribuito a più parti. Questo approccio aiuta a ridurre il rischio di ritardi nella risposta anche se i destinatari sono in vacanza, in malattia o hanno lasciato l'azienda.

Raggruppamento dei carichi di lavoro in base alle finalità commerciali e non alla struttura del report

Consigliamo di isolare gli ambienti e i dati dei carichi di lavoro di produzione nelle unità organizzative di alto livello orientate ai carichi di lavoro. Le unità organizzative devono basarsi su un set comune di controlli anziché rispecchiare la struttura di report dell'azienda. Oltre alle unità organizzative di produzione, consigliamo di definire una o più unità organizzative non di produzione che contengano account e ambienti di carico di lavoro utilizzati per sviluppare e testare i carichi di lavoro. Per ulteriori linee guida, consulta Organizing workload-oriented OUs.

Utilizzo di più account per organizzare i carichi di lavoro

Un Account AWS fornisce sicurezza, accesso e limiti di fatturazione naturali per le risorse AWS. L'utilizzo di più account offre vantaggi, in quanto consente di distribuire quote a livello di account e limiti di frequenza delle richieste API, oltre ai vantaggi aggiuntivi elencati qui. Consigliamo di utilizzare una serie di account di base a livello di organizzazione, ad esempio account per la sicurezza, la registrazione e l'infrastruttura. Per gli account relativi ai carichi di lavoro, devi separare i carichi di lavoro di produzione da quelli di test/sviluppo in più account.

Abilitazione dei servizi AWS a livello organizzativo utilizzando la console del servizio o le operazioni API/CLI

Come best practice, consigliamo di abilitare o disabilitare tutti i servizi con cui desideri integrarti in AWS Organizations utilizzando la console di tale servizio oppure i comandi della CLI o le operazioni API equivalenti. Utilizzando questo metodo, il servizio AWS può eseguire tutte le fasi di

inizializzazione richieste per l'organizzazione, come la creazione delle risorse necessarie e la pulizia delle risorse quando si disabilita il servizio. AWS Account Management è l'unico servizio che richiede l'utilizzo della console o delle API AWS Organizations per l'abilitazione. Per verificare l'elenco dei servizi che sono integrati con AWS Organizations, consulta AWS servizi che puoi utilizzare con AWS Organizations.

Utilizzo degli strumenti di fatturazione per monitorare i costi e ottimizzare l'utilizzo delle risorse

Quando gestisci un'organizzazione, ricevi una fattura consolidata che copre tutti gli addebiti relativi ai conti dell'organizzazione. Per gli utenti aziendali che necessitano di accedere alla visibilità dei costi, puoi fornire un ruolo nell'account di gestione con autorizzazioni di sola lettura limitate per verificare gli strumenti di fatturazione e dei costi. Ad esempio, puoi creare un set di autorizzazioni che fornisce l'accesso ai report di fatturazione o utilizzare AWS Cost Explorer Service (uno strumento per visualizzare l'andamento dei costi nel tempo) e servizi convenienti come Amazon S3 Storage Lens e Sistema di ottimizzazione del calcolo AWS.

Pianificazione della strategia di etichettatura e dell'applicazione dei tag nelle risorse dell'organizzazione

Con il dimensionamento degli account e dei carichi di lavoro, i tag possono essere una funzionalità utile per il monitoraggio dei costi, il controllo degli accessi e l'organizzazione delle risorse. Per le strategie di tagging dei nomi, segui la guida in Tagging your AWS resources. Oltre alle risorse, puoi creare tag nel root, negli account, nelle unità organizzative e nelle policy dell'organizzazione. Per ulteriori informazioni, consulta Building your tagging strategy.

Best practice per l'account di gestione

Segui questi suggerimenti per proteggere la sicurezza dell'account di gestione in AWS Organizations. Questi suggerimenti presuppongono che tu segua anche la best practice di utilizzare l'utente root soltanto per le attività che realmente lo richiedono.

Argomenti

- Limitazione di chi ha accesso all'account di gestione
- Verifica e monitoraggio di chi ha accesso

- Utilizzare l'account di gestione solo per le attività che richiedono l'account di gestione
- Evitare di distribuire carichi di lavoro sull'account di gestione dell'organizzazione
- Delegazione delle responsabilità esterne all'account di gestione per la decentralizzazione

Limitazione di chi ha accesso all'account di gestione

L'account di gestione è fondamentale per tutte le attività amministrative menzionate come la gestione degli account, le policy, l'integrazione con altri servizi AWS, la fatturazione consolidata e così via. Pertanto, dovresti limitare l'accesso all'account di gestione solo agli utenti amministratori che necessitano dei diritti per apportare modifiche all'organizzazione.

Verifica e monitoraggio di chi ha accesso

Per assicurarti di mantenere l'accesso all'account di gestione, verifica periodicamente il personale dell'azienda che ha accesso all'indirizzo e-mail, alla password, alla MFA e al numero di telefono associato. Allinea la revisione alle procedure aziendali esistenti. Aggiungi la verifica mensile o trimestrale di queste informazioni per garantire che solo le persone giuste dispongano dell'accesso. Assicurati che il completamento del processo di ripristino o reimpostazione dell'accesso alle credenziali utente root non dipenda da un individuo specifico. Tutti i processi dovrebbero tenere in considerazione la possibilità che le persone non siano disponibili.

Utilizzare l'account di gestione solo per le attività che richiedono l'account di gestione

Consigliamo di utilizzare l'account di gestione e i relativi utenti e ruoli per le attività che devono essere eseguite solo da tale account. Archivia tutte le risorse AWS in altri Account AWS nell'organizzazione e tienile fuori dall'account di gestione. Un motivo importante per mantenere le risorse in altri account è che le policy di controllo dei servizi (SCP) di Organizations non funzionano per limitare gli utenti o i ruoli nell'account di gestione. Inoltre, la separazione delle risorse dall'account di gestione consente di comprendere gli addebiti sulle fatture.

Evitare di distribuire carichi di lavoro sull'account di gestione dell'organizzazione

Le operazioni privilegiate possono essere eseguite all'interno dell'account di gestione di un'organizzazione e le SCP non si applicano all'account di gestione. Ecco perché dovresti limitare le

risorse e i dati cloud contenuti nell'account di gestione solo a quelli che devono essere gestiti in tale account.

Delegazione delle responsabilità esterne all'account di gestione per la decentralizzazione

Ove possibile, consigliamo di delegare responsabilità e servizi al di fuori dell'account di gestione. Fornisci ai tuoi team le autorizzazioni nei propri account per gestire le esigenze dell'organizzazione, senza richiedere l'accesso all'account di gestione. Inoltre, puoi registrare più amministratori delegati per i servizi che supportano questa funzionalità, ad esempio il AWS Service Catalog per la condivisione del software all'interno dell'organizzazione o AWS CloudFormation StackSets per la creazione e l'implementazione di stack.

Per ulteriori informazioni, consulta Security Reference Architecture, Organizing Your AWS Environment Using Multiple Accounts e AWS servizi che puoi utilizzare con AWS Organizations per suggerimenti sulla registrazione degli account membro come amministratori delegati per più servizi AWS. Per ulteriori informazioni sulla configurazione degli amministratori delegati, consulta Enabling a delegated admin account for AWS Account Management e Amministratore delegato per AWS Organizations.

Best practice per gli account membri

Segui questi suggerimenti per proteggere la sicurezza degli account membro nella tua organizzazione. Questi suggerimenti presuppongono che tu segua anche la best practice di utilizzare l'utente root soltanto per le attività che realmente lo richiedono.

Argomenti

- Definizione del nome e degli attributi dell'account
- Dimensionamento efficiente dell'utilizzo dell'ambiente e dell'account
- Utilizza una SCP per limitare ciò che le operazioni che un utente root nei tuoi account membri può eseguire

Definizione del nome e degli attributi dell'account

Per gli account membro, utilizza una struttura di denominazione e un indirizzo e-mail che riflettono l'utilizzo dell'account. Ad esempio, `Workloads+fooA+dev@domain.com` per `WorkloadsFooADev`,

`Workloads+fooB+dev@domain.com` per `WorkloadsFooBDev`. Se hai definito tag personalizzati per l'organizzazione, consigliamo di assegnarli agli account che riflettono l'utilizzo dell'account, il centro di costo, l'ambiente e il progetto. Ciò semplifica l'identificazione, l'organizzazione e la ricerca degli account.

Dimensionamento efficiente dell'utilizzo dell'ambiente e dell'account

Mentre esegui il dimensionamento, prima di creare nuovi account, assicurati che non esistano già account per esigenze simili, al fine evitare duplicazioni inutili. Gli Account AWS dovrebbero basarsi su requisiti di accesso comuni. Se hai intenzione di riutilizzare gli account, ad esempio un account utilizzato come ambiente di sperimentazione (sandbox) o equivalente, consigliamo di eliminare le risorse o i carichi di lavoro non necessari dagli account e di salvare gli account per un utilizzo futuro.

Prima di chiudere gli account, tieni presente che sono soggetti ai limiti delle quote di chiusura degli account. Per ulteriori informazioni, consulta Quote per AWS Organizations. Valuta l'implementazione di un processo di pulizia per riutilizzare gli account invece di chiuderli e crearne di nuovi quando possibile. In questo modo, eviti di incorrere in costi derivanti dall'utilizzo delle risorse e dal raggiungimento dei limiti dell'API CloseAccount.

Utilizza una SCP per limitare ciò che le operazioni che un utente root nei tuoi account membri può eseguire

Si consiglia di creare una policy di controllo dei servizi nell'organizzazione e di collegarla alla sua directory principale, in modo che venga applicata a tutti gli account membri. Per ulteriori informazioni, consulta la pagina Secure your Organizations account root user credentials.

Puoi negare tutte le operazioni root tranne una specifica che devi eseguire nell'account membro. Ad esempio, la seguente SCP impedisce all'utente root di qualsiasi account membro di effettuare chiamate API del servizio AWS tranne "Aggiornamento di una policy del bucket S3 che è stata configurata in modo errato e nega l'accesso a tutti i principali" (una delle operazioni che richiede le credenziali root). Per ulteriori informazioni, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

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

    "Statement": [

        {
```

```
            "Effect": "Deny",

            "NotAction":[

            "s3:GetBucketPolicy",

            "s3:PutBucketPolicy",

            "s3:DeleteBucketPolicy"

                 ],

            "Resource": "*",

            "Condition": {
"StringLike": { "aws:PrincipalArn": "arn:aws:iam::*:root" }

            }

       }

   ]
}
```

Nella maggior parte dei casi, qualsiasi attività amministrativa può essere eseguita da un ruolo AWS Identity and Access Management (IAM) nell'account membro che dispone delle autorizzazioni di amministratore pertinenti. A tali ruoli devono essere applicati controlli adeguati per limitare, registrare e monitorare le attività.

Creazione e gestione di un'organizzazione

Si possono eseguire le seguenti attività utilizzando la console AWS Organizations o eseguendo un comando AWS Command Line Interface (AWS CLI) o le operazioni equivalenti dell'API SDK AWS:

- Creazione di un'organizzazione. Puoi creare un'organizzazione con il tuo account corrente come account di gestione. Puoi creare account membri nella tua organizzazione e invita altri account a farvi parte.
- Abilitazione di tutte le caratteristiche nell'organizzazione. L'abilitazione di tutte le caratteristiche è il modo migliore per utilizzare AWS Organizations. Quando si crea un'organizzazione, è possibile abilitare tutte le caratteristiche o un sottoinsieme di caratteristiche per consolidare la fatturazione. L'abilitazione di tutte le caratteristiche è l'impostazione predefinita e include le caratteristiche di fatturazione consolidata.

  Con tutte le caratteristiche abilitate, è possibile utilizzare le funzionalità di gestione di account avanzate disponibili in AWS Organizations ad esempio le policy di controllo dei servizi (SCP). Le SCP offrono il controllo centralizzato sulle autorizzazioni massime disponibili per tutti gli account nell'organizzazione, aiutandoti a mantenere tutti gli account all'interno delle linee guida di controllo degli accessi dell'organizzazione.
- Visualizzazione dei dettagli relativi all'organizzazione. Puoi visualizzare i dettagli della tua organizzazione e delle sue root, delle unità organizzative (UO) e degli account.
- Eliminazione di un'organizzazione. Puoi eliminare un'organizzazione quando non ne hai più bisogno.

> **Note**
>
> Le procedure in questa sezione specificano le autorizzazioni minime necessarie per eseguire le azioni. Normalmente, queste si applicano all'API o all'accesso allo strumento a riga di comando.
> L'esecuzione di un'attività nella console potrebbe richiedere ulteriori autorizzazioni.
> Ad esempio, potresti concedere autorizzazioni di sola lettura a tutti gli utenti nella tua organizzazione, quindi concederne altre che permettano a utenti selezionati di eseguire attività specifiche.

Creazione di un'organizzazione

Puoi creare un'organizzazione che si basa sul tuo Account AWS come account di gestione. Quando crei un'organizzazione, puoi impostarla affinché supporti tutte le caratteristiche (scelta consigliata) oppure solo le caratteristiche di fatturazione consolidata.

Dopo avere creato un'organizzazione, puoi aggiungere degli account a partire da quello di gestione nei seguenti modi:

- Creando altri Account AWS che vengono aggiunti automaticamente alla tua organizzazione come account membri
- Dopo avere verificato l'indirizzo e-mail, invitando degli Account AWS a entrare a far parte della tua organizzazione come account membri

Creazione di un'organizzazione

È possibile creare un'organizzazione utilizzando la AWS Management Console, un comando della AWS CLI o una delle API SDK.

> **Autorizzazioni minime**
>
> Per creare un'organizzazione con il tuo Account AWS corrente, devi disporre delle autorizzazioni seguenti:
>
> - `organizations:CreateOrganization`
> - `iam:CreateServiceLinkedRole`
>
> È possibile limitare questa autorizzazione solo all'entità del servizio `organizations.amazonaws.com`.

AWS Management Console

Per creare un'organizzazione

1. Accedere 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. Per impostazione predefinita, l'organizzazione viene creata con tutte le caratteristiche abilitate. Tuttavia, è possibile procedere in questo modo:

   - Per creare un'organizzazione con tutte le funzionalità abilitate, nella pagina di introduzione scegli Create an organization (Crea un'organizzazione).
   - Per creare un'organizzazione con solo le funzionalità di fatturazione consolidata, nella pagina di introduzione e in Create an organization (Crea un'organizzazione), scegli Funzionalità di fatturazione consolidata, quindi nella finestra di dialogo di conferma scegli Crea un'organizzazione.

   Se scegli accidentalmente l'opzione sbagliata, puoi accedere immediatamente alla pagina Settings (Impostazioni), quindi scegli Delete organization (Elimina organizzazione) e ricomincia da capo.

3. L'organizzazione viene creata e viene visualizzata la pagina Account AWS. L'unico account presente è il tuo account di gestione, che è attualmente archiviato nella unità organizzativa (UO) root.

   Se necessario, Organizations invia automaticamente un messaggio di verifica all'indirizzo associato all'account di gestione. Potrebbe verificarsi un ritardo prima di ricevere l'e-mail di verifica. Verificare l'indirizzo e-mail entro 24 ore. Per ulteriori informazioni, consultare Verifica dell'indirizzo e-mail. È possibile aggiungere nuovi account all'organizzazione senza verificare l'indirizzo e-mail dell'account di gestione. Tuttavia, per invitare degli account esistenti, devi prima completare la verifica dell'indirizzo e-mail.

   > **Note**
   >
   > Se questo account ha già verificato in precedenza l'indirizzo e-mail, non sarà più necessario effettuare la verifica più quando si utilizza l'account per creare un'organizzazione.

AWS CLI & AWS SDKs

Per creare un'organizzazione

Per creare un'organizzazione, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: create-organization

L'esempio seguente crea un'organizzazione e rende l'Account AWS attualmente registrato l'account di gestione dell'organizzazione.

```
$ aws organizations create-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
        "FeatureSet": "ALL",
        "MasterAccountArn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [  ...DEPRECATED - DO NOT USE ... ]
    }
}
```

> **Important**
>
> Il campo `AvailablePolicyTypes` è obsoleto e non contiene informazioni accurate sulle policy abilitate nell'organizzazione. Per visualizzare l'elenco accurato e completo dei tipi di policy effettivamente abilitati per l'organizzazione, utilizza il comando `ListRoots`, come descritto nella sezione AWS CLI seguente.

- SDK AWS: CreateOrganization

Ora puoi aggiungere altri account all'organizzazione nel modo seguente:

- Per creare un Account AWS che venga automaticamente inserito nell'organizzazione AWS, consulta Creazione di un account membro nell'organizzazione.
- Per invitare un account esistente a partecipare all'organizzazione, consultare Invitare un uomo Account AWS a entrare a far parte della propria organizzazione.

Verifica dell'indirizzo e-mail

Dopo avere creato un'organizzazione e prima di poter invitare degli account a parteciparvi, devi verificare l'indirizzo e-mail che hai fornito per l'account di gestione nell'organizzazione.

Quando si crea un'organizzazione, se l'account di gestione non è stato verificato in precedenza, AWS invia automaticamente un messaggio di verifica all'indirizzo e-mail che hai specificato. Potrebbe verificarsi un ritardo prima di ricevere l'e-mail di verifica.

Entro 24 ore, segui le istruzioni contenute nell'e-mail per verificare il tuo indirizzo e-mail.

Se non verifichi il tuo indirizzo e-mail entro 24 ore, puoi reinviare la richiesta di verifica in modo da poter invitare altri Account AWS a partecipare all'organizzazione. Se non ricevi l'e-mail di verifica, verifica che il tuo indirizzo e-mail sia corretto e, se necessario, modificalo.

- Per sapere quale indirizzo e-mail è associato all'account di gestione, consulta Visualizzazione dei dettagli di un'organizzazione dall'account di gestione.
- Per modificare l'indirizzo e-mail associato all'account di gestione, consulta Gestione di un Account AWS nella Guida per l'utente di AWS Billing.

AWS Management Console

Per reinviare la richiesta di verifica

1. Accedere 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. Vai alla pagina Settings (Impostazioni), quindi scegli Send verification request (Invia richiesta di verifica). L'opzione è presente solo se l'account di gestione non è ancora stato verificato.
3. Verificare l'indirizzo e-mail entro 24 ore.

   Dopo avere verificato l'indirizzo e-mail, puoi invitare altri Account AWS a far parte della tua organizzazione. Per ulteriori informazioni, consultare Invitare un uomo Account AWS a entrare a far parte della propria organizzazione.

Se modifichi l'indirizzo e-mail dell'account di gestione, lo stato dell'account viene ripristinato su "email unverified" (indirizzo e-mail non verificato) e devi completare il processo di verifica del nuovo indirizzo e-mail.

> **Note**
>
> Se hai invitato gli account a unirsi all'organizzazione prima di modificare l'indirizzo e-mail dell'account di gestione e tali inviti non sono ancora stati accettati, non potranno essere

accettati finché non verifichi il nuovo indirizzo e-mail dell'account di gestione. Utilizza la procedura precedente per inviare nuovamente la richiesta di verifica. Dopo avere completato il processo rispondendo all'e-mail, gli account invitati possono accettare gli inviti.

Abilitazione di tutte le caratteristiche nell'organizzazione

AWS Organizations ha due set di caratteristiche disponibili:

- Tutte le caratteristiche - Questo set di caratteristiche è il modo preferito per utilizzare AWS Organizations e include le caratteristiche di fatturazione consolidata. Quando si crea un'organizzazione, l'abilitazione di tutte le caratteristiche è l'impostazione predefinita. Con tutte le caratteristiche abilitate, è possibile utilizzare le funzionalità di gestione dell'account avanzate disponibili in AWS Organizations, come ad esempio l'integrazione con i servizi AWS supportati e le policy di gestione dell'organizzazione.
- Caratteristiche di fatturazione consolidata - Tutte le organizzazioni supportano questo sottoinsieme di caratteristiche, che offre strumenti per la gestione di base utilizzabili per gestire centralmente gli account dell'organizzazione.

Se si crea un'organizzazione solo con le caratteristiche di fatturazione consolidata, è possibile abilitare tutte le caratteristiche in un secondo momento. Questa pagina descrive il processo di abilitazione di tutte le caratteristiche.

Prima di abilitare tutte le caratteristiche

Prima di passare da un'organizzazione che supporta solo le caratteristiche di fatturazione consolidata a un'organizzazione che supporta tutte le caratteristiche, si noti quanto segue:

- Quando avvii il processo di abilitazione di tutte le caratteristiche, AWS Organizations invia una richiesta a ogni account membro che hai invitato a unirsi alla tua organizzazione. Ogni account invitato deve approvare l'abilitazione di tutte le caratteristiche accettando la richiesta. Solo così potrai completare il processo di abilitazione nell'organizzazione. Se un account rifiuta la richiesta, devi rimuovere l'account dall'organizzazione o inviare nuovamente la richiesta. La richiesta deve essere accettata per poter completare il processo per abilitare tutte le funzionalità. Gli account creati utilizzando AWS Organizations non ricevono alcuna richiesta in quanto non hanno bisogno di approvare il controllo aggiuntivo.

- Puoi continuare a invitare gli account a fa parte dell'organizzazione abilitando tutte le caratteristiche. Il proprietario di un account invitato viene informato dall'invito se sta entrando a far parte di un'organizzazione con la sola fatturazione consolidata o con tutte le funzionalità abilitate.
  - Se inviti un account durante il processo per abilitare tutte le funzionalità, l'invito indica che l'organizzazione di cui entrerà a far parte ha tutte le funzionalità abilitate. Se si annulla il processo per abilitare tutte le funzionalità prima che l'account accetti l'invito, tale invito viene annullato. È necessario invitare nuovamente l'account a far parte di un'organizzazione solo con le caratteristiche di fatturazione consolidata.
  - Se inviti un account e l'invito non è ancora stato accettato prima che avvii il processo per abilitare tutte le funzionalità, tale invito viene annullato perché l'invito indica che l'organizzazione dispone solo di funzionalità di fatturazione consolidate. È necessario invitare nuovamente l'account a far parte di un'organizzazione con tutte le caratteristiche abilitate.
- Puoi inoltre continuare a creare account nell'organizzazione. Questo processo non è influenzato da questa modifica.
- AWS Organizations verifica che ogni account disponga di un ruolo collegato ai servizi denominato `AWSServiceRoleForOrganizations`. Questo ruolo è obbligatorio in tutti gli account per abilitare tutte le caratteristiche. Se hai eliminato il ruolo in un account invitato, l'accettazione dell'invito per abilitare tutte le caratteristiche ricrea il ruolo. Se hai eliminato il ruolo in un account che è stato creato utilizzando AWS Organizations, tale account riceve un invito specificamente per ricreare quel ruolo. Tutti questi inviti devono essere accettati affinché l'organizzazione possa completare il processo di abilitazione di tutte le caratteristiche.
- Poiché l'abilitazione di tutte le caratteristiche consente di utilizzare le SCP, accertarsi che gli amministratori dell'account comprendano gli effetti del collegamento di SCP all'organizzazione, unità organizzative o account. Le SCP possono limitare le operazioni che gli utenti e anche gli amministratori possono eseguire negli account interessati. Ad esempio, l'account di gestione può applicare le SCP in grado di impedire agli account membri di lasciare l'organizzazione.
- L'account di gestione non è influenzato da nessuna SCP. Non è possibile limitare le operazioni che gli utenti e i ruoli nell'account di gestione possono eseguire applicando delle SCP: queste policy influenzano solo gli account membri.
- La migrazione da caratteristiche di fatturazione consolidata a tutte le caratteristiche è unidirezionale. Non puoi tornare alle sole caratteristiche di fatturazione consolidata se nella tua organizzazione hai abilitato tutte le caratteristiche.
- (Non consigliato) Se nell'organizzazione sono abilitate solo le caratteristiche di fatturazione consolidata, gli amministratori degli account membri possono decidere di eliminare il ruolo collegato ai servizi denominato `AWSServiceRoleForOrganizations`. Se successivamente scegli di

abilitare tutte le caratteristiche in un'organizzazione, questo ruolo è necessario e viene ricreato in tutti gli account come parte dell'accettazione dell'invito ad abilitare tutte le caratteristiche. Per ulteriori informazioni su come AWS Organizations utilizza questo ruolo, consultare AWS Organizations e ruoli collegati ai servizi.

Avvio del processo di abilitazione di tutte le caratteristiche

Quando effettui l'accesso con autorizzazioni all'account di gestione della tua organizzazione, puoi avviare il processo che ti permette di abilitare tutte le caratteristiche. Per farlo, completa le seguenti fasi.

> **Autorizzazioni minime**
>
> Per abilitare tutte le caratteristiche nella tua organizzazione, devi disporre della seguente autorizzazione:
>
> - `organizations:EnableAllFeatures`
> - `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations

AWS Management Console

Per chiedere agli account membri invitati di confermare l'abilitazione di tutte le caratteristiche nell'organizzazione

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. Nella pagina Impostazioni, scegliere Inizia il processo per abilitare tutte le caratteristiche.
3. Nella pagina Abilita tutte le caratteristiche, riconosci che non è possibile tornare alle caratteristiche di sola fatturazione consolidata dopo la modifica scegliendo Inizia il processo per abilitare tutte le caratteristiche.

   AWS Organizations invia una richiesta a ogni account invitato (non creato) nell'organizzazione, chiedendo l'approvazione per abilitare tutte le caratteristiche nell'organizzazione. In presenza di account creati utilizzando AWS Organizations e se l'amministratore degli account membri ha eliminato il ruolo collegato ai servizi denominato

`AWSServiceRoleForOrganizations`, a tali account AWS Organizations invia una richiesta per ricreare il ruolo.

La console visualizza l'elenco Request approval status (Stato di approvazione della richiesta) per gli account invitati.

> **Tip**
>
> Per tornare a questa pagina in un secondo momento, apri la pagina Settings (Impostazioni) e nella sezione Request sent date (Richiesta inviata in data) scegli View status (Visualizza stato).

4. Nella pagina Enable all features (Abilita tutte le caratteristiche) è mostrato lo stato corrente della richiesta per ogni account nell'organizzazione. Gli account che hanno accettato la richiesta mostrano lo stato ACCEPTED (Accettato). Gli account che non hanno ancora accettato la richiesta mostrano lo stato OPEN (Aperto).

AWS CLI & AWS SDKs

Per chiedere agli account membri invitati di confermare l'abilitazione di tutte le caratteristiche nell'organizzazione

Per abilitare tutte le caratteristiche in un'organizzazione, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: enable-all-features

  Il seguente comando avvia il processo di abilitazione di tutte le caratteristiche nell'organizzazione.

```
$ aws organizations enable-all-features
{
    "Handshake": {
        "Id": "h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
```

```
        "State": "REQUESTED",
        "RequestedTimestamp": "2020-11-19T16:21:46.995000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:21:46.995000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

L'output mostra i dettagli dell'handshake che gli account membri invitati devono accettare.

- SDK AWS: EnableAllFeatures

> **Note**
>
> - Quando la richiesta viene inviata agli account membri ha inizio un conto alla rovescia di 90 giorni. Tutti gli account devono approvare la richiesta entro questo periodo di tempo, altrimenti la richiesta scadrà. Se la richiesta scade, tutte le richieste relative a questo tentativo verranno annullate e sarà necessario iniziare di nuovo dalla fase 2.
> - Una volta effettuata la richiesta di attivazione di tutte le funzionalità, tutti gli inviti all'account non accettati esistenti verranno annullati.
> - Durante il processo di migrazione di tutte le funzionalità, puoi comunque inviare inviti a nuovi account e creare nuovi account.

Una volta che tutti gli account invitati nell'organizzazione hanno approvato le richieste, è possibile finalizzare il processo e abilitare tutte le caratteristiche. Puoi anche finalizzare immediatamente il processo se nell'organizzazione non sono presenti account membri invitati. Per finalizzare il processo, procedi con Finalizzazione del processo per abilitare tutte le caratteristiche.

Approvazione della richiesta per abilitare tutte le caratteristiche o ricreare il ruolo collegato ai servizi

Quando effettui l'accesso con le autorizzazioni a uno degli account membri invitati dell'organizzazione, puoi approvare una richiesta a partire dall'account di gestione. Se il tuo account è stato originariamente invitato a unirsi all'organizzazione, l'invito è per abilitare tutte le caratteristiche e include implicitamente l'approvazione per ricreare il ruolo `AWSServiceRoleForOrganizations`, se necessario. Se invece il tuo account è stato creato utilizzando AWS Organizations e hai eliminato il ruolo `AWSServiceRoleForOrganizations` collegato ai servizi, riceverai un invito solo per ricreare il ruolo. Per farlo, completa le seguenti fasi.

Important

Se abiliti tutte le funzionalità, l'account di gestione dell'organizzazione potrà applicare i controlli basati su policy all'account membro. Questi controlli possono limitare le operazioni che gli utenti e anche tu come amministratore potete eseguire nel tuo account. Tali restrizioni potrebbero impedire al tuo account di lasciare l'organizzazione.

Autorizzazioni minime

Per approvare una richiesta di abilitazione di tutte le caratteristiche per il tuo account membro, devi disporre delle autorizzazioni seguenti:

- `organizations:AcceptHandshake`
- `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations
- `organizations:ListHandshakesForAccount` - Obbligatorio solo quando si utilizza la console Organizations
- `iam:CreateServiceLinkedRole` - Richiesta solo se il ruolo `AWSServiceRoleForOrganizations` deve essere ricreato nell'account membro

AWS Management Console

Per confermare la richiesta di abilitazione di tutte le caratteristiche nell'organizzazione

1. Accedi alla console AWS Organizations all'indirizzo AWS Organizations console. È necessario accedere come utente IAM, assumere un ruolo IAM o accedere come utente root (non consigliato) in un account membro.
2. Leggere le implicazioni per l'account derivanti dall'accettazione della richiesta di abilitazione di tutte le caratteristiche nell'organizzazione, quindi scegliere Accetta. La pagina continua a visualizzare il processo come incompleto finché tutti gli account nell'organizzazione non accettano le richieste e l'amministratore dell'account di gestione non finalizza il processo.

AWS CLI & AWS SDKs

Per confermare la richiesta di abilitazione di tutte le caratteristiche nell'organizzazione

Per accettare la richiesta, è necessario accettare l'handshake con `"Action": "APPROVE_ALL_FEATURES"`.

- AWS CLI:
  - accept-handshake
  - list-handshakes-for-account

  Nell'esempio seguente viene illustrato come elencare le handshake disponibili per l'account. Il valore di `"Id"` nella quarta riga dell'output è il valore necessario per il comando successivo.

```
$ aws organizations list-handshakes-for-account
{
    "Handshakes": [
        {
            "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "111122223333",
```

```
                    "Type": "ACCOUNT"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
            "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
            "Action": "APPROVE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "c440da758cab44068cdafc812EXAMPLE",
                    "Type": "PARENT_HANDSHAKE"
                },
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                },
                {
                    "Value": "111122223333",
                    "Type": "ACCOUNT"
                }
            ]
        }
    ]
}
```

Nell'esempio seguente viene utilizzato l'ID dell'handshake del comando precedente per accettare tale handshake.

```
$ aws organizations accept-handshake --handshake-id h-
a2d6ecb7dbdc4540bc788200aEXAMPLE
{
    "Handshake": {
        "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "111122223333",
                "Type": "ACCOUNT"
```

```
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
        "Action": "APPROVE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "c440da758cab44068cdafc812EXAMPLE",
                "Type": "PARENT_HANDSHAKE"
            },
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            },
            {
                "Value": "111122223333",
                "Type": "ACCOUNT"
            }
        ]
    }
}
```

- SDK AWS:
  - list-handshakes-for-account
  - AcceptHandshake

Finalizzazione del processo per abilitare tutte le caratteristiche

Tutti gli account membri invitati devono approvare la richiesta per abilitare tutte le caratteristiche. Se nell'organizzazione non sono presenti account membri invitati, la pagina Enable all features progress (Avanzamento dell'abilitazione di tutte le caratteristiche) indica con un banner verde che è possibile finalizzare il processo.

> **Autorizzazioni minime**
>
> Per finalizzare il processo di abilitazione di tutte le caratteristiche per l'organizzazione, devi disporre della seguente autorizzazione:
>
> - `organizations:AcceptHandshake`
> - `organizations:ListHandshakesForOrganization`

- `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations

AWS Management Console

Per finalizzare il processo di abilitazione di tutte le caratteristiche

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. Nella pagina Settings (Impostazioni), se tutti gli account invitati hanno accettato la richiesta di abilitazione di tutte le caratteristiche, nella parte superiore della pagina viene visualizzata una casella verde per tua informazione. Nella casella verde, scegli Go to finalize (Vai a finalizzare).
3. Nella pagina Enable all features (Abilita tutte le caratteristiche) scegliFinalize (Finalizza), quindi nella finestra di dialogo di conferma scegli nuovamente Finalize.
4. A questo punto, l'organizzazione dispone di tutte le caratteristiche abilitate.

AWS CLI & AWS SDKs

Per finalizzare il processo di abilitazione di tutte le caratteristiche

Per finalizzare il processo, è necessario accettare l'handshake con `"Action": "ENABLE_ALL_FEATURES"`.

- AWS CLI:
  - list-handshakes-for-organization
  - accept-handshake

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Parties": [
```

```
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
            "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
            "Action": "ENABLE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                }
            ]
        }
    ]
}
```

Nell'esempio seguente viene illustrato come elencare le handshake disponibili per l'organizzazione. Il valore di `"Id"` nella quarta riga dell'output è il valore necessario per il comando successivo.

```
$ aws organizations accept-handshake \
    --handshake-id h-43a871103e4c4ee399868fbf2EXAMPLE
{
    "Handshake": {
        "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
        "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-aa111bb222",
```

```
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

- SDK AWS:
  - AcceptHandshake
  - AcceptHandshake

Le fasi successive:

- Abilita i tipi di policy che desideri utilizzare. Quindi, è possibile collegare le policy che permettono di gestire gli account nell'organizzazione. Per ulteriori informazioni, consulta Gestione delle policy in AWS Organizations.
- Abilita l'integrazione con i servizi supportati. Per ulteriori informazioni, consulta Uso di AWS Organizations con altri servizi AWS.

Visualizzazione dei dettagli relativi all'organizzazione

È possibile eseguire le seguenti attività per visualizzare i dettagli relativi agli elementi dell'organizzazione.

Argomenti

- Visualizzazione dei dettagli di un'organizzazione dall'account di gestione
- Visualizzazione dei dettagli del container root
- Visualizzazione dei dettagli di un'UO
- Visualizzazione dei dettagli di un account
- Visualizzazione dei dettagli di una policy

Visualizzazione dei dettagli di un'organizzazione dall'account di gestione

Una volta effettuato l'accesso all'account di gestione dell'organizzazione nella console AWS Organizations, puoi visualizzare i dettagli dell'organizzazione.

Autorizzazioni minime

Per visualizzare i dettagli di un'organizzazione, è necessario disporre dell'autorizzazione seguente:

- `organizations:DescribeOrganization`

AWS Management Console

Per visualizzare i dettagli dell'organizzazione

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. Vai alla pagina Settings (Impostazioni). In questa pagina vengono visualizzati i dettagli relativi all'organizzazione, inclusi l'ID dell'organizzazione e il nome account e l'indirizzo e-mail assegnati all'account di gestione dell'organizzazione.

AWS CLI & AWS SDKs

Per visualizzare i dettagli dell'organizzazione

Per visualizzare i dettagli di un'organizzazione, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: describe-organization

  Nell'esempio seguente vengono illustrate le informazioni incluse nell'output di questo comando.

```
$ aws organizations describe-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
        "FeatureSet": "ALL",
        "MasterAccountArn": "arn:aws:organizations::128716708097:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [ ...DEPRECATED - DO NOT USE... ]
    }
```

```
}
```

> **Important**
>
> Il campo `AvailablePolicyTypes` è obsoleto e non contiene informazioni accurate sulle policy abilitate nell'organizzazione. Per visualizzare l'elenco accurato e completo dei tipi di policy effettivamente abilitati per l'organizzazione, utilizza il comando `ListRoots`, come descritto nella sezione AWS CLI seguente.

- SDK AWS: DescribeOrganization

Visualizzazione dei dettagli del container root

Una volta effettuato l'accesso all'account di gestione dell'organizzazione nella console AWS Organizations, puoi visualizzare i dettagli del container root.

> **Autorizzazioni minime**
>
> Per visualizzare i dettagli di un root, è necessario disporre delle autorizzazioni seguenti:
>
> - `organizations:DescribeOrganization` (solo console)
> - `organizations:ListRoots`

Il root è il container più in alto nella gerarchia delle unità organizzative (UO) e in genere si comporta come un'UO. Tuttavia, essendo il container in cima alla gerarchia, le modifiche al root influiscono su ogni altra UO e Account AWS all'interno dell'organizzazione.

AWS Management Console

Per visualizzare i dettagli del root

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. Vai alla pagina Account AWS e scegli l'UO Root (il nome, non il pulsante di opzione).
3. Viene visualizzata la pagina dei dettagli Root, che mostra i dettagli del root.

AWS CLI & AWS SDKs

Per visualizzare i dettagli del root

Per visualizzare i dettagli di una root, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: list-roots

  Nell'esempio seguente viene illustrato come recuperare i dettagli del root, inclusi i tipi di policy attualmente abilitati nell'organizzazione:

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": [
                {
                    "Type": "BACKUP_POLICY",
                    "Status": "ENABLED"
                }
            ]
        }
    ]
}
```

- SDK AWS: ListRoots

Visualizzazione dei dettagli di un'UO

Una volta effettuato l'accesso all'account di gestione dell'organizzazione nella console AWS Organizations, puoi visualizzare i dettagli delle unità organizzative all'interno dell'organizzazione.

> **Autorizzazioni minime**
>
> Per visualizzare i dettagli di un'unità organizzativa (UO), è necessario disporre delle autorizzazioni seguenti:
>
> - `organizations:DescribeOrganizationalUnit`

- `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations
- `organizations:ListOrganizationsUnitsForParent` - Obbligatorio solo quando si utilizza la console Organizations
- `organizations:ListRoots` - Obbligatorio solo quando si utilizza la console Organizations

AWS Management Console

Per visualizzare i dettagli di un'UO

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. Nella pagina Account AWS, scegli il nome dell'unità organizzativa (non il pulsante di opzione) che desideri esaminare. Se l'UO desiderata è figlia di un'altra UO, scegli l'icona del triangolo accanto alla rispettiva UO padre per espanderla e visualizzare gli elementi nel livello successivo della gerarchia. Ripeti l'operazione fino a trovare l'unità organizzativa desiderata.

   La casella Organizational unit details (Dettagli dell'unità organizzativa) mostra le informazioni sull'unità organizzativa.

AWS CLI & AWS SDKs

Per visualizzare i dettagli di un'UO

Per visualizzare i dettagli di un'UO, puoi utilizzare uno dei seguenti comandi:

- AWS CLI, SDK AWS:
  - list-roots
  - list-children
  - describe-organizational-unit

Nell'esempio seguente viene illustrato come trovare l'ID di un'UO utilizzando la AWS CLI. È possibile trovare l'ID dell'unità organizzativa attraverso la gerarchia eseguendo il comando

`list-roots`, quindi eseguendo `list-children` sul root e ripetendo l'operazione su ciascuno dei suoi figli fino a trovare quello desiderato.

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
        }
    ]
}
$ aws organizations list-children --parent-id r-a1b2 --child-type
 ORGANIZATIONAL_UNIT
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
```

Dopo avere ottenuto l'ID dell'unità organizzativa, nell'esempio seguente viene illustrato come recuperare i dettagli dell'UO.

```
$ aws organizations describe-organizational-unit --organizational-unit-id ou-a1b2-
f6g7h111
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h111",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
        "Name": "Production-Apps"
    }
}
```

- SDK AWS:
  - ListRoots

- ListChildren
- DescribeOrganizationalUnit

Visualizzazione dei dettagli di un account

Una volta effettuato l'accesso all'account di gestione dell'organizzazione nella console AWS Organizations, puoi visualizzare i dettagli degli account.

> **Autorizzazioni minime**
>
> Per visualizzare i dettagli di un Account AWS, è necessario disporre delle autorizzazioni seguenti:
>
> - `organizations:DescribeAccount`
> - `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations
> - `organizations:ListAccounts` - Obbligatorio solo quando si utilizza la console Organizations

AWS Management Console

Per visualizzare i dettagli di un Account AWS

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. Vai alla pagina Account AWS e scegli il nome del nome dell'account (non il pulsante di opzione) che desideri esaminare. Se l'account desiderato è figlio di un'UO, scegli l'icona del triangolo  accant a un'UO per espanderla e visualizzarne i figli. Ripeti l'operazione fino a quando non trovi l'account.

   La casella Account details (Dettagli account) mostra le informazioni sull'account.

AWS CLI & AWS SDKs

Per visualizzare i dettagli di un Account AWS

Per visualizzare i dettagli di un account, puoi utilizzare uno dei seguenti comandi:

- AWS CLI:
  - list-accounts: elenca i dettagli di tutti gli account nell'organizzazione
  - describe-account: elenca i dettagli solo dell'account specificato

  Entrambi i comandi restituiscono gli stessi dettagli per ogni account incluso nella risposta.

  Nell'esempio seguente viene illustrato come recuperare i dettagli relativi a un account specificato.

```
$ aws organizations describe-account --account-id 123456789012

{
    "Account": {
        "Id": "123456789012",
        "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "Email": "admin@example.com",
        "Name": "Example.com Organization's Management Account",
        "Status": "ACTIVE",
        "JoinedMethod": "INVITED",
        "JoinedTimestamp": "2020-11-20T09:04:20.346000-08:00"
    }
}
```

- SDK AWS:
  - ListAccounts
  - DescribeAccount

Visualizzazione dei dettagli di una policy

Una volta effettuato l'accesso all'account di gestione dell'organizzazione nella console AWS Organizations, puoi visualizzare i dettagli delle policy.

Autorizzazioni minime

Per visualizzare i dettagli di una policy, è necessario disporre delle seguenti autorizzazioni:

- `organizations:DescribePolicy`
- `organizations:ListPolicies`

AWS Management Console

Per visualizzare i dettagli di una policy

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. Effettua una delle seguenti operazioni:
   - Vai alla pagina Policies (Policy), quindi scegli il tipo di policy della policy che desideri esaminare.
   - Vai alla pagina Account AWS, quindi vai a un'unità organizzativa o a un account a cui è associata la policy. Infine, scegli la scheda Policies (Policy) per visualizzare l'elenco delle policy collegate.
3. Scegli il nome della policy (non il pulsante di opzione).

   Nella pagina Details (Dettagli) della policy, è possibile visualizzare tutte le informazioni relative alla policy, incluso il testo della policy JSON e l'elenco delle unità organizzative e degli account a cui è associata la policy.

AWS CLI & AWS SDKs

Per visualizzare i dettagli di una policy

Per visualizzare i dettagli di una policy, puoi utilizzare uno dei seguenti comandi:

- AWS CLI:
  - list-policies
  - describe-policy: elenca i dettagli solo della policy specificata

Nell'esempio seguente viene illustrato come trovare l'ID policy della policy che desideri esaminare. È necessario specificare un tipo di policy e il comando restituisce tutte le policy esclusivamente di tale tipo.

```
$ aws organizations list-policies --filter BACKUP_POLICY
{
    "Policies": [
        {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "test-backup-policy",
            "Description": "test-policy-description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        }
    ]
}
```

La risposta include tutti i dettagli tranne il documento delle policy JSON.

Nell'esempio seguente viene illustrato come recuperare i dettagli solo della policy specificata, incluso il documento delle policy JSON.

```
$ aws organizations describe-policy --policy-id p-i9j8k7l6m5
{
    "Policies": [
        {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "test-backup-policy",
            "Description": "test-policy-description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"plans\":{\"My-Backup-Plan\":{\"regions\":{\"@@assign\":
[\"us-west-2\"]},\"rules\":{\"My-Backup-Rule\"
                    :{\"target_backup_vault_name\":{\"@@assign\":\"My-Primary-
Backup-Vault\"}}},\"selections\":{\"tags\":{
```

```
                    \"My-Backup-Plan-Resource-Assignment\":{\"iam_role_arn\":
{\"@@assign\":\"arn:aws:iam::$account:role/
                    My-Backup-Role\"},\"tag_key\":{\"@@assign\":\"Stage\"},
\"tag_value\":{\"@@assign\":[\"Production\"]}}}}}}"
    ]
}
```

- SDK AWS:
  - ListPolicies
  - DescribePolicy

Eliminazione di un'organizzazione

Puoi eliminare un'organizzazione quando non è più necessaria. L'eliminazione di un'organizzazione non chiude l'account di gestione, ma lo rimuove dall'organizzazione ed elimina l'organizzazione stessa. Il precedente account di gestione diventa un Account AWS autonomo che non è più gestito da AWS Organizations. A questo punto, puoi procedere in tre modi: continuare a usarlo come account standalone, utilizzarlo per creare un'altra organizzazione o accettare un invito da un'altra organizzazione per aggiungervi l'account come account membro.

Important

- Se elimini un'organizzazione, non puoi ripristinarla. Se hai creato delle policy all'interno dell'organizzazione, anch'esse verranno eliminate e non potrai recuperarle.
- Puoi eliminare un'organizzazione solo dopo avere rimosso tutti gli account membri. Se hai creato alcuni degli account membri utilizzando AWS Organizations, potrebbe risultare impossibile rimuoverli. Puoi rimuovere un account membro solo se include tutte le informazioni necessarie per funzionare come Account AWS standalone. Per ulteriori informazioni su come fornire tali informazioni e rimuovere l'account, consulta Abbandono di un'organizzazione da un account membro.
- Se hai chiuso un account membro prima di rimuoverlo dall'organizzazione, questo entra in uno stato "sospeso" per un periodo di tempo e non puoi rimuoverlo dall'organizzazione finché non viene chiuso definitivamente. Questa operazione può richiedere fino a 90 giorni e impedire l'eliminazione dell'organizzazione fino a quando tutti gli account membri non siano stati completamente chiusi.

Quando elimini l'account di gestione da un'organizzazione eliminando l'organizzazione stessa, l'account potrà essere influenzato nei seguenti modi:

- L'account è esclusivamente responsabile del pagamento dei propri addebiti e non più dei costi sostenuti da qualsiasi altro account.
- L'integrazione con altri servizi potrebbe essere disabilitata. Ad esempio, AWS IAM Identity Center richiede un'organizzazione per operare, in modo che se elimini un account da un'organizzazione che supporta IAM Identity Center, gli utenti in tale account non sono più in grado di utilizzare il servizio.

L'account di gestione di un'organizzazione non è mai influenzato dalle policy di controllo dei servizi (SCP), pertanto la cessazione della loro disponibilità non comporta alcuna modifica delle autorizzazioni.

Argomenti

Eliminazione di un'organizzazione

Utilizza la procedura seguente per eliminare un'organizzazione che ripristina il precedente account di gestione a un Account AWS autonomo che non è più gestito da AWS Organizations.

> **Autorizzazioni minime**
>
> Per eliminare un'organizzazione, è necessario effettuare l'accesso come utente o ruolo nell'account di gestione e disporre delle seguenti autorizzazioni:
>
> - `organizations:DeleteOrganization`
> - `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations

AWS Management Console

Per eliminare un'organizzazione

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. Prima di poter eliminare l'organizzazione, occorre innanzitutto rimuovere tutti gli account da essa. Per ulteriori informazioni, consulta Rimozione di un account membro dall'organizzazione.
3. Vai alla pagina Settings (Impostazioni), quindi scegli Delete organization (Elimina organizzazione).
4. Nella finestra di dialogo di conferma Delete organization (Elimina organizzazione), inserisci l'ID dell'organizzazione visualizzato nella riga sopra la casella di testo. Quindi, scegli Delete organization (Elimina organizzazione).

> **Important**
>
> Questa operazione non chiude l'account di gestione, ma lo restituisce a un Account AWS autonomo. Per chiudere l'account, segui i passaggi indicati in Chiusura di un account membro nell'organizzazione.

AWS CLI & AWS SDKs

Per eliminare un'organizzazione

Utilizza uno dei seguenti comandi per eliminare un'organizzazione:

- AWS CLI: delete-organization

  L'esempio seguente elimina l'organizzazione per la quale l'Account AWS del quale vengono utilizzate le credenziali è l'account di gestione.

  ```
  $ aws organizations delete-organization
  ```

  Questo comando non produce alcun output se ha esito positivo.
- SDK AWS: DeleteOrganization

Gestione degli Account AWS nell'organizzazione

Un'organizzazione è una raccolta di Account AWS che è possibile gestire centralmente. È possibile eseguire le seguenti attività per gestire gli account che fanno parte dell'organizzazione:

- Visualizzare i dettagli dell'account nell'organizzazione. È possibile visualizzare il numero di ID univoco dell'account, il suo ARN (Amazon Resource Name) e le policy collegate.
- Esporta un elenco di tutti gli Account AWS nell'organizzazione. È possibile scaricare un file con estensione .csv che contiene i dettagli dell'account per ogni account all'interno dell'organizzazione.
- Invita gli Account AWS esistenti a far parte dell'organizzazione. Crea inviti, gestisci gli inviti creati e accetta o rifiuta gli inviti.
- Crea un Account AWS come parte dell'organizzazione. Crea e accedi a un Account AWS che fa automaticamente parte dell'organizzazione.
- Aggiornare i contatti alternativi nell'organizzazione. Aggiornare i contatti alternativi per gli Account AWS nell'organizzazione.
- Rimuovi un Account AWS dall'organizzazione. In qualità di amministratore nell'account di gestione, rimuovi gli account membri che non desideri più gestire dall'organizzazione. In qualità di amministratore di un membro account, rimuovi l'account dall'organizzazione. Se l'account di gestione dispone di una policy collegata all'account membro, la rimozione dell'account potrebbe essere bloccata.
- Elimina (o chiudi) un Account AWS. Quando un Account AWS non è più necessario, è possibile chiudere l'account per evitare qualsiasi utilizzo o l'accumulo di addebiti.

Impatto dell'appartenenza a un'organizzazione

- Qual è l'impatto per un Account AWS che entra a far parte di un'organizzazione?
- Qual è l'impatto per un Account AWS che viene creato in un'organizzazione?

Impatto per un Account AWS che entra a far parte di un'organizzazione?

Quando inviti un Account AWS a far parte di un'organizzazione e il proprietario dell'account accetta l'invito, AWS Organizations apporta automaticamente le seguenti modifiche al nuovo account membro:

- AWS Organizations Crea un ruolo collegato al servizio chiamato `AWSServiceRoleForOrganizations`. Se l'organizzazione supporta tutte le funzionalità, l'account deve disporre di questo ruolo. È possibile eliminare il ruolo se l'organizzazione supporta solo il set di funzionalità di fatturazione consolidata. Se elimina il ruolo e successivamente abilita tutte le funzionalità nell'organizzazione, AWS Organizations ricrea il ruolo per l'account.
- È possibile che siano presenti diverse policy collegate al root o all'unità organizzativa dell'organizzazione che contiene l'account. In tal caso, le policy si applicano immediatamente a tutti gli utenti e ai ruoli dell'account invitato.
- Puoi abilitare l'attendibilità per un altro servizio AWS per l'organizzazione. In questo caso, il servizio sicuro può creare ruoli collegati ai servizi o eseguire operazioni in qualsiasi account membro dell'organizzazione, incluso un account invitato.

> **Note**
>
> Per gli account dei membri invitati, AWS Organizations non crea automaticamente il ruolo IAM OrganizationAccountAccessRole. Questo ruolo concede agli utenti dell'account di gestione l'accesso amministrativo all'account membro. Se desideri abilitare tale livello di controllo amministrativo a un account invitato, è possibile aggiungere manualmente il ruolo. Per ulteriori informazioni, consulta Creazione di OrganizationAccountAccessRole un account utente invitato.

Puoi invitare un account a partecipare a un'organizzazione in cui sono abilitate solo le caratteristiche di fatturazione consolidata. Se in un secondo momento vuoi abilitare tutte le caratteristiche per l'organizzazione, gli account invitati devono approvare la modifica.

Impatto su un Account AWS che viene creato in un'organizzazione?

Quando crei un Account AWS nell'organizzazione, AWS Organizations apporta automaticamente le seguenti modifiche al nuovo account membro:

- AWS Organizations Crea un ruolo collegato al servizio chiamato `AWSServiceRoleForOrganizations`. Se l'organizzazione supporta tutte le funzionalità, l'account deve disporre di questo ruolo. È possibile eliminare il ruolo se l'organizzazione supporta solo il set di funzionalità di fatturazione consolidata. Se elimina il ruolo e successivamente abilita tutte le funzionalità nell'organizzazione, AWS Organizations ricrea il ruolo per l'account.

- AWS Organizationscrea il ruolo IAM OrganizationAccountAccessRole. Questo ruolo concede l'accesso all'account di gestione al nuovo account membro. Anche se questo ruolo può essere eliminato, ti consigliamo di non eliminarlo in modo che sia disponibile come opzione di ripristino.
- Se disponi di policy collegate al root di una gerarchia di UO, tali policy si applicano immediatamente a tutti gli utenti e a tutti i ruoli creati nell'account. I nuovi account vengono aggiunti alla UO radice per impostazione predefinita.
- Se hai abilitato l'attendibilità del servizio per un altro servizio AWS per l'organizzazione, tale servizio sicuro può creare ruoli collegati ai servizi o eseguire operazioni in qualsiasi membro account nell'organizzazione, incluso l'account creato.

Invitare un uomo Account AWS a entrare a far parte della propria organizzazione

Dopo aver creato un'organizzazione e verificato di essere il proprietario dell'indirizzo e-mail associato all'account di gestione, puoi invitare gli esistenti Account AWS a entrare a far parte della tua organizzazione.

Quando inviti un account, AWS Organizations invia un invito al proprietario dell'account, che decide se accettare o rifiutare l'invito. Puoi utilizzare la AWS Organizations console per avviare e gestire gli inviti da inviare ad altri account. È possibile inviare un invito a un altro account solo dall'account di gestione dell'organizzazione.

> **Note**
>
> La cronologia di fatturazione e i report per tutti gli account si trovano nell'account dell'entità pagante in un'organizzazione. Prima di spostare l'account in una nuova organizzazione, scarica tutta la cronologia di fatturazione e i report per qualsiasi account membro che desideri conservare. Ciò potrebbe includere report di utilizzo e costi, Report di fatturazione dettagliati o report generati dal servizio Cost Explorer.

Se sei l'amministratore di un'organizzazione Account AWS, puoi anche accettare o rifiutare un invito da un'organizzazione. Se accetti, l'account diventa un membro di tale organizzazione. L'account può far parte di una sola organizzazione, perciò se ricevi più inviti, puoi accettarne solo uno.

Nel momento in cui un account accetta l'invito a unirsi a un'organizzazione, l'account di gestione di tale organizzazione diventa responsabile per tutte le spese maturate dal nuovo account membro. Il

metodo di pagamento associato all'account membro non viene più utilizzato. Al contrario, il metodo di pagamento associato all'account di gestione dell'organizzazione viene addebitato per tutte le spese maturate dall'account membro.

Quando un account invitato entra a far parte dell'organizzazione e quest'ultima è in modalità Tutte le funzionalità, l'account di gestione dispone dell'accesso amministrativo completo e del controllo sull'account del membro invitato. Tuttavia, a differenza degli account creati, il ruolo `OrganizationAccountAccessRole` IAM non viene creato automaticamente nell'account membro con le autorizzazioni che l'account di gestione può assumere. Per crearlo e configurarlo dopo che l'account invitato diventa membro, segui i passaggiCreazione di OrganizationAccountAccessRole un account utente invitato.

> **Note**
>
> Quando crei un account nella tua organizzazione invece di invitare un account esistente a iscriversi, crea AWS Organizations automaticamente un ruolo IAM (denominato di `OrganizationAccountAccessRole` default) che puoi utilizzare per concedere agli utenti dell'account di gestione l'accesso come amministratore all'account creato.

AWS Organizations crea automaticamente un ruolo collegato ai servizi negli account dei membri invitati per supportare l'integrazione tra AWS Organizations e altri servizi. AWS Per ulteriori informazioni, consulta AWS Organizations e ruoli collegati ai servizi.

Per il numero di inviti che puoi inviare al giorno, consulta Valori massimi e minimi. Gli inviti accettati non rientrano nel calcolo di questa quota. Non appena un invito viene accettato, è possibile inviare un altro invito lo stesso giorno. Ogni invito deve ricevere risposta entro 15 giorni o scadrà.

Un invito che viene inviato a un account non rientra nel calcolo della quota degli account nell'organizzazione. Il conteggio viene ripristinato se l'account invitato rifiuta, l'account di gestione annulla l'invito o l'invito scade.

Per creare un account che faccia automaticamente parte dell'organizzazione, consulta Creazione di un account membro nell'organizzazione.

> **Important**
>
> A causa di vincoli legali e di fatturazione, puoi invitare Account AWS solo dallo stesso AWS venditore e dallo stesso AWS partizionamento dell'account di gestione. Ad esempio, in

un'organizzazione AWS EMEA, puoi invitare solo account del venditore registrato di AWS EMEA SARL.

- Tutti gli account di un'organizzazione devono provenire dal medesimo venditore di record dell'account di gestione se l'account di gestione dell'organizzazione è stato creato da Amazon Internet Services Pvt. Ltd (AISPL). Ad esempio, in qualità di AWS venditore in India, puoi invitare nella tua organizzazione solo altri account AISPL. Non puoi combinare account di AISPL AWS e/o di altri AWS venditori.
- Tutti gli account di un'organizzazione devono provenire dalla stessa AWS partizione dell'account di gestione. Gli account nella Regioni AWS partizione commerciale non possono appartenere a un'organizzazione con account della partizione China Regions o account nella AWS GovCloud (US) partizione Regioni.

Invio degli inviti agli Account AWS

Per invitare gli account a far parte dell'organizzazione, è necessario prima confermare di essere il proprietario dell'indirizzo e-mail associato all'account di gestione. Per ulteriori informazioni, consulta Verifica dell'indirizzo e-mail. Dopo avere verificato l'indirizzo e-mail, completa le seguenti fasi per invitare gli account a far parte dell'organizzazione.

Autorizzazioni minime

Per invitare un utente Account AWS a far parte della propria organizzazione, è necessario disporre delle seguenti autorizzazioni:

- `organizations:DescribeOrganization` (solo console)
- `organizations:InviteAccountToOrganization`

AWS Management Console

Per invitare un altro account a far parte dell'organizzazione

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. Se hai già verificato il tuo indirizzo email con AWS, salta questo passaggio.

Se l'indirizzo e-mail non è ancora stato verificato, segui le istruzioni contenute nell'e-mail di verifica entro 24 ore dal momento di creazione dell'organizzazione. Potrebbe trascorrere del tempo prima di ricevere il messaggio e-mail di verifica. Fino a quando non verifichi l'indirizzo e-mail, non puoi invitare altri account a far parte della tua organizzazione.

3. Passare alla pagina Account AWS e scegliere Add an AWS account (Aggiungi un account AWS).
4. Nella pagina Add an Account AWS (Aggiungi un Account AWS), scegliere Invite an existing AWS account (Invita un account AWS esistente).
5. Nella AWS pagina Invita un account esistente, per Indirizzo e-mail o ID account del Account AWS destinatario dell'invito inserisci l'indirizzo e-mail associato all'account da invitare o il relativo numero ID dell'account.
6. (Facoltativo) Per Message to include in the invitation email message (Messaggio da includere nel messaggio e-mail di invito), inserisci il testo da includere nell'invito e-mail al proprietario dell'account invitato.
7. (Facoltativo) Nella sezione Add tags (Aggiungi tag), specifica uno o più tag da assegnare automaticamente all'account dopo l'accettazione dell'invito da parte dell'amministratore. A questo scopo, scegli Add tag (Aggiungi tag) e inserisci una chiave e un valore facoltativo. Lasciando vuoto il valore, questo viene impostato su una stringa vuota; non è `null`. Puoi associare fino a 50 tag a un Account AWS.
8. Selezionare Send invitation (Invia invito).

> **Important**
>
> Se viene visualizzato un messaggio che indica il superamento delle quote degli account per l'organizzazione o l'impossibilità di aggiungere un account poiché l'organizzazione è ancora in fase di inizializzazione, contattare AWS Support.

9. La console reindirizza alla pagina Invitations (Inviti), dove è possibile visualizzare tutti gli inviti aperti e accettati. L'invito appena creato viene visualizzato nella parte superiore della lista con lo stato impostato su OPEN (APERTO).

   AWS Organizations invia un invito all'indirizzo e-mail del proprietario dell'account che hai invitato all'organizzazione. Questo messaggio e-mail include un collegamento alla AWS Organizations console, in cui il proprietario dell'account può visualizzare i dettagli e scegliere di accettare o rifiutare l'invito. In alternativa, il proprietario dell'account invitato può ignorare

il messaggio e-mail, accedere direttamente alla AWS Organizations console, visualizzare l'invito e accettarlo o rifiutarlo.

L'invito a questo account rientra immediatamente nel calcolo del numero massimo di account che è possibile avere nell'organizzazione. AWS Organizations non attende fino a quando l'account accetta l'invito. Se l'account invitato rifiuta, l'account di gestione annulla l'invito. Se l'account invitati non risponde entro il periodo di tempo specificato, l'invito scade. In entrambi i casi, l'invito non rientra più nel calcolo della quota.

AWS CLI & AWS SDKs

Per invitare un altro account a far parte dell'organizzazione

È possibile utilizzare uno dei seguenti comandi per invitare un altro account a far parte dell'organizzazione:

- AWS CLI: invite-account-to-organization

```
$ aws organizations invite-account-to-organization \
    --target '{"Type": "EMAIL", "Id": "juan@example.com"}' \
    --notes "This is a request for Juan's account to join Bill's organization."
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                 "Type": "ORGANIZATION"
            },
            {
                 "Id": "juan@example.com",
                 "Type": "EMAIL"
            }
        ],
        "RequestedTimestamp": 1481656459.257,
        "Resources": [
            {
                "Resources": [
```

```
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                         "Type": "MASTER_NAME",
                         "Value": "Management Account"
                    },
                    {
                         "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "FULL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "OPEN"
    }
}
```

- AWS SDK: InviteAccountToOrganization

Gestione degli inviti in sospeso per l'organizzazione

Quando effettui l'accesso all'account di gestione, puoi visualizzare tutti gli Account AWS collegati nell'organizzazione e annullare eventuali inviti in attesa (aperti). Per farlo, completa le seguenti fasi.

Autorizzazioni minime

Per gestire gli inviti in sospeso per l'organizzazione, è necessario disporre delle seguenti autorizzazioni:

- `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations
- `organizations:ListHandshakesForOrganization`

- `organizations:CancelHandshake`

AWS Management Console

Per visualizzare o annullare inviti che vengono inviati dall'organizzazione ad altri 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. Vai alla pagina Invitations (Inviti).

   La pagina mostra tutti gli inviti inviati dall'organizzazione e il loro stato attuale.

   > **Note**
   >
   > Gli inviti accettati, annullati e rifiutati continuano a essere visualizzati nell'elenco per 30 giorni. Successivamente, vengono eliminati e non vengono più visualizzati nell'elenco.

3. Seleziona il pulsante di opzione
   
   accant
   all'invito da annullare e scegli Cancel invitation (Cancella invito). Se il pulsante di opzione è disattivato, l'invito non può essere annullato.

   Lo stato dell'invito passa da OPEN (APERTO) a CANCELED (ANNULLATO).

   AWS invia un messaggio e-mail al proprietario dell'account indicando che hai annullato l'invito. L'account non può più far parte dell'organizzazione a meno che non venga inviato un nuovo invito.

AWS CLI & AWS SDKs

Per visualizzare o annullare inviti che vengono inviati dall'organizzazione ad altri account

È possibile utilizzare i comandi seguenti per visualizzare o annullare inviti:

- AWS CLI:, annulla-handshake list-handshakes-for-organization

- Nell'esempio seguente vengono illustrati gli inviti inviati da questa organizzazione ad altri account.

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Action": "INVITE",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1482952459.257,
            "Id": "h-examplehandshakeid111",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "juan@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1481656459.257,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type": "MASTER_EMAIL",
                            "Value": "bill@amazon.com"
                        },
                        {
                            "Type": "MASTER_NAME",
                            "Value": "Management Account"
                        },
                        {
                            "Type": "ORGANIZATION_FEATURE_SET",
                            "Value": "FULL"
                        }
                    ],
                    "Type": "ORGANIZATION",
                    "Value": "o-exampleorgid"
                },
                {
```

```
                    "Type": "EMAIL",
                    "Value": "juan@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Juan's account to join
 Bill's organization."
                }
            ],
            "State": "OPEN"
        },
        {
            "Action": "INVITE",
            "State":"ACCEPTED",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1.471797437427E9,
            "Id": "h-examplehandshakeid222",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "anika@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1.469205437427E9,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type":"MASTER_EMAIL",
                             "Value":"bill@example.com"
                        },
                        {
                            "Type":"MASTER_NAME",
                            "Value":"Management Account"
                        }
                    ],
                    "Type":"ORGANIZATION",
                    "Value":"o-exampleorgid"
                },
```

```
                {
                    "Type":"EMAIL",
                    "Value":"anika@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Anika's account to join
 Bill's organization."
                }
            ]
        }
    ]
}
```

L'esempio seguente mostra come annullare un invito a un account.

```
$ aws organizations cancel-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
        "Id": "h-examplehandshakeid111",
        "State":"CANCELED",
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "susan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid",
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@example.com"
                    },
```

```
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                        "Value": "CONSOLIDATED_BILLING"
                    }
                ]
            },
            {
                "Type": "EMAIL",
                "Value": "anika@example.com"
            },
            {
                "Type": "NOTES",
                "Value": "This is a request for Susan's account to join Bob's
 organization."
            }
        ],
        "RequestedTimestamp": 1.47008383521E9,
        "ExpirationTimestamp": 1.47137983521E9
    }
}
```

- AWS ListHandshakesForOrganizationSDK:, CancelHandshake

Accettazione o rifiuto di un invito da parte di un'organizzazione

Account AWS Potresti ricevere un invito a entrare a far parte di un'organizzazione. È possibile accettare o rifiutare l'invito. Per farlo, completa le seguenti fasi.

> **Note**
>
> Lo stato di un account rispetto a un'organizzazione determina quali dati su costi e utilizzo sono visibili:
>
> - Se un account membro non fa più parte dell'organizzazione e diventa un account standalone, non ha più accesso ai dati su costi e utilizzo da quando l'account è diventato membro dell'organizzazione. L'account ha accesso solo ai dati generati come account standalone.

- Se un account membro non fa più parte dell'organizzazione A ed entra a far parte dell'organizzazione B, non ha più accesso ai dati su costi e utilizzo relativi all'organizzazione A, ma solo ai dati generati come membro dell'organizzazione B. L'account ha accesso solo ai dati generati come membro dell'organizzazione B.
- Se un account entra di nuovo a far parte di un'organizzazione cui apparteneva in precedenza, riottiene l'accesso ai dati cronologici su costi e utilizzo.

Note

Solo gli account membri e gli account autonomi possono accettare o rifiutare un invito a entrare a far parte di un'organizzazione. Se un invito viene inviato a un account membro, tale account deve lasciare l'organizzazione attuale prima di accettare l'invito. Se un invito viene inviato a un account di gestione che fa già parte di un'organizzazione AWS , tale account non sarà in grado di accettarlo finché non rimuoverà tutti gli account membri dalla propria organizzazione ed eliminerà l'organizzazione.

Autorizzazioni minime

Per accettare o rifiutare un invito a entrare a far parte di un' AWS organizzazione, devi disporre delle seguenti autorizzazioni:

- `organizations:ListHandshakesForAccount`— Necessario per visualizzare l'elenco degli inviti nella AWS Organizations console.
- `organizations:AcceptHandshake`.
- `organizations:DeclineHandshake`.
- `iam:CreateServiceLinkedRole`— Richiesto solo quando l'accettazione dell'invito richiede la creazione di un ruolo collegato al servizio nell'account del membro per supportare l'integrazione con altri servizi. AWS Per ulteriori informazioni, consulta AWS Organizations e ruoli collegati ai servizi.

AWS Management Console

Per accettare o rifiutare un invito

1. Un invito a far parte di un'organizzazione viene inviato all'indirizzo e-mail del proprietario dell'account. Se il proprietario dell'account riceve un messaggio e-mail di invito, seguire le istruzioni contenute nell'invito e-mail o passare alla console AWS Organizations nel browser, quindi scegliere Invitations (Inviti) oppure andare direttamente alla pagina member account's Invitation (Invito dell'account membro).
2. Se richiesto, accedi all'account invitato come un utente IAM, assumi un ruolo IAM o accedi come utente root dell'account (non consigliato).
3. La pagina Inviti dell'account membro visualizza gli inviti a partecipare alle organizzazioni attualmente disponibili per il tuo account.

   Scegli Accept invitation (Accetta l'invito) o Decline invitation (Rifiuta l'invito) in base alle esigenze.

   - Se nella fase precedente scegli Accept invitation (Accetta invito), la console reindirizza alla pagina Organization overview (Panoramica dell'organizzazione) con i dettagli relativi all'organizzazione di cui l'account è ora membro. È possibile visualizzare l'ID dell'organizzazione e l'indirizzo e-mail del proprietario.

     > **Note**
     >
     > Gli inviti accettati continuano a essere visualizzati nell'elenco per 30 giorni. Successivamente, vengono eliminati e non vengono più visualizzati nell'elenco.

     AWS Organizations crea automaticamente un ruolo collegato al servizio nell'account del nuovo membro per supportare l'integrazione tra e AWS Organizations altri servizi. AWS Per ulteriori informazioni, consulta AWS Organizations e ruoli collegati ai servizi.

     AWS invia un messaggio di posta elettronica al proprietario dell'account di gestione dell'organizzazione indicando che hai accettato l'invito. Inoltre, invia un messaggio e-mail al proprietario dell'account membro affermando che l'account è ora un membro dell'organizzazione.
   - Se scegli Decline (Rifiuta) nella fase precedente, l'account rimarrà nella pagina Inviti dell'account membro in cui vengono elencati tutti gli inviti in sospeso.

AWS invia un messaggio di posta elettronica al proprietario dell'account di gestione dell'organizzazione indicando che hai rifiutato l'invito.

> **Note**
>
> Gli inviti rifiutati continuano a essere visualizzati nell'elenco per 30 giorni. Successivamente, vengono eliminati e non vengono più visualizzati nell'elenco.

AWS CLI & AWS SDKs

Per accettare o rifiutare un invito

È possibile utilizzare i comandi seguenti per accettare o rifiutare un invito:

- AWS CLI: accept-handshake, decline-handshake

  L'esempio seguente mostra come accettare un invito a far parte di un'organizzazione.

```
$ aws organizations accept-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "RequestedTimestamp": 1481656459.257,
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "juan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Resources": [
                    {
```

```
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "ALL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "ACCEPTED"
    }
}
```

L'esempio seguente mostra come rifiutare un invito a far parte di un'organizzazione.

- AWS SDK:, AcceptHandshakeDeclineHandshake

Creazione di un account membro nell'organizzazione

In questa pagina viene descritto come creare Account AWS all'interno dell'organizzazione in AWS Organizations. Per ulteriori informazioni sulle nozioni di base su AWS e sulla creazione di un singolo Account AWS, consulta il Centro risorse per le nozioni di base.

Un'organizzazione è una raccolta di Account AWS che è possibile gestire centralmente. È possibile eseguire le seguenti procedure per gestire gli account che fanno parte dell'organizzazione:

- Creazione di un Account AWS che fa parte dell'organizzazione
- Accesso a un account membro con ruolo di accesso all'account di gestione

Important

- Quando crei un account membro nell'organizzazione, AWS Organizations crea automaticamente un ruolo AWS Identity and Access Management (IAM) `OrganizationAccountAccessRole` nell'account membro che consente agli utenti e ai ruoli nell'account di gestione di esercitare il pieno controllo amministrativo sull'account membro. Questo ruolo è soggetto a qualsiasi policy di controllo dei servizi (SCP) che si applica all'account membro.

  AWS Organizations inoltre aggiunge automaticamente una policy gestita con il ruolo `OrganizationAccountAccessRole` dell'account membro. Ciò consente il controllo centralizzato, in modo che tutti gli account aggiuntivi collegati alla stessa policy gestita vengano aggiornati automaticamente ogni volta che la policy viene aggiornata. In precedenza, i nuovi account creati all'interno di un'organizzazione hanno aggiunto una policy in linea applicato solo a quel singolo account. Per ulteriori informazioni sulle policy inline, consulta Policy gestite e policy inline nella Guida per l'utente di IAM.

  Inoltre, AWS Organizations crea automaticamente anche un ruolo collegato al servizio denominato `AWSServiceRoleForOrganizations` che consente l'integrazione con determinati servizi AWS. È necessario configurare gli altri servizi per consentire l'integrazione. Per ulteriori informazioni, consulta AWS Organizations e ruoli collegati ai servizi.
- Se questa organizzazione è gestita con AWS Control Tower, crea gli account utilizzando l'account factory AWS Control Tower nella console AWS Control Tower o con le API. Se crei un account in Organizations, tale account non viene registrato a AWS Control Tower. Per ulteriori informazioni, consulta Riferimento alle risorse esterne a AWS Control Tower nella Guida per l'utente di AWS Control Tower.

Note

Gli Account AWS creati come parte di un'organizzazione non vengono automaticamente iscritti alle e-mail di marketing di AWS. Per attivare la ricezione delle e-mail di marketing per gli account, consulta https://pages.awscloud.com/communication-preferences.

Creazione di un Account AWS che fa parte dell'organizzazione

Una volta effettuato l'accesso all'account di gestione dell'organizzazione, è possibile creare account membri che fanno automaticamente parte dell'organizzazione. Quando crei un account utilizzando la seguente procedura, AWS Organizations copia automaticamente le seguenti informazioni relative al Contatto principale dall'account di gestione al nuovo account membro:

- Numero di telefono
- Company name (Nome dell'azienda)
- L'URL del sito Web
- Indirizzo

Copia inoltre il linguaggio di comunicazione e le informazioni del Marketplace (in alcuni casi il fornitore dell'account Regioni AWS) dall'account di gestione.

> **Note**
>
> AWS non raccoglie automaticamente tutte le informazioni necessarie affinché un account membro funzioni come account standalone. Se è necessario rimuovere un account membro da un'organizzazione e renderlo un account standalone, è necessario fornire tali informazioni per l'account prima di poterlo rimuovere. Per ulteriori informazioni, consulta Abbandono di un'organizzazione da un account membro.

> **Autorizzazioni minime**
>
> Per creare un account membro nell'organizzazione, è necessario disporre delle seguenti autorizzazioni:
>
> - `organizations:CreateAccount`
> - `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations
> - `iam:CreateServiceLinkedRole` (concesso all'entità `organizations.amazonaws.com` per abilitare la creazione del ruolo collegato al servizio richiesto negli account membro).

AWS Management Console

Per creare un Account AWS che faccia automaticamente parte dell'organizzazione

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. Nella pagina Account AWS, scegli Add an (Aggiungi un) Account AWS.
3. Nella pagina Add an Account AWS (Aggiungi un), scegli Create an Account AWS (Crea un) (è selezionato per impostazione predefinita).
4. Nella pagina Create an Account AWS (Crea un), per nomeAccount AWS inserisci il nome che desideri assegnare all'account. Questo nome consente di distinguere l'account da tutti gli altri account nell'organizzazione ed è separato dall'alias IAM o dal nome e-mail del proprietario.
5. Per Email address of the account's owner (Indirizzo e-mail del proprietario dell'account), inserisci l'indirizzo e-mail del proprietario dell'account. Questo indirizzo e- mail non può essere già associato a un altro Account AWS perché diventa la credenziale del nome utente per l'utente root dell'account.
6. (Facoltativo) Specifica il nome da assegnare al ruolo IAM che viene automaticamente creato nel nuovo account. Questo ruolo concede l'autorizzazione dell'account di gestione dell'organizzazione per accedere all'account membro appena creato. Se non specifichi un nome, AWS Organizations offre al ruolo un nome predefinito di `OrganizationAccountAccessRole`. Consigliamo di utilizzare il nome predefinito per tutti gli account per garantire coerenza.

   > **Important**
   >
   > Ricordare questo nome di ruolo. Sarà necessario in un secondo momento per concedere l'accesso al nuovo account per utenti e ruoli nell'account di gestione.

7. (Facoltativo) Nella sezione Tag, aggiungi uno o più tag al nuovo account scegliendo Aggiungi tag e inserendo una chiave e facoltativamente un valore. Lasciando vuoto il valore, questo viene impostato su una stringa vuota; non è `null`. Puoi associare fino a 50 tag a un account.
8. Scegli Create (Crea) Account AWS.

   - Se ricevi un messaggio di errore che indica che sono stati superati la quota di account per l'organizzazione, consulta Visualizzo un messaggio di "quota superata" quando cerco di aggiungere un account alla mia organizzazione.

- Se si riceverà un messaggio di errore che indica che non è possibile aggiungere un account perché l'inizializzazione dell'organizzazione è ancora in corso, attendere un'ora e riprovare.
- È anche possibile controllare il log AWS CloudTrail per scoprire se la creazione di un account è riuscita. Per ulteriori informazioni, consulta Registrazione e monitoraggio in AWS Organizations.
- Se l'errore persiste, contatta AWS Support.

Viene visualizzata la pagina Account AWS con il nuovo account aggiunto all'elenco.

9. Ora che l'account esiste e ha un ruolo IAM che concede l'accesso di amministratore agli utenti nell'account di gestione, è possibile accedere all'account seguendo le fasi in Accesso agli account membri nell'organizzazione.

> **Note**
>
> Quando crei un account, AWS Organizations assegna inizialmente all'utente root una password lunga (64 caratteri) e complessa, generata casualmente. Non è possibile recuperare questa password iniziale. Per accedere all'account come utente root per la prima volta, è necessario eseguire il processo di recupero della password. Per ulteriori informazioni, consulta Accesso a un account membro come utente root.

AWS CLI & AWS SDKs

Per creare un Account AWS che faccia automaticamente parte dell'organizzazione

È possibile utilizzare uno dei seguenti comandi per creare un account:

- AWS CLI: create-account

```
$ aws organizations create-account \
    --email susan@example.com \
    --account-name "Production Account"
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
```

```
}
```

Puoi quindi verificare lo stato della creazione dell'account con il seguente comando.

```
$ aws organizations describe-create-account-status \
    --create-account-request-id car-examplecreateaccountrequestid111
{
  "CreateAccountStatus": {
    "State": "SUCCEEDED",
    "AccountId": "555555555555",
    "AccountName": "Production account",
    "RequestedTimestamp": 1470684478.687,
    "CompletedTimestamp": 1470684532.472,
    "Id": "car-examplecreateaccountrequestid111"
  }
}
```

- SDK AWS: CreateAccount

Accesso agli account membri nell'organizzazione

Quando crei un account nell'organizzazione, oltre all'utente root, AWS Organizations crea automaticamente un ruolo IAM denominato per impostazione predefinita `OrganizationAccountAccessRole`. Puoi specificare un nome diverso al momento della creazione, tuttavia ti consigliamo di assegnare un nome coerente in tutti i tuoi account. In questa guida si fa riferimento al ruolo con il nome predefinito. AWS Organizations non crea altri utenti o ruoli. Per accedere all'account nell'organizzazione, è necessario utilizzare uno dei seguenti metodi:

- Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWS e le risorse nell'account. Tale identità è detta utente root Account AWS ed è possibile accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzarle 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 di IAM. Per ulteriori consigli sulla sicurezza degli utenti root, consulta la pagina Root user best practices for your Account AWS.
- Se crei un account utilizzando gli strumenti forniti come parte di AWS Organizations, puoi accedere all'account utilizzando il ruolo preconfigurato denominato `OrganizationAccountAccessRole`

che esiste in tutti i nuovi account creati in questo modo. Per ulteriori informazioni, consulta Accesso a un account membro con ruolo di accesso all'account di gestione.

- Se inviti un account esistente a far parte dell'organizzazione e l'account accetta l'invito, puoi scegliere di creare un ruolo IAM che consente all'account di gestione di accedere all'account membro invitato. Si presume che questo ruolo sia identico al ruolo aggiunto automaticamente a un account creato con AWS Organizations. Per creare questo ruolo, consulta Creazione di OrganizationAccountAccessRole un account utente invitato. Una volta creato il ruolo, è possibile accedervi tramite le fasi in Accesso a un account membro con ruolo di accesso all'account di gestione.
- Utilizzare AWS IAM Identity Center e abilitare l'accesso sicuro per IAM Identity Center con AWS Organizations. Ciò consente agli utenti di accedere al portale di accesso AWS con le proprie credenziali aziendali e di accedere alle risorse nel loro account di gestione o membro assegnato.

  Per ulteriori informazioni, consulta Autorizzazioni multi-account nella Guida per l'utente di AWS IAM Identity Center. Per ulteriori informazioni su come configurare l'accesso sicuro a IAM Identity Center, consulta AWS IAM Identity Center e AWS Organizations.

> **Autorizzazioni minime**
>
> Per accedere a un Account AWS da qualsiasi altro account nell'organizzazione, è necessario disporre delle autorizzazioni seguenti:
>
> - `sts:AssumeRole` - L'elemento `Resource` deve essere impostato su un asterisco (*) o sul numero di ID dell'account per l'account con l'utente che deve accedere al nuovo account membro

Accesso a un account membro come utente root

Quando crei un nuovo account, AWS Organizations inizialmente assegna una password all'utente root, composta da un minimo di 64 caratteri. Tutti i caratteri sono generati casualmente senza garanzie sull'aspetto di determinati set di caratteri. Non è possibile recuperare questa password iniziale. Per accedere all'account come utente root per la prima volta, è necessario eseguire il processo di recupero della password. Per ulteriori informazioni, consulta Ho dimenticato la mia password utente root Account AWS nella Guida per l'utente di AWS accesso.

> **Note**
>
> - Come best practice, consigliamo di non utilizzare l'utente root per accedere all'account, tranne per creare altri utenti e altri ruoli con più autorizzazioni limitate. Quindi accedi come uno di questi utenti o questi ruoli.
> - Inoltre, consigliamo di impostare l'autenticazione a più fattori (MFA) sull'utente root. Reimposta la password e assegna un dispositivo MFA all'utente root.
> - Se hai creato un account membro in un'organizzazione con un indirizzo e-mail non corretto, non è possibile accedere all'account come utente root. Contatta Fatturazione e AWS Support per assistenza.

Creazione di OrganizationAccountAccessRole un account utente invitato

Per impostazione predefinita, se crei un account membro come parte dell'organizzazione, AWS crea automaticamente un ruolo nell'account che concede le autorizzazioni di amministratore agli utenti IAM delegati nell'account di gestione. Per impostazione predefinita, tale ruolo è denominato `OrganizationAccountAccessRole`. Per ulteriori informazioni, consulta Accesso a un account membro con ruolo di accesso all'account di gestione.

Tuttavia, gli account membro invitati a far parte dell'organizzazione non ottengono automaticamente un ruolo amministratore creato. È necessario eseguire questa operazione manualmente, come illustrato nella procedura seguente. Essenzialmente, in questo modo viene duplicato il ruoto automaticamente configurato per gli account creati. Consigliamo di utilizzare lo stesso nome, `OrganizationAccountAccessRole`, per i ruoli creati manualmente per coerenza e facilità di memorizzazione.

AWS Management Console

Per creare un ruolo amministratore di AWS Organizations in un account membro

1. Accedi alla console IAM all'indirizzo https://console.aws.amazon.com/iam/. È necessario accedere come utente IAM, assumere un ruolo IAM o accedere come utente root (non consigliato) nell'account membro. L'utente o il ruolo devono avere autorizzazioni per creare i ruoli e le policy IAM.
2. Nella console IAM, accedi a Ruoli e quindi scegli Crea ruolo.
3. Scegli Account AWS, quindi seleziona Altro Account AWS.

4. Inserisci il numero ID dell'account a 12 cifre dell'account di gestione a cui desideri concedere l'accesso come amministratore. In Opzioni, tieni presente quanto segue:

   - Per questo ruolo, poiché gli account sono interni all'azienda, non è necessario scegliere Require external ID (Richiedi ID esterno). Per ulteriori informazioni sull'opzione ID esterno, vedi Quando devo usare un ID esterno? nella Guida per l'utente IAM.
   - Se l'MFA è abilitata e configurata, è possibile scegliere di richiedere l'autenticazione utilizzando un dispositivo MFA. Per ulteriori informazioni sulla MFA, consulta Using Multi-Factor Authentication (MFA) AWS nella IAM User Guide.

5. Seleziona Avanti.
6. Nella pagina Aggiungi autorizzazioni, scegli la policy AWS gestita denominata, quindi scegli **`AdministratorAccess`** Avanti.
7. Nella pagina Nome, revisione e creazione, specifica un nome di ruolo e una descrizione facoltativa. Consigliamo di utilizzare `OrganizationAccountAccessRole`, per coerenza con il nome predefinito assegnato al ruolo nei nuovi account. Per rendere effettive le modifiche, scegliere Create role (Crea ruolo).
8. Il nuovo ruolo viene visualizzato nell'elenco di ruoli disponibili. Scegli il nome del nuovo ruolo per visualizzare i dettagli, facendo particolare attenzione all'URL del link che viene fornito. Assegnare questo URL agli utenti nell'account membro che deve accedere al ruolo. Inoltre, prendere nota del Role ARN (ARN ruolo) perché sarà necessario nella fase 15.
9. Accedi alla console IAM all'indirizzo https://console.aws.amazon.com/iam/. A questo punto, accedi come utente nell'account di gestione che dispone delle autorizzazioni per creare policy e assegnare le policy a utenti o gruppi.
10. Passa a Politiche e quindi scegli Crea politica.
11. In Service (Servizio), scegliere STS.
12. In Azioni, iniziare a digitare **`AssumeRole`** nella casella Filtro e quindi selezionare la casella di controllo accanto quando viene visualizzata.
13. In Risorse, assicurati che sia selezionato Specifico, quindi scegli Aggiungi ARN.
14. Inserisci il numero di ID dell'account membro AWS e quindi inserisci il nome del ruolo creato in precedenza alle fasi 1-8. Scegli Aggiungi ARN.
15. Se si concede l'autorizzazione per assumere il ruolo in più account membri, ripetere le fasi 14 e 15 per ogni account.
16. Seleziona Avanti.

17. Nella pagina Rivedi e crea, inserisci un nome per la nuova politica, quindi scegli Crea politica per salvare le modifiche.
18. Scegli Gruppi di utenti nel riquadro di navigazione, quindi scegli il nome del gruppo (non la casella di controllo) che desideri utilizzare per delegare l'amministrazione dell'account membro.
19. Scegli la scheda Permissions (Autorizzazioni).
20. Scegli Aggiungi autorizzazioni, scegli Allega politiche, quindi seleziona la politica che hai creato nei passaggi 11—18.

Gli utenti che sono membri del gruppo selezionato ora possono utilizzare l'URL che hai acquisito nella fase 9 per accedere a ciascun ruolo dell'account membro. Possono accedere a questi account membri esattamente come se accedessero a un account creato nell'organizzazione. Per ulteriori informazioni su come utilizzare il ruolo per amministrare un account membro, consulta Accesso a un account membro con ruolo di accesso all'account di gestione.

Accesso a un account membro con ruolo di accesso all'account di gestione

Quando crei un account membro utilizzando la console AWS Organizations, AWS Organizations crea automaticamente un ruolo IAM denominato `OrganizationAccountAccessRole` nell'account. Questo ruolo dispone di autorizzazioni amministrative complete nell'account membro. L'ambito di accesso per questo ruolo include tutti i principali nell'account di gestione, in modo che sia in grado di concedere l'accesso all'account di gestione dell'organizzazione. È possibile creare un ruolo identico per un account membro invitato seguendo le fasi indicate in Creazione di OrganizationAccountAccessRole un account utente invitato. Per utilizzare questo ruolo per accedere all'account membro, è necessario accedere come utente dall'account di gestione che dispone delle autorizzazioni per assumere il ruolo. Per configurare queste autorizzazioni, eseguire la procedura seguente. Consigliamo di concedere le autorizzazioni ai gruppi anziché agli utenti per semplificare la manutenzione.

AWS Management Console

Per concedere autorizzazioni ai membri di un gruppo IAM nell'account di gestione per accedere al ruolo (console)

1. Accedi alla console IAM all'indirizzo https://console.aws.amazon.com/iam/come utente con autorizzazioni di amministratore nell'account di gestione. Questo passaggio è obbligatorio per

delegare le autorizzazioni al gruppo IAM i cui utenti potranno accedere al ruolo nell'account membro.

2. Iniziare creando le policy gestite necessarie in seguito in ???.

   Nel pannello di navigazione, seleziona Policy e Crea policy.

3. Nella scheda Editor visivo scegliere Scegli un servizio, digitare **`STS`** nella casella di ricerca per filtrare l'elenco e quindi scegliere l'opzione STS.

4. Nella sezione Azioni, digita **`assume`** nella casella di ricerca per filtrare l'elenco, quindi scegli l'opzione. AssumeRole

5. Nella sezione Risorse, scegli Specifico, scegli Aggiungi ARN, quindi digita il numero di account del membro e il nome del ruolo che hai creato nella sezione precedente (ti consigliamo di assegnargli un nome). `OrganizationAccountAccessRole`

6. Scegliete Aggiungi ARN quando nella finestra di dialogo viene visualizzato l'ARN corretto.

7. (Opzionale) Se si desidera richiedere Multi-Factor Authentication (MFA) o limitare l'accesso al ruolo da un intervallo di indirizzi IP specificato, espandere la sezione Condizioni di richiesta e selezionare le opzioni che si desidera applicare.

8. Seleziona Avanti.

9. Nella pagina Rivedi e crea, inserisci un nome per la nuova politica. Ad esempio: **`GrantAccessToOrganizationAccountAccessRole`**. Puoi anche aggiungere una descrizione opzionale.

10. Selezionare Crea policy per salvare la nuova policy gestita.

11. Ora che la policy è disponibile, è possibile collegarla a un gruppo.

    Nel riquadro di navigazione, scegli Gruppi di utenti, quindi scegli il nome del gruppo (non la casella di controllo) i cui membri desideri che assumano il ruolo nell'account membro. Se necessario, è possibile creare un nuovo gruppo.

12. Nella scheda Permissions (Autorizzazioni), scegli Add permissions (Aggiungi autorizzazioni), quindi Attach policies (Collega policy).

13. (Opzionale) Nella casella Cerca è possibile iniziare a digitare il nome della policy per filtrare l'elenco finché non viene visualizzato il nome della policy appena creata in Step 2 tramite Step 10. Puoi anche filtrare tutte le politiche AWS gestite selezionando Tutti i tipi e quindi scegliendo Gestito dal cliente.

14. Seleziona la casella accanto alla tua politica, quindi scegli Allega politiche.

Gli utenti IAM che sono membri del gruppo ora dispongono delle autorizzazioni per passare al nuovo ruolo nella console AWS Organizations seguendo la procedura riportata di seguito.

AWS Management Console

Per passare al ruolo per l'account membro

Quando si utilizza il ruolo, l'utente dispone di autorizzazioni di amministratore nel nuovo account membro. Spiega agli utenti IAM che sono membri del gruppo di eseguire le seguenti operazioni per passare al nuovo ruolo.

1. Dall'angolo in alto a destra della console AWS Organizations, scegliere il link che contiene l'attuale nome di accesso e quindi scegliere Switch role (Cambia ruolo).
2. Inserire il numero di ID dell'account fornito dall'amministratore e il nome del ruolo.
3. In Display Name (Nome visualizzazione), inserire il testo che si desidera visualizzare sulla barra di navigazione nell'angolo in alto a destra al posto dell'attuale nome utente mentre si sta utilizzando il ruolo. È anche possibile scegliere un colore.
4. Seleziona Switch Role (Cambia ruolo). Ora tutte le azioni eseguite vengono effettuate con le autorizzazioni concesse al ruolo a cui si è passati. Non sono più disponibili le autorizzazioni associate all'utente IAM originale finché non si cambia nuovamente questa opzione.
5. Una volta completata l'esecuzione delle operazioni che richiedono le autorizzazioni del ruolo, è possibile tornare all'utente IAM normale. Scegli il nome del ruolo nell'angolo in alto a destra (qualunque cosa tu abbia specificato come nome visualizzato), quindi scegli Torna a. ***UserName***

Risorse aggiuntive

- Per ulteriori informazioni sulla concessione delle autorizzazioni per cambiare ruolo, consulta Concedere a un utente le autorizzazioni per cambiare ruolo nella Guida per l'utente IAM.
- Per ulteriori informazioni sull'utilizzo di un ruolo per il quale ti è stata concessa l'autorizzazione ad assumere, consulta Switching to a role (console) nella IAM User Guide.
- Per un tutorial sull'utilizzo dei ruoli per l'accesso tra account diversi, consulta Tutorial: Delegate access across Account AWS using IAM roles nella IAM User Guide.
- Per informazioni sulla chiusura degli Account AWS, consulta Chiusura di un account membro nell'organizzazione.

Esportazione dei dettagli dell'Account AWS per la tua organizzazione

Con AWS Organizations, gli utenti di account di gestione e gli amministratori delegati di un'organizzazione possono esportare un file .csv con tutti i dettagli dell'account all'interno di un'organizzazione. Di conseguenza, gli amministratori dell'organizzazione possono facilmente visualizzare gli account e filtrare per stato: `ACTIVE`, `SUSPENDED`, oppure `PENDING`. Se la tua organizzazione ha molti account, l'opzione di download del file .csv fornisce un modo semplice per visualizzare e ordinare i dettagli dell'account in un foglio di calcolo.

In precedenza era possibile solo visualizzare la gerarchia degli account o un elenco nella AWS Organizationsconsole.

> **Note**
>
> Solo le entità nell'account di gestione possono scaricare l'elenco degli account.

Esporta un elenco di tutti gli Account AWS nell'organizzazione.

Una volta effettuato l'accesso all'account di gestione dell'organizzazione, è possibile creare account membri che fanno automaticamente parte dell'organizzazione. L'elenco contiene i dettagli di ogni account; tuttavia, non specifica a quale unità organizzativa (OU) appartengono.

Il file .csv contiene le informazioni seguenti per ciascun account:

- ID account - Identificatore numerico dell'account. Ad esempio: 123456789012.
- ARN - Amazon Resource Name per l'account. Ad esempio: `arn:aws:organizations::123456789012account/o-o1gb0d1234/123456789012`
- E-mail - L'indirizzo e-mail associato all'account. Ad esempio: marymajor@example.com
- Nome- Nome dell'account fornito dal creatore dell'account. Ad esempio: account di test della fase
- Stato- Stato dell'account all'interno dell'organizzazione. Il valore può essere `PENDING`, `ACTIVE` o `SUSPENDED`.
- Metodo Joined - Specifica come è stato creato l'account. Il valore può essere `INVITED` o `CREATED`.
- Timestamp Joined - Data e ora in cui l'account si è unito all'organizzazione.

Autorizzazioni minime

Per esportare un file .csv con tutti gli account membri nell'organizzazione, è necessario disporre delle seguenti autorizzazioni:

- `organizations:DescribeOrganization`
- `organizations:ListAccounts`

AWS Management Console

Per esportare un file .csv per tutti gli Account AWS nell'organizzazione

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 Actions (Operazioni), quindi per Account AWS scegli Export account list (Esporta l'elenco degli account). Il banner blu nella parte superiore della pagina indica “Export is in progress!” (L'esportazione è in corso).
3. Quando il file è pronto, il banner diventa verde e indica: “Download is ready!” (Il download è pronto). Scegli Download CSV (Scarica CSV). Il file `Organization_accounts_information.csv` si scarica sul tuo dispositivo.

AWS CLI & AWS SDKs

L'unico modo per esportare il file .csv con i dettagli dell'account è utilizzare laAWS Management Console. Non è possibile esportare il file con estensione .csv dell'elenco degli account utilizzando la AWS CLI.

Rimozione di un account membro dall'organizzazione

Parte della gestione degli account in un'organizzazione consiste nella rimozione degli account membro che non ti servono più. La rimozione di un account membro non chiude l'account, ma lo rimuove dall'organizzazione. Il precedente account membro diventa un Account AWS autonomo che non è più gestito da AWS Organizations. Successivamente, l'account non è più soggetto ad alcuna policy ed è responsabile del pagamento delle proprie fatture. All'account di gestione

dell'organizzazione non vengono più addebitate le spese sostenute dall'account dopo la rimozione dall'organizzazione.

Per ulteriori informazioni sulla rimozione dell'account di gestione, consulta Eliminazione di un'organizzazione.

Argomenti

Considerazioni prima della rimozione di un account da un'organizzazione

Prima di rimuovere un account, è importante considerare le seguenti informazioni:

- È possibile rimuovere un account dall'organizzazione solo se l'account dispone delle informazioni richieste per operare come account standalone. Quando crei un account in un'organizzazione utilizzando la console AWS Organizations, l'API o i comandi della AWS CLI, tutte le informazioni richieste per gli account autonomi non vengono raccolte automaticamente. Se desideri rendere standalone un account, devi scegliere un piano di supporto, fornire e verificare le informazioni di contatto richieste e fornire un metodo di pagamento valido. AWS utilizza il metodo di pagamento per addebitare le attività fatturabili (non il piano gratuito AWS) di AWS effettuate durante il periodo in cui l'account non è associato a un'organizzazione. Per rimuovere un account che non dispone ancora di queste informazioni, completa le operazioni riportate in Abbandono di un'organizzazione da un account membro.
- Per rimuovere un account creato nell'organizzazione, è necessario attendere almeno sette giorni dopo la creazione dell'account. Gli account invitati non sono soggetti a questo tempo di attesa.
- Al momento l'account lascia con successo l'organizzazione, il proprietario dell'Account AWSdiventa responsabile di tutti i nuovi costi AWS sostenuti e viene utilizzato il metodo di pagamento dell'account. L'account di gestione dell'organizzazione non è più responsabile.
- L'account che desideri rimuovere non deve essere un account di amministratore delegato per qualsiasi servizio AWS abilitato per l'organizzazione. Se l'account è un amministratore delegato, devi prima modificare l'account di amministratore delegato in un altro account che rimane nell'organizzazione. Per ulteriori informazioni su come disabilitare o modificare l'account amministratore delegato per un servizio AWS, consulta la documentazione del rispettivo servizio.

- Anche dopo la rimozione degli account creati (account creati utilizzando la console AWS Organizations o l'API `CreateAccount`) all'interno di un'organizzazione, (i) gli account creati sono disciplinati dai termini previsti dall'accordo con noi sull'account di gestione di creazione e (ii) l'account di gestione di creazione rimane responsabile in solido per le operazioni intraprese dai suoi account creati. Gli accordi dei clienti con noi e i diritti e gli obblighi derivanti da tali accordi non possono essere assegnati o trasferiti senza il nostro previo consenso. Per ottenere il nostro consenso, contatta AWS.
- Quando un account membro non fa più parte dell'organizzazione, non ha più accesso ai dati su costi e utilizzo relativi all'intervallo di tempo in cui l'account era membro dell'organizzazione. Tuttavia, l'account di gestione dell'organizzazione può comunque accedere ai dati. Se l'account torna a far parte dell'organizzazione, potrà accedere di nuovo a tali dati.
- Quando un account membro lascia un'organizzazione, tutti i tag associati all'account vengono eliminati.
- Quando rimuovi un account membro dall'organizzazione, qualsiasi ruolo IAM creato per consentire l'accesso da parte dell'account di gestione dell'organizzazione non viene eliminato automaticamente. Se desideri terminare l'accesso dall'account di gestione dell'organizzazione precedente, è necessario eliminare manualmente il ruolo IAM. Per informazioni sull'eliminazione di un ruolo, consulta Eliminazione di ruoli o profili delle istanze nella Guida per l'utente di IAM.

Effetti della rimozione di un account da un'organizzazione

Quando rimuovi un account da un'organizzazione, non vengono apportate modifiche dirette all'account. Tuttavia, si verificano i seguenti effetti indiretti:

- L'account è ora responsabile del pagamento delle proprie spese e deve disporre di un metodo di pagamento valido collegato all'account.
- I principali nell'account non sono più interessati da alcuna policy applicata nell'organizzazione. Ciò significa che le restrizioni imposte dalle SCP non sono più presenti e che gli utenti e i ruoli nell'account potrebbero disporre di più autorizzazioni rispetto a prima. Altri tipi di policy dell'organizzazione non possono più essere applicati o elaborati.
- Se utilizzi la chiave di condizione `aws:PrincipalOrgID` in qualsiasi policy per limitare l'accesso solo agli utenti e ai ruoli dagli Account AWS nell'organizzazione, è necessario esaminare ed eventualmente aggiornare queste policy prima di rimuovere l'account membro. Se non si aggiornano le policy, gli utenti e i ruoli dell'account potrebbero perdere l'accesso alle risorse quando l'account lascia l'organizzazione.

- L'integrazione con altri servizi potrebbe essere disabilitata. Se elimini un account da un'organizzazione che dispone dell'integrazione abilitata con un servizio AWS, gli utenti in tale account non saranno più in grado di utilizzare il servizio.

Rimozione di un account membro dall'organizzazione

Quando effettui l'accesso all'account di gestione dell'organizzazione, è possibile rimuovere gli account membri non più necessari dall'organizzazione. Per farlo, completare la seguente procedura. Questa procedura si applica solo agli account membro. Per rimuovere l'account di gestione, è necessario eliminare l'organizzazione.

> **Note**
>
> Se un account membro viene rimosso da un'organizzazione, non sarà più coperto dagli accordi dell'organizzazione. Prima della rimozione, gli amministratori degli account di gestione devono avvertire gli account membri che saranno rimossi dall'organizzazione, per consentire loro di attivare nuovi accordi se necessario. È possibile visualizzare l'elenco degli accordi attivi dell'organizzazione nella console AWS Artifact, nella pagina Accordi dell'organizzazione AWS Artifact.

> **Autorizzazioni minime**
>
> Per rimuovere uno o più account membri dall'organizzazione, è necessario effettuare l'accesso come utente o ruolo nell'account di gestione con le seguenti autorizzazioni:
>
> - `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations
> - `organizations:RemoveAccountFromOrganization`
>
> Se scegli di accedere come utente o ruolo in un account membro nel passaggio 5, tale utente o tale ruolo deve disporre delle seguenti autorizzazioni:
>
> - `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations.

- `organizations:LeaveOrganization` - Tieni presente che l'amministratore dell'organizzazione può applicare una policy all'account che rimuove questa autorizzazione, impedendoti di rimuovere l'account dall'organizzazione.
- Se accedi come utente IAM e l'account non dispone di informazioni di pagamento, l'utente deve disporre delle autorizzazioni `aws-portal:ModifyBilling` e `aws-portal:ModifyPaymentMethods` (se l'account non è ancora migrato alle autorizzazioni granulari) oppure delle autorizzazioni `payments:CreatePaymentInstrument` e `payments:UpdatePaymentPreferences` (se l'account è migrato alle autorizzazioni granulari). Inoltre, per l'account membro deve essere abilitato l'accesso utente IAM alla fatturazione. Se non è già abilitato, consulta Attivazione dell'accesso alla console Gestione fatturazione e costi nella Guida per l'utente di AWS Billing.

AWS Management Console

Per rimuovere un account membro dall'organizzazione

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. Nella pagina Account AWS, individua e seleziona la casella di controllo
   ☑
   accanto all'account membro che desideri rimuovere dall'organizzazione. È possibile spostarsi nella gerarchia delle unità organizzative o abilitare View Account AWS only (Visualizza solo gli Account AWS) per visualizzare un elenco dei soli account senza la struttura dell'unità organizzativa. Se hai molti account, potresti dover scegliere Load more accounts (Carica più account) in 'nome-UO' nella parte inferiore dell'elenco per trovare tutti gli oggetti da spostare.

   Nella pagina Account AWS, individua e seleziona il nome dell'account membro che desideri rimuovere dall'organizzazione. Potrebbe essere necessario espandere le UO (scegli l'opzione ▶) per individuare l'account desiderato.
3. Scegli Actions (Operazioni), quindi in Account AWS scegli Remove from organization (Rimuovi dall'organizzazione).
4. Nella casella di testo Remove (Rimuovere) account 'nome-account' (#numero-id-account) from organization (dall'organizzazione)?, scegli Remove account (Rimuovi account).

5. Se AWS Organizations non è stato in grado di rimuovere uno o più account, in genere è perché non sono state fornite tutte le informazioni necessarie affinché l'account operi come account standalone. Esegui queste fasi:

   a. Accedi agli account con esito negativo. Consigliamo di accedere all'account utente scegliendo Copy link (Copia link) e quindi incollandolo nella barra degli indirizzi di una nuova finestra del browser in incognito. Se non utilizzi una finestra di navigazione in incognito, viene effettuata la disconnessione dell'account di gestione e non sarà possibile tornare a questa finestra di dialogo.

   b. Il browser reindirizza direttamente alla procedura di accesso per completare eventuali fasi mancanti per questo account. Completare tutte le fasi presentate. Queste possono includere quanto segue:

      - Fornisci informazioni di contatto
      - Fornire un metodo di pagamento valido
      - Verificare il numero di telefono
      - Selezionare un'opzione di piano di supporto

   c. Una volta completata l'ultima fase di registrazione, AWS reindirizza automaticamente il browser alla console AWS Organizations per l'account membro. Scegliere Lascia l'organizzazione e quindi confermare la scelta nella finestra di dialogo di conferma. Viene effettuato il reindirizzamento alla pagina Getting Started (Nozioni di base) della console AWS Organizations, in cui è possibile visualizzare eventuali inviti in sospeso dell'account per far parte di altre organizzazioni.

   d. Rimuovi i ruoli IAM che concedono l'accesso all'account dall'organizzazione.

      > **Important**
      >
      > Se l'account è stato creato nell'organizzazione, Organizations crea automaticamente un ruolo IAM nell'account che abilita l'accesso dall'account di gestione dell'organizzazione. Se l'account è stato invitato a unirsi, Organizations non crea automaticamente un tale ruolo, ma è possibile che uno sia stato creato dall'utente o da un altro amministratore per ottenere gli stessi vantaggi. In entrambi i casi, quando si rimuove l'account dall'organizzazione, tale ruolo non viene eliminato automaticamente. Se desideri terminare l'accesso dall'account di gestione dell'organizzazione precedente, è necessario eliminare manualmente

questo ruolo IAM. Per informazioni sull'eliminazione di un ruolo, consulta Eliminazione di ruoli o profili delle istanze nella Guida per l'utente di IAM.

AWS CLI & AWS SDKs

Per rimuovere un account membro dall'organizzazione

È possibile utilizzare uno dei seguenti comandi per rimuovere un account membro:

- AWS CLI: remove-account-from-organization

```
$ aws organizations remove-account-from-organization \
    --account-id 123456789012
```

Questo comando non produce alcun output se ha esito positivo.

- SDK AWS: RemoveAccountFromOrganization

Dopo la rimozione dell'account membro dall'organizzazione, assicurati di rimuovere i ruoli IAM che concedono l'accesso all'account dall'organizzazione.

> **Important**
>
> Se l'account è stato creato nell'organizzazione, Organizations crea automaticamente un ruolo IAM nell'account che abilita l'accesso dall'account di gestione dell'organizzazione. Se l'account è stato invitato a unirsi, Organizations non crea automaticamente un tale ruolo, ma è possibile che uno sia stato creato dall'utente o da un altro amministratore per ottenere gli stessi vantaggi. In entrambi i casi, quando si rimuove l'account dall'organizzazione, tale ruolo non viene eliminato automaticamente. Se desideri terminare l'accesso dall'account di gestione dell'organizzazione precedente, è necessario eliminare manualmente questo ruolo IAM. Per informazioni sull'eliminazione di un ruolo, consulta Eliminazione di ruoli o profili delle istanze nella Guida per l'utente di IAM.

Gli account membro possono invece rimuovere se stessi con leave-organization. Per ulteriori informazioni, consulta Abbandono di un'organizzazione da un account membro.

Abbandono di un'organizzazione da un account membro

Quando effettui l'accesso a un account membro, è possibile rimuovere quell'unico account dalla sua organizzazione. Per farlo, completare la seguente procedura. Questa procedura si applica solo agli account membro. L'account di gestione non è in grado di lasciare l'organizzazione utilizzando questa tecnica. Per rimuovere l'account di gestione, è necessario eliminare l'organizzazione.

Note

Lo stato di un account rispetto a un'organizzazione determina quali dati su costi e utilizzo sono visibili:

- Se un account membro non fa più parte dell'organizzazione e diventa un account standalone, non ha più accesso ai dati su costi e utilizzo da quando l'account è diventato membro dell'organizzazione. L'account ha accesso solo ai dati generati come account standalone.
- Se un account membro non fa più parte dell'organizzazione A ed entra a far parte dell'organizzazione B, non ha più accesso ai dati su costi e utilizzo relativi all'organizzazione A, ma solo ai dati generati come membro dell'organizzazione B. L'account ha accesso solo ai dati generati come membro dell'organizzazione B.
- Se un account entra di nuovo a far parte di un'organizzazione cui apparteneva in precedenza, riottiene l'accesso ai dati cronologici su costi e utilizzo.

Important

Se lasci un'organizzazione, non sarà più effettiva la copertura degli accordi dell'organizzazione accettati per tuo conto dall'account di gestione dell'organizzazione. È possibile visualizzare un elenco di questi accordi dell'organizzazione nella console AWS Artifact, nella pagina Accordi dell'organizzazione AWS Artifact. Prima di lasciare l'organizzazione, dovresti determinare (con l'assistenza dei tuoi team legali, sulla privacy o di conformità, ove appropriato) se è necessario per te avere nuovi contratti in atto.

Autorizzazioni minime

Per lasciare un'organizzazione AWS, è necessario disporre delle seguenti autorizzazioni:

- `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations.
- `organizations:LeaveOrganization` - Tieni presente che l'amministratore dell'organizzazione può applicare una policy all'account che rimuove questa autorizzazione, impedendoti di rimuovere l'account dall'organizzazione.
- Se accedi come utente IAM e l'account non dispone di informazioni di pagamento, l'utente deve disporre delle autorizzazioni `aws-portal:ModifyBilling` e `aws-portal:ModifyPaymentMethods` (se l'account non è ancora migrato alle autorizzazioni granulari) oppure delle autorizzazioni `payments:CreatePaymentInstrument` e `payments:UpdatePaymentPreferences` (se l'account è migrato alle autorizzazioni granulari). Inoltre, per l'account membro deve essere abilitato l'accesso utente IAM alla fatturazione. Se non è già abilitato, consulta Attivazione dell'accesso alla console Gestione fatturazione e costi nella Guida per l'utente di AWS Billing.

AWS Management Console

Per abbandonare un'organizzazione dall'account membro

1. Accedi alla console AWS Organizations all'indirizzo AWS Organizations console. È necessario accedere come utente IAM, assumere un ruolo IAM o accedere come utente root (non consigliato) in un account membro.

   Per impostazione predefinita, non è necessario effettuare l'accesso alla password dell'utente root in un account membro che è stato creato utilizzando AWS Organizations. Se necessario, recuperare la password dell'utente root seguendo le fasi in Accesso a un account membro come utente root.
2. Nella pagina Pannello di controllo dell'organizzazione, scegli Lascia questa organizzazione.
3. Nella finestra di dialogo Conferma l'abbandono dell'organizzazione, scegliere Lascia l'organizzazione. Quando richiesto, confermare la scelta per rimuovere l'account. Una volta confermato, viene effettuato il reindirizzamento alla pagina Nozioni di base della console AWS Organizations, in cui è possibile visualizzare eventuali inviti in sospeso dell'account a far parte di altre organizzazioni.

Se viene visualizzato il messaggio Non puoi ancora lasciare l'organizzazione, significa che il tuo account non dispone di tutte le informazioni necessarie per funzionare come account indipendente. In tal caso, procedi alla fase successiva.

4. Se nella finestra di dialogo Conferma l'abbandono dell'organizzazione viene visualizzato il messaggio Non puoi ancora lasciare l'organizzazione, scegli il link Completa le fasi di accesso dell'account.
5. Nella pagina Registrati a AWS, inserisci tutte le informazioni necessarie affinché questo diventi un account indipendente. Potrebbe includere i seguenti tipi di informazioni:

   - Nome e indirizzo del contatto
   - Metodo di pagamento valido
   - Verifica del numero di telefono
   - Opzioni del piano di supporto
6. Quando viene visualizzata la finestra di dialogo che indica che il processo di registrazione è completo, scegliere Lascia organizzazione.

   Viene visualizzata una finestra di dialogo di conferma. Confermare la scelta per rimuovere l'account. Viene effettuato il reindirizzamento alla pagina Getting Started (Nozioni di base) della console AWS Organizations, in cui è possibile visualizzare eventuali inviti in sospeso dell'account per far parte di altre organizzazioni.
7. Rimuovi i ruoli IAM che concedono l'accesso all'account dall'organizzazione.

   > **Important**
   >
   > Se l'account è stato creato nell'organizzazione, Organizations crea automaticamente un ruolo IAM nell'account che abilita l'accesso dall'account di gestione dell'organizzazione. Se l'account è stato invitato a unirsi, Organizations non crea automaticamente un tale ruolo, ma è possibile che uno sia stato creato dall'utente o da un altro amministratore per ottenere gli stessi vantaggi. In entrambi i casi, quando si rimuove l'account dall'organizzazione, tale ruolo non viene eliminato automaticamente. Se desideri terminare l'accesso dall'account di gestione dell'organizzazione precedente, è necessario eliminare manualmente questo ruolo IAM. Per informazioni sull'eliminazione di un ruolo, consulta Eliminazione di ruoli o profili delle istanze nella Guida per l'utente di IAM.

AWS CLI & AWS SDKs

Per lasciare un'organizzazione come account membro

Per lasciare un'organizzazione, è possibile utilizzare uno dei seguenti comandi:

- AWS CLI: leave-organization

  Nell'esempio seguente l'account le cui credenziali vengono utilizzate per eseguire il comando viene fatto uscire dall'organizzazione.

  ```
  $ aws organizations leave-organization
  ```

  Questo comando non produce alcun output se ha esito positivo.
- SDK AWS: LeaveOrganization

Dopo che l'account membro ha lasciato l'organizzazione, assicurati di rimuovere i ruoli IAM che concedono l'accesso all'account dall'organizzazione.

> **Important**
>
> Se l'account è stato creato nell'organizzazione, Organizations crea automaticamente un ruolo IAM nell'account che abilita l'accesso dall'account di gestione dell'organizzazione. Se l'account è stato invitato a unirsi, Organizations non crea automaticamente un tale ruolo, ma è possibile che uno sia stato creato dall'utente o da un altro amministratore per ottenere gli stessi vantaggi. In entrambi i casi, quando si rimuove l'account dall'organizzazione, tale ruolo non viene eliminato automaticamente. Se desideri terminare l'accesso dall'account di gestione dell'organizzazione precedente, è necessario eliminare manualmente questo ruolo IAM. Per informazioni sull'eliminazione di un ruolo, consulta Eliminazione di ruoli o profili delle istanze nella Guida per l'utente di IAM.

Gli account membro possono anche essere rimossi da un utente nell'account di gestione con remove-account-from-organization. Per ulteriori informazioni, consulta Rimozione di un account membro dall'organizzazione.

Chiusura di un account membro nell'organizzazione

Se non hai più bisogno di un account membro nella tua organizzazione, puoi chiuderlo dalla AWS Organizations console seguendo le istruzioni in questa sezione. Puoi chiudere un account membro utilizzando la AWS Organizations console solo se l'organizzazione è in modalità Tutte le funzionalità.

Puoi anche chiuderlo Account AWS direttamente dalla pagina Account AWS Management Console dopo aver effettuato l'accesso come utente root. Per step-by-step istruzioni, consulta Close an Account AWS nella Guida alla gestioneAWS dell'account.

Per chiudere un account di gestione, consultaChiusura di un account di gestione nell'organizzazione.

Come chiudere un account membro

Una volta effettuato l'accesso all'account di gestione dell'organizzazione, è possibile chiudere gli account membri che fanno parte dell'organizzazione. Per farlo, completa le seguenti fasi.

> **Important**
>
> Prima di chiudere il tuo account membro, ti consigliamo vivamente di esaminare le considerazioni e comprendere l'impatto della chiusura di un account. Per ulteriori informazioni, consulta Cosa devi sapere prima di chiudere l'account e Cosa aspettarti dopo la chiusura dell'account nella Guida alla gestione dell'AWS account.

AWS Management Console

Per chiudere un account membro dalla AWS Organizations console

1. Accedi alla consoleAWS Organizations.
2. Nella pagina Account AWS, individua e seleziona il nome dell'account membro che desideri chiudere. È possibile spostarsi nella gerarchia delle unità organizzative o visualizzare un elenco dei soli account senza la struttura dell'unità organizzativa.
3. Scegli Close (Chiudi) accanto al nome dell'account nella parte superiore della pagina. Le organizzazioni in modalità di fatturazione consolidata non saranno in grado di visualizzare il pulsante Chiudi nella console. Per chiudere un account in modalità di fatturazione consolidata, segui i passaggi nella scheda Account autonomo da Come chiudere l'account nella Guida alla gestione dell'account.AWS

4. Seleziona ciascuna casella di controllo per confermare tutte le istruzioni di chiusura dell'account richieste.
5. Inserisci l'ID dell'account membro, quindi scegli Chiudi account.

> **Note**
>
> Qualsiasi account membro che chiudi mostrerà un'SUSPENDEDetichetta accanto al nome dell'account nella AWS Organizations console.

Per chiudere un account membro dalla pagina Account

Facoltativamente, puoi chiudere un account AWS membro direttamente dalla pagina Account di. AWS Management ConsolePer ulteriori step-by-step informazioni, segui le istruzioni riportate in Chiudi e Account AWSnella Guida alla gestioneAWS dell'account.

AWS CLI & AWS SDKs

Per chiudere un Account AWS

Per chiudere un account AWS , puoi utilizzare uno dei seguenti comandi:

- AWS CLI: close-account

```
$ aws organizations close-account \
    --account-id 123456789012
```

Questo comando non produce alcun output se ha esito positivo.

- AWS SDK: CloseAccount

Protezione degli account membri dalla chiusura

Se desideri proteggere un account membro dalla chiusura accidentale, puoi creare una policy IAM per specificare quali account devono essere esclusi dalla chiusura. Gli account membri protetti attraverso queste policy non possono essere chiusi. Non è possibile utilizzare una SCP a tale scopo perché non influisce sui principali nell'account di gestione.

Puoi creare una policy IAM che impedisce la chiusura degli account in due modi:

- Elencando esplicitamente ogni account da proteggere nella policy includendo l'`arn` nell'elemento `Resource`. Per un esempio, consulta la sezione Impedire la chiusura degli account membri elencati in questa policy.
- Aggiungendo un tag ai singoli account per proteggerli dalla chiusura. Utilizza la chiave di condizione globale del tag `aws:ResourceTag` nella policy per impedire la chiusura di qualsiasi account taggato in questo modo. Per ulteriori informazioni su come taggare un account, consulta la sezione Aggiunta di tag alle risorse di Organizations. Per un esempio, consulta la sezione Impedire la chiusura di account membri con tag .

Esempio di policy IAM che impediscono la chiusura di un account membro

I seguenti esempi di codice mostrano due diversi metodi che puoi utilizzare per impedire agli account dei membri di chiudere i loro account.

Impedire la chiusura di account membri con tag

Puoi associare la seguente policy a un'identità nell'account di gestione. Questa policy impedisce ai principali nell'account di gestione di chiudere qualsiasi account membro contrassegnato con la chiave di condizione globale del tag `aws:ResourceTag`, la chiave `AccountType` e il valore di tag `Critical`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccountForTaggedAccts",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/AccountType": "Critical"}
            }
        }
    ]
}
```

Impedire la chiusura degli account membri elencati in questa policy

Puoi associare la seguente policy a un'identità nell'account di gestione. Questa policy impedisce ai principali nell'account di gestione di chiudere gli account membri esplicitamente specificati nell'elemento `Resource`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccount",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": [
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789012",
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789014"
            ]
        }
    ]
}
```

Chiusura di un account di gestione nell'organizzazione

Per chiudere l'account di gestione dell'organizzazione, è necessario innanzitutto chiudere o rimuovere tutti gli account dei membri dell'organizzazione. La chiusura dell'account di gestione comporta anche l'eliminazione dell'istanza AWS Organizations e di tutte le politiche create all'interno dell'organizzazione dopo la scadenza del periodo successivo alla chiusura.

Come chiudere un account di gestione

Utilizzare la procedura seguente per chiudere un account di gestione.

> **Important**
>
> Prima di chiudere l'account di gestione, ti consigliamo vivamente di esaminare le considerazioni e comprendere l'impatto della chiusura di un account. Per ulteriori informazioni, consulta Cosa devi sapere prima di chiudere l'account e Cosa aspettarti dopo la chiusura dell'account nella Guida alla gestione dell'AWSaccount.

AWS Management Console

Per chiudere un account di gestione dalla pagina Account

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

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 Organizationsconsole 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 indicazioni fornite Chiusura di un account membro nell'organizzazione 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, scorri fino alla fine della pagina fino alla sezione Chiudi account. Leggi e assicurati di aver 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.

AWS CLI & AWS SDKs

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

Aggiornamento dei contatti alternativi nell'organizzazione

È possibile aggiornare i contatti alternativi per gli account all'interno dell'organizzazione utilizzando la console AWS Organizations o a livello di programmazione tramite AWS CLI o gli SDK AWS. Per informazioni su come aggiornare i contatti alternativi, consultare Accesso o aggiornamento dei contatti alternativi nella Documentazione di riferimento per la gestione degli account AWS.

Aggiornamento delle informazioni di contatto principali nella tua organizzazione

È possibile aggiornare le informazioni di contatto principali per gli account all'interno della tua organizzazione utilizzando la console AWS Organizations o a livello di programmazione tramite AWS CLI o gli SDK AWS. Per informazioni su come aggiornare le informazioni di contatto principali, consulta Accesso o aggiornamento del contatto principale dell'account in AWS Riferimento per la gestione dell'account.

Aggiornamento delle Regioni AWS abilitate nell'organizzazione

Puoi aggiornare le Regioni AWS abilitate per gli account nell'organizzazione utilizzando la console AWS Organizations. Per scoprire come aggiornare le Regioni AWS abilitate, consulta Specifica delle Regioni AWS che possono essere utilizzate dall'account nella Guida di riferimento per la gestione degli account AWS.

Gestione delle policy in AWS Organizations

Le policy in AWS Organizations ti permettono di applicare ulteriori tipi di gestione agli Account AWS nella tua organizzazione. Puoi usare le policy quando tutte le caratteristiche sono abilitate nella tua organizzazione.

La console AWS Organizations visualizza lo stato abilitato o disabilitato per ogni tipo di policy. Nella scheda Organizza account, scegliere `Root` (root) nel riquadro di navigazione a sinistra. Il riquadro dei dettagli sul lato destro dello schermo mostra tutti i tipi di policy disponibili. L'elenco indica quali sono abilitate e quali disabilitate nella root dell'organizzazione. Se l'opzione per abilitare un tipo è presente, significa che quel tipo è attualmente disabilitato. Se l'opzione per disabilitare un tipo è presente, significa che quel tipo al momento è abilitato.

Tipi di policy

Organizations offre i tipi di policy nelle due categorie generali seguenti:

Policy di autorizzazione

Le policy di autorizzazione consentono di gestire centralmente la sicurezza degli Account AWS nell'organizzazione.

- Le policy di controllo dei servizi (SCP) offrono un controllo centralizzato sulle autorizzazioni massime disponibili per tutti gli account dell'organizzazione.

Policy di gestione

Le policy di gestione consentono di configurare e gestire centralmente i servizi AWS e le relative caratteristiche.

- Le Policy di rifiuto dei servizi di intelligenza artificiale (IA) consentono di controllare la raccolta dei dati per i servizi di IA di AWS per tutti gli account della tua organizzazione.
- Policy di backup consentono di gestire centralmente e applicare piani di backup alle risorse AWS negli account dell'organizzazione.
- Policy di tag consentono di standardizzare i tag collegati alle risorse AWS negli account dell'organizzazione.

La tabella riportata di seguito riepiloga alcune delle caratteristiche di ciascun tipo di policy. Per altre caratteristiche di questi tipi di policy, consulta Quote per AWS Organizations.

Tipo di policy	Influenza l'account di gestione	Numero massimo che è possibile collegare a un root, una UO o un account	Dimensione massima	Supporta la visualizzazione di policy in vigore per UO o account
SCP	 No	5	5.120 caratteri	 No
Policy di rifiuto dei servizi di IA	 Sì	5	2.500 caratteri	 Sì
Policy di backup	 Sì	10	10,000 caratteri	 Sì
Policy di tag	 Sì	10	10,000 caratteri	 Sì

Utilizzo di policy nell'organizzazione

- Abilitazione e disabilitazione di tipi di policy
- Ottenere informazioni sulle policy dell'organizzazione
- Amministratore delegato per AWS Organizations

- Policy di gestione
- Policy di controllo dei servizi (Service Control Policies, SCP)

Abilitazione e disabilitazione di tipi di policy

Abilitazione di un tipo di policy

Prima di poter creare e collegare una policy all'organizzazione, è necessario abilitare tale tipo di policy per l'utilizzo. L'abilitazione di un tipo di policy è un'attività una tantum nella directory principale dell'organizzazione. È possibile abilitare un tipo di policy solo dall'account di gestione dell'organizzazione.

> **Autorizzazioni minime**
>
> Per abilitare un tipo di policy, è necessaria l'autorizzazione per eseguire le operazioni seguenti:
>
> - `organizations:EnablePolicyType`
> - `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations
> - `organizations:ListRoots` - Obbligatorio solo quando si utilizza la console Organizations

AWS Management Console

Per abilitare un tipo di policy

1. Accedere 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. Nella pagina Policies (Policy), scegli il nome del tipo di policy da abilitare.
3. Nella pagina del tipo di policy, scegli Enable ***policy type*** (Abilita tipo di policy).

   La pagina viene sostituita da un elenco delle policy disponibili del tipo specificato.

AWS CLI & AWS SDKs

Per abilitare un tipo di policy

È possibile utilizzare uno dei comandi seguenti per abilitare un tipo di policy:

- AWS CLI: enable-policy-type

  L'esempio seguente mostra come abilitare le policy di backup per l'organizzazione. È necessario specificare l'ID della directory principale dell'organizzazione.

```
$ aws organizations enable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": [
            {
                "Type": "BACKUP_POLICY",
                "Status": "ENABLED"
            }
        ]
    }
}
```

  L'elenco di `PolicyTypes` nell'output ora include il tipo di policy specificato con lo `Status` di `ENABLED`.

- SDK AWS: EnablePolicyType

Disabilitazione di un tipo di policy

Se non desideri più utilizzare un determinato tipo di policy nell'organizzazione, puoi disabilitarlo per impedirne l'utilizzo accidentale. Puoi disabilitare un tipo di policy solo dall'account di gestione dell'organizzazione.

Important

- Quando disabiliti un tipo di policy, tutte le policy del tipo specificato vengono automaticamente distaccate da tutte le entità nella directory principale dell'organizzazione. Le policy non vengono eliminate.
- (Solo tipo di policy di controllo dei servizi) Se si abilita nuovamente il tipo di policy SCP in un secondo momento, tutte le entità nella directory principale dell'organizzazione vengono inizialmente collegate solo alla SCP `FullAWSAccess` predefinita. I collegamenti delle SCP alle entità vanno persi quando si disabilitano le SCP nell'organizzazione. Se in seguito si desidera riattivare le SCP, è necessario ricollegarle al root, alle unità organizzative e agli account dell'organizzazione, a seconda delle esigenze.

Autorizzazioni minime

Per disabilitare le policy di controllo dei servizi, è necessaria l'autorizzazione per le seguenti operazioni:

- `organizations:DisablePolicyType`
- `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations
- `organizations:ListRoots` - Obbligatorio solo quando si utilizza la console Organizations

AWS Management Console

Per disabilitare un tipo di policy

1. Accedere 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. Nella pagina Policies (Policy), scegli il nome del tipo di policy da disabilitare.
3. Nella pagina del tipo di policy, scegli Disable ***policy type*** (Disabilita tipo di policy).
4. Nella finestra di dialogo di conferma, inserisci la parola **`disable`** e quindi seleziona Disable (Disabilita).

L'elenco delle policy disponibili del tipo specificato scompare.

AWS CLI & AWS SDKs

Per disabilitare un tipo di policy

Per disabilitare un tipo di policy, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: disable-policy-type

  L'esempio seguente mostra come disabilitare le policy di backup per l'organizzazione. È necessario specificare l'ID della directory principale dell'organizzazione.

```
$ aws organizations disable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": []
    }
}
```

  L'elenco di `PolicyTypes` nell'output non include più il tipo di policy specificato.

- SDK AWS: DisablePolicyType

Ottenere informazioni sulle policy dell'organizzazione

Questa sezione descrive diversi modi per ottenere i dettagli sulle policy nella tua organizzazione. Queste procedure si applicano a tutti i tipi di policy. Devi abilitare un tipo di policy nella root dell'organizzazione prima di poter collegare policy di questo tipo a un'entità nella root dell'organizzazione.

Elenco di tutte le policy

> **Autorizzazioni minime**
>
> Per elencare le policy che si trovano nella tua organizzazione, devi disporre della seguente autorizzazione:
>
> - `organizations:ListPolicies`

È possibile visualizzare le policy nell'organizzazione nella AWS Management Console o utilizzando un comando della AWS Command Line Interface (AWS CLI) o un'operazione dell'SDK AWS.

AWS Management Console

Per elencare tutte le policy nell'organizzazione

1. Accedere 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. Nella pagina Policies (Policy), scegli la policy che desideri elencare.

   Se il tipo di policy specificato è abilitato, nella console viene visualizzato un elenco di tutte le policy di quel tipo attualmente disponibili nell'organizzazione.
3. Torna alla pagina Policies (Policy) e ripeti l'operazione per ogni tipo di policy.

AWS CLI & AWS SDKs

Per elencare tutte le policy nell'organizzazione

Per elencare le policy in un'organizzazione, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: list-policies

  Nell'esempio seguente viene illustrato come ottenere un elenco di tutte le policy di controllo dei servizi nell'organizzazione. È necessario specificare il tipo di policy che si desidera visualizzare. Ripeti il comando per ogni tipo di policy che desideri includere.

```
$ aws organizations list-policies \
```

```
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
        {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        }
    ]
}
```

- SDK AWS: ListPolicies

Elenco di tutte le policy collegate a un root, un'UO o un account

Autorizzazioni minime

Per elencare le policy collegate a un root, un'unità organizzativa (UO) o un account nella tua organizzazione, devi disporre delle autorizzazioni seguenti:

- `organizations:ListPoliciesForTarget` con un elemento `Resource` nella stessa istruzione di policy che includa l'Amazon Resource Name (ARN) del target specificato (oppure "*")

AWS Management Console

Per elencare tutte le policy collegate direttamente a un root, un'UO o un account specifici

1. Accedere 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. Nella pagina Account AWS, scegli il nome del root, dell'UO o dell'account per il quale desideri visualizzare le policy. Potrebbe essere necessario espandere le UO (scegli l'opzione ▶) per individuare quella desiderata.

3. Nella pagina del root, dell'UO o dell'account, scegli la scheda Policies (Policy).

   La scheda Policies (Policy) visualizza tutte le policy collegate al root, all'UO o all'account, raggruppate per tipo di policy.

AWS CLI & AWS SDKs

Per elencare tutte le policy collegate direttamente a un root, un'UO o un account specifici

Per elencare le policy collegate a un'entità, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: list-policies-for-target

  Nell'esempio seguente vengono elencate tutte le policy di controllo dei servizi associate all'unità organizzativa specificata. È necessario specificare sia l'ID del root, dell'unità organizzativa o dell'account, sia il tipo di policy che si desidera elencare.

```
$ aws organizations list-policies-for-target \
    --target-id ou-a1b2-f6g7h222 \
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
        {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        }
    ]
}
```

- SDK AWS: ListPoliciesForTarget

Elencazione di tutte le root, le UO e gli account ai quali è collegata una policy

Autorizzazioni minime

Per elencare le entità alle quali è collegata una policy, devi disporre della seguente autorizzazione:

- `organizations:ListTargetsForPolicy` con un elemento `Resource` nella stessa istruzione di policy che includa l'ARN della policy specificata (oppure "*")

AWS Management Console

Per elencare tutti i root, le UO e gli account ai quali è collegata una policy specifica

1. Accedere 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. Nella pagina Policies (Policy), scegli il tipo di policy e quindi il nome della policy di cui desideri esaminare i collegamenti.
3. Seleziona la scheda Targets (Destinazioni) per visualizzare una tabella di ogni root, UO e account ai quali è collegata la policy scelta.

AWS CLI & AWS SDKs

Per elencare tutti i root, le UO e gli account ai quali è collegata una policy specifica

Per elencare le entità che dispongono di una policy, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: list-targets-for-policy

Nell'esempio seguente vengono illustrati tutti i collegamenti al root, alle unità organizzative e agli account per la policy specificata.

```
$ aws organizations list-targets-for-policy \
    --policy-id p-FullAWSAccess
{
```

```
    "Targets": [
        {
            "TargetId": "ou-a1b2-f6g7h111",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
            "Name": "testou2",
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "ou-a1b2-f6g7h222",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
            "Name": "testou1",
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "123456789012",
            "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
            "Name": "My Management Account (bisdavid)",
            "Type": "ACCOUNT"
        },
        {
            "TargetId": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "Type": "ROOT"
        }
    ]
}
```

- SDK AWS: ListTargetsForPolicy

Recupero dei dettagli di una policy

Autorizzazioni minime

Per visualizzare i dettagli di una policy, devi disporre della seguente autorizzazione:

- `organizations:DescribePolicy` con un elemento `Resource` nella stessa istruzione di policy che includa l'ARN della policy specificata (oppure "*")

AWS Management Console

Per ottenere i dettagli di una policy

1. Accedere 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. Nella pagina Policies (Policy), scegli il tipo di policy e quindi il nome della policy di cui desideri esaminare i collegamenti.

   La pagina delle policy visualizza le informazioni disponibili sulla policy, inclusi l'ARN, la descrizione e i target collegati.

   - La scheda Content (Contenuti) visualizza i contenuti correnti della policy in formato JSON.
   - La scheda Targets visualizza un elenco dei root, delle UO e degli account ai quali è collegata la policy.
   - La scheda Tag mostra i tag associati alla policy. Nota: la scheda Tags (Tag) non è disponibile per le policy gestite da AWS.

   Per modificare la policy, seleziona Edit Policy (Modifica policy). Poiché ogni tipo di policy ha requisiti di modifica diversi, consulta le istruzioni per la creazione e l'aggiornamento delle policy del tipo di policy specificato.

AWS CLI & AWS SDKs

Per ottenere i dettagli di una policy

Per ottenere i dettagli di una policy, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: describe-policy

  L'esempio seguente mostra i dettagli della policy specificata.

```
$ aws organizations describe-policy \
    --policy-id p-FullAWSAccess
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-FullAWSAccess",
```

```
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        },
        "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n    {\n
      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n      \"Resource\": \"*
\"\n    }\n  ]\n}"
    }
}
```

- SDK AWS: DescribePolicy

Amministratore delegato per AWS Organizations

Consigliamo di utilizzare l'account di gestione AWS Organizations e i relativi utenti e ruoli solo per le attività che devono essere eseguite da tale account. Consigliamo anche di archiviare tutte le risorse AWS in altri account membro nell'organizzazione ed escluderle dall'account di gestione. Questo perché le funzionalità di sicurezza come le policy di controllo dei servizi (SCP) di Organizations non limitano gli utenti o i ruoli nell'account di gestione.

Dall'account di gestione dell'organizzazione, puoi delegare la gestione delle policy di Organizations per gli account membro specificati in modo da eseguire operazioni di policy che sono disponibili per impostazione predefinita solo per l'account di gestione.

Creazione o aggiornamento di una policy di delega basata sulle risorse

Dall'account di gestione, crea o aggiorna una policy di delega basata sulle risorse per la tua organizzazione e aggiungi una istruzione che specifichi quali account membri possono eseguire azioni sulle policy. Puoi aggiungere più istruzioni nella policy per indicare un diverso set di autorizzazioni per gli account membri.

> **Autorizzazioni minime**
>
> Per creare la policy di delega basata sulle risorse, sono necessarie le autorizzazioni per completare le seguenti operazioni:
>
> - `organizations:PutResourcePolicy`

- `organizations:DescribeResourcePolicy`

Inoltre, devi concedere ai ruoli e agli utenti nell'account amministratore delegato le autorizzazioni IAM corrispondenti alle azioni richieste. Senza le autorizzazioni IAM, si presume che il principale del chiamante non disponga delle autorizzazioni necessarie per gestire le policy AWS Organizations.

AWS Management Console

Aggiungi le istruzioni alla policy di delega basata sulle risorsa nella AWS Management Console utilizzando uno dei seguenti metodi:

- Policy JSON: incolla e personalizza un esempio di policy di delega basata sulle risorse da utilizzare nel tuo account o digita il tuo documento di policy JSON nell'editor JSON.
- Editor visivo: crea una nuova policy di delega nell'editor visivo che ti guidi nella creazione di una policy di delega senza dover scrivere una sintassi JSON.

Utilizzo dell'editor di policy JSON per creare o aggiornare una policy di delega

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. Seleziona Impostazioni.
3. Nella sezione Amministratore delegato per AWS Organizations, scegli Delega per creare la policy di delega di Organizations. Per aggiornare una policy di delega esistente, scegli Edit (Modifica).
4. Digitare o incollare un documento di policy JSON. Per dettagli sul linguaggio della policy IAM, consulta la Documentazione di riferimento delle policy JSON IAM.
5. Risolvi eventuali avvisi di sicurezza, errori o avvisi generali generati durante la convalida delle policy, quindi scegli Create policy (Crea policy) per salvare il lavoro.

Utilizzo dell'editor visivo per creare o aggiornare una policy di delega

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. Seleziona Impostazioni.
3. Nella sezione Amministratore delegato per AWS Organizations, scegli Delega per creare la policy di delega di Organizations. Per aggiornare una policy di delega esistente, scegli Edit (Modifica).
4. Nella pagina Create Delegation policy (Crea politica di delega), scegli Add new statement (Aggiungi nuova istruzione).
5. Imposta Effect (Effetto) su `Allow`.
6. Aggiungi `Principal` per definire gli account dei membri a cui desideri delegare. Per informazioni dettagliate sulla sintassi, consulta gli Policy di delega basate sulle risorse di esempio.
7. Dall'elenco di operazioni, scegli le operazioni che desideri delegare. Puoi utilizzare il campo Filter actions (Filtra operazioni) per limitare le scelte.
8. Per specificare se l'account del membro delegato può collegare policy alla root dell'organizzazione o alle unità organizzative (UO), imposta `Resources`. Dovrai inoltre selezionare `policy` come tipo di risorsa. Per ulteriori dettagli, consulta gli Policy di delega basate sulle risorse di esempio. È possibile specificare le risorse nei seguenti modi:
   - Scegli Add a resource (Aggiungi una risorsa) e crea il nome della risorsa Amazon (ARN) seguendo le istruzioni nella finestra di dialogo.
   - Elenca gli ARN delle risorse manualmente nell'editor. Per maggiori informazioni sulla sintassi dell'ARN, consulta Nome della risorsa Amazon (ARN) nella Guida di riferimento generale per AWS. Per informazioni sull'utilizzo di ARN nell'elemento di risorse di una policy, consulta Elementi di policy JSON di IAM: risorsa.
9. Scegli Add a condition (Aggiungi una condizione) per specificare altre condizioni, incluso il tipo di policy che desideri delegare. Scegli la chiave di condizione, la chiave di tag, il qualificatore e l'operatore, quindi digita un **`Value`**. Per ulteriori dettagli, vedere Policy di delega basate sulle risorse di esempio. Una volta terminato, scegli Add condition (Aggiungi condizione). Per ulteriori informazioni sull'elemento Condition, consulta Elementi della policy JSON IAM: Condition nella Documentazione di riferimento delle policy JSON IAM.

10. Per aggiungere più blocchi di autorizzazioni, consulta Add new statement (Aggiungi nuova istruzione). Per ogni blocco, ripetere i passaggi da 5 a 9.
11. Risolvi eventuali avvisi di sicurezza, errori o avvisi generali generati durante la convalida delle policy, quindi scegli Create policy (Crea policy) per salvare il lavoro.

AWS CLI & AWS SDKs

Creazione o aggiornamento di una policy di delega

Per creare o aggiornare una policy di delega, puoi utilizzare il seguente comando:

- AWS CLI: put-resource-policy

  Nell'esempio seguente viene creata o aggiornata la policy di delega.

```
$ aws organizations put-resource-policy --content
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Fully_manage_backup_policies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "135791357913"
            }
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:CreatePolicy",
                "organizations:DescribePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
                "organizations:AttachPolicy",
                "organizations:DetachPolicy"
            ],
            "Resource": [
                "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
                "arn:aws:organizations::246802468024:ou/o-abcdef/*",
                "arn:aws:organizations::246802468024:account/o-abcdef/*",
                "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
            ],
```

```
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [
                        "BACKUP_POLICY"
                    ]
                }
            }
        }
    ]
}
```

- SDK AWS: PutResourcePolicy

Operazioni di policy di delega supportate

Le seguenti operazioni sono supportate per la policy di delega:

- `AttachPolicy`
- `CreatePolicy`
- `DeletePolicy`
- `DescribeAccount`
- `DescribeCreateAccountStatus`
- `DescribeEffectivePolicy`
- `DescribeHandshake`
- `DescribeOrganization`
- `DescribeOrganizationalUnit`
- `DescribePolicy`
- `DescribeResourcePolicy`
- `DetachPolicy`
- `DisablePolicyType`
- `EnablePolicyType`
- `ListAccounts`
- `ListAccountsForParent`
- `ListAWSServiceAccessForOrganization`

- `ListChildren`
- `ListCreateAccountStatus`
- `ListDelegatedAdministrators`
- `ListDelegatedServicesForAccount`
- `ListHandshakesForAccount`
- `ListHandshakesForOrganization`
- `ListOrganizationalUnitsForParent`
- `ListParents`
- `ListPolicies`
- `ListPoliciesForTarget`
- `ListRoots`
- `ListTagsForResource`
- `ListTargetsForPolicy`
- `TagResource`
- `UntagResource`
- `UpdatePolicy`

Visualizzazione di una policy di delega basata sulle risorse

Dall'account di gestione, visualizza la policy di delega basata sulle risorse dell'organizzazione per capire quali amministratori delegati hanno accesso per gestire quali tipi di policy.

> **Autorizzazioni minime**
>
> Per visualizzare la policy di delega basata sulle risorse, sono necessarie le autorizzazioni per eseguire l'operazione seguente: `organizations:DescribeResourcePolicy`.

AWS Management Console

Visualizzazione di una policy di delega

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. Seleziona Impostazioni.
3. Nella sezione Amministratore delegato per AWS Organizations, scorri per visualizzare la policy di delega completa.

AWS CLI & AWS SDKs

Visualizzazione di una policy di delega

Per visualizzare una policy di delega, puoi utilizzare il seguente comando:

- AWS CLI: describe-resource-policy

  Nell'esempio seguente viene richiamata la policy.

  ```
  $ aws organizations describe-resource-policy
  ```

- SDK AWS: DescribeResourcePolicy

Eliminazione di una policy di delega basata sulle risorse

Quando non è più necessario delegare la gestione delle policy nell'organizzazione, è possibile eliminare la policy di delega basata sulle risorse dall'account di gestione dell'organizzazione.

> **Important**
>
> Se elimini una policy di delega basata sulle risorse, non potrai più ripristinarla.

> **Autorizzazioni minime**
>
> Per eliminare la policy di delega basata sulle risorse, sono necessarie le autorizzazioni per eseguire l'operazione seguente: `organizations:DeleteResourcePolicy`.

AWS Management Console

Eliminazione di una policy di delega

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. Seleziona Impostazioni.
3. Nella sezione Amministratore delegato per AWS Organizations, scegli Elimina.
4. Nella finestra di dialogo di conferma Delete policy, digita **`delete`**. Quindi, scegli Delete policy (Elimina policy).

AWS CLI & AWS SDKs

Eliminazione di una policy di delega

Per eliminare una policy di delega, puoi utilizzare il seguente comando:

- AWS CLI: delete-resource-policy

  Nell'esempio seguente la policy viene eliminata.

  ```
  $ aws organizations delete-resource-policy
  ```

- SDK AWS: DeleteResourcePolicy

Policy di delega basate sulle risorse di esempio

I seguenti esempi di codice mostrano come è possibile utilizzare le policy di delega basate sulle risorse.

Examples (Esempi)

- Esempio: visualizzazione dell'organizzazione, delle unità organizzative, degli account e delle policy
- Esempio: autorizzazioni consolidate per gestire le policy di backup di un'organizzazione

Esempio: visualizzazione dell'organizzazione, delle unità organizzative, degli account e delle policy

Prima di delegare la gestione delle policy, è necessario delegare le autorizzazioni per navigare nella struttura di un'organizzazione e visualizzare le unità organizzative (UO), gli account e le policy ad essi collegate.

Questo esempio mostra come potresti includere queste autorizzazioni nella tua policy di delega basata sulle risorse per l'account membro, *AccountId*.

> **Important**
>
> È consigliabile includere le autorizzazioni solo per le operazioni minime richieste, come mostrato nell'esempio, sebbene sia possibile delegare qualsiasi operazione di sola lettura di Organizations utilizzando questa policy.

Questa policy di delega di esempio concede le autorizzazioni necessarie per completare le operazioni a livello di programmazione dall'API AWS o dalla AWS CLI. Per utilizzare questa policy di delega, sostituisci il testo del segnaposto di AWS per *AccountId* con le tue informazioni. Quindi, segui le indicazioni in Amministratore delegato per AWS Organizations.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
```

```
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

Esempio: autorizzazioni consolidate per gestire le policy di backup di un'organizzazione

Questo esempio mostra come è possibile creare una policy di delega basata sulle risorse che consenta all'account di gestione di delegare le autorizzazioni complete necessarie per gestire le policy di backup all'interno dell'organizzazione, tra cui le operazioni `create`, `read`, `update` e `delete`, così come le operazioni di policy `attach` e `detach`. Per comprendere il significato di ogni operazione, risorsa e condizione, consulta Policy di delega basate sulle risorse di esempio.

> **Important**
>
> Questa policy consente agli amministratori delegati di eseguire le operazioni specificate sulle policy create da qualsiasi account dell'organizzazione, incluso l'account di gestione.

Questa policy di delega di esempio concede le autorizzazioni necessarie per completare le operazioni a livello di programmazione dall'API AWS o dalla AWS CLI. Per utilizzare questa policy di delega, sostituisci il testo del segnaposto AWSper *`MemberAccountId`*, *`ManagementAccountId`*, *`OrganizationId`* e *`RootId`* con le tue informazioni. Quindi, segui le indicazioni in Amministratore delegato per AWS Organizations.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
          "organizations:PolicyType": "BACKUP_POLICY"
        }
      }
    },
    {
      "Sid": "DelegatingAllActionsForBackupPolicies",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
```

```
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource": [
        "arn:aws:organizations::ManagementAccountId:root/o-OrganizationId/r-RootId",
        "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
backup_policy/*"
      ]
    }
  ]
}
```

Policy di gestione

Le policy di gestione consentono di configurare e gestire centralmente i servizi AWS e le relative caratteristiche. Il modo esatto in cui le policy influiscono sulle unità organizzative e sugli account che le ereditano dipende dal tipo di policy di gestione applicato in AWS Organizations. Consulta gli argomenti di questa sezione per saperne di più sui termini e sui concetti pertinenti relativi alle policy di gestione.

Argomenti

- Comprendere l'ereditarietà delle policy di gestione
- Policy di rifiuto dei servizi di IA
- Policy di backup
- Policy di tag

Comprendere l'ereditarietà delle policy di gestione

> **Note**
>
> Le informazioni contenute in questa sezione non si applicano alle SCP perché le SCP gestiscono sia l'autorizzazione che il rifiuto delle operazioni IAM. Sebbene le SCP siano collegate alla radice, alle unità organizzative (UO) e agli account, l'autorizzazione delle operazioni richiede una istruzione `allow` esplicita nelle SCP a ogni livello, dalla radice a ciascuna unità organizzativa nel percorso diretto verso l'account (incluso l'account di

destinazione stesso). Per ulteriori informazioni su come le SCP funzionano in una gerarchia AWS Organizations, consulta Valutazione SCP.

Puoi collegare le policy di gestione alle entità dell'organizzazione, ovvero root dell'organizzazione, unità organizzativa (UO) o account, all'interno dell'organizzazione:

- Quando colleghi una policy di gestione alla root dell'organizzazione, tutte le unità organizzative e gli account dell'organizzazione ereditano tale policy.
- Quando colleghi una policy di gestione a un'unità organizzativa specifica, gli account che si trovano direttamente sotto tale unità organizzativa o qualsiasi unità organizzativa figlio ereditano la policy.
- Quando colleghi una policy di gestione a un account specifico, essa influisce solo su tale account.

Poiché è possibile associare policy di gestione a più livelli nell'organizzazione, gli account possono ereditare più policy.

In questa sezione viene illustrato come le policy padre e le policy figlio vengono elaborate nella policy operativa di un account.

Argomenti

Terminologia dell'ereditarietà

Quando si discute dell'ereditarietà delle policy di gestione, in questo argomento vengono utilizzati i termini seguenti.

Ereditarietà delle policy

> Interazione dei criteri a diversi livelli di un'organizzazione, passando dalla root di livello superiore dell'organizzazione e procedendo verso il basso attraverso la gerarchia delle unità organizzative (OU) fino ai singoli account.

È possibile associare delle policy alla root dell'organizzazione, alle unità organizzative, ai singoli account e a qualsiasi combinazione di queste entità dell'organizzazione. L'ereditarietà delle policy si riferisce alle policy di gestione collegate alla root dell'organizzazione o a un'unità organizzativa. Tutti gli account che appartengono alla root dell'organizzazione o all'unità organizzativa a cui è collegata una policy di gestione ereditano tale policy.

Ad esempio, quando le policy di gestione sono collegate alla root dell'organizzazione, tale policy viene ereditata da tutti gli account dell'organizzazione. Questo perché tutti gli account di un'organizzazione si trovano sempre sotto la root dell'organizzazione. Quando associ una policy a un'unità organizzativa specifica, gli account direttamente sotto l'unità organizzativa o qualsiasi unità organizzativa figlio ereditano tale policy. Poiché è possibile collegare le policy a più livelli nell'organizzazione, gli account potrebbero ereditare più documenti di policy per un singolo tipo di policy.

Policy padre

Nell'albero dell'organizzazione sono le policy collegate a un livello più alto rispetto alle policy collegate alle entità inferiori dell'albero.

Ad esempio, se colleghi la policy di gestione A alla root dell'organizzazione, parliamo semplicemente di una policy. Se a un'unità organizzativa sotto tale root associ anche la policy B, la policy A è la policy padre della policy B. La policy B è la policy figlio della policy A. La policy A e la policy B si uniscono per creare la policy di tag operativa per gli account nell'unità organizzativa.

Policy figlio

Nell'albero dell'organizzazione sono le policy collegate a un livello inferiore rispetto alla policy padre.

Policy operative

Il singolo documento di policy finale che specifica le regole applicabili a un account. La policy operativa è l'aggregazione di tutte le policy ereditate dall'account, oltre a qualsiasi policy collegata direttamente all'account. Ad esempio, le policy di tag consentono di visualizzare la policy di tag operativa applicabile a qualsiasi account. Per ulteriori informazioni, consulta Visualizzazione delle policy di tag operative.

Operatori di ereditarietà

Operatori che controllano il modo in cui le policy ereditate si uniscono in un'unica policy operativa. Questi operatori costituiscono una funzionalità avanzata. Gli autori di policy esperti possono

utilizzarli per limitare le modifiche apportate da una policy figlio e la modalità di unione delle impostazioni nelle policy. Per ulteriori informazioni, consulta Operatori di ereditarietà.

Sintassi della policy ed ereditarietà per i tipi di policy di gestione

Il modo esatto in cui le policy influiscono sulle unità organizzative e sugli account che le ereditano dipende dal tipo di policy di gestione scelto. I tipi di policy di gestione includono:

- Policy di rifiuto dei servizi di Intelligenza Artificiale (IA)
- Policy di backup
- Policy di tag

La sintassi per questo tipo di policy di gestione include Operatori di ereditarietà, che consentono di specificare con granularità fine quali elementi delle policy padre vengono applicati e quali elementi possono essere sovrascritti o modificati quando vengono ereditati dalle unità organizzative figlio e dagli account.

La policy operativa è l'insieme di regole ereditate dalla root dell'organizzazione e dalle unità organizzative insieme a quelle direttamente associate all'account. La policy effettiva specifica l'insieme finale di regole applicabili all'account. Puoi visualizzare la policy operativa per un account, che include l'effetto di tutti gli operatori di ereditarietà nelle policy applicate. Per ulteriori informazioni, consulta Visualizzazione delle policy di tag operative.

Operatori di ereditarietà

Gli operatori di ereditarietà controllano il modo in cui le policy ereditate e le policy dell'account si uniscono nella policy operativa dell'account. Tali operatori comprendono gli operatori di impostazione del valore e gli operatori del controllo degli elementi figlio.

Quando si utilizza l'editor visivo nella console AWS Organizations, è possibile usare solo l'operatore `@@assign`. Altri operatori costituiscono una funzionalità avanzata. Per utilizzare gli altri operatori, è necessario creare manualmente la policy JSON. Gli autori esperti di policy possono utilizzare gli operatori di ereditarietà per controllare quali valori vengono applicati alla policy operativa e limitare le modifiche che le policy figlio possono apportare.

Operatori di impostazione del valore

È possibile utilizzare gli operatori di impostazione del valore per controllare il modo in cui la policy interagisce con le policy padre:

- `@@assign` - Sovrascrive le impostazioni delle policy ereditate con le impostazioni specificate. Se l'impostazione specificata non è ereditata, questo operatore la aggiunge alla policy operativa. Questo operatore può essere applicato a un'impostazione di policy di qualsiasi tipo.
  - Per le impostazioni a valore singolo, questo operatore sostituisce il valore ereditato con il valore specificato.
  - Per le impostazioni con più valori (array JSON), questo operatore rimuove eventuali valori ereditati e li sostituisce con i valori specificati da questa policy.
- `@@append` - Aggiunge le impostazioni specificate (senza rimuoverne nessuna) a quelle ereditate. Se l'impostazione specificata non è ereditata, questo operatore la aggiunge alla policy operativa. Puoi utilizzare questo operatore solo con impostazioni con più valori.
  - Questo operatore aggiunge i valori specificati a qualsiasi valore nell'array ereditato.
- `@@remove` - Rimuove le impostazioni ereditate specificate dalla policy effettiva, se esistono. Puoi utilizzare questo operatore solo con impostazioni con più valori.
  - Questo operatore rimuove solo i valori specificati dall'array di valori ereditati dalle policy padre. Altri valori possono continuare a esistere nell'array e possono essere ereditati dalle policy figlio.

Operatori di controllo figlio

L'utilizzo degli operatori di controllo figlio è facoltativo. È possibile utilizzare l'operatore `@@operators_allowed_for_child_policies` per controllare quali operatori di impostazione del valore possono utilizzare le policy di tag figlio. Puoi consentire tutti gli operatori, alcuni operatori specifici o nessun operatore. Per impostazione predefinita, tutti gli operatori (`@@all`) sono consentiti.

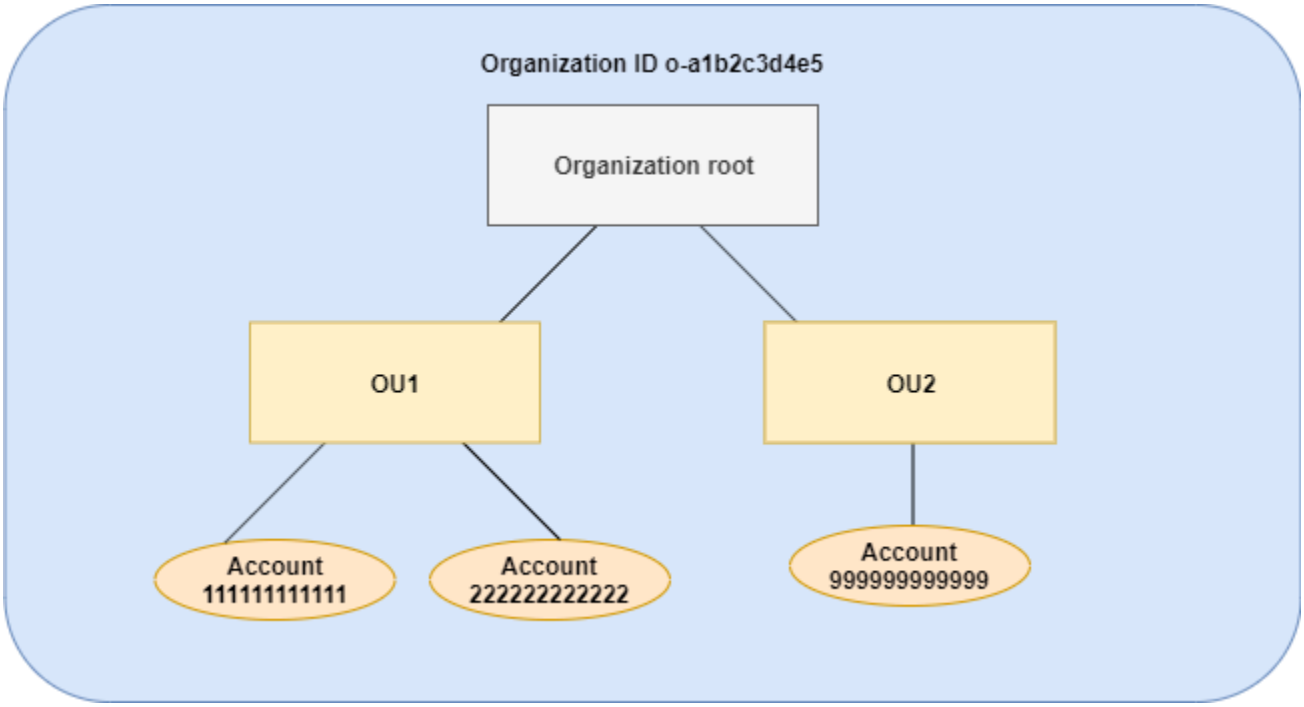
- `"@@operators_allowed_for_child_policies":["@@all"]` - Le unità organizzative e gli account figli possono usare qualsiasi operatore nelle policy. Per impostazione predefinita, tutti gli operatori sono consentiti nelle policy figlio.
- `"@@operators_allowed_for_child_policies":["@@assign", "@@append", "@@remove"]` - Le unità organizzative e gli account figli possono usare solo gli operatori specificati nelle policy figlio. Puoi specificare uno o più operatori di impostazione del valore in questo operatore di controllo figlio.
- `"@@operators_allowed_for_child_policies":["@@none"]` - Le unità organizzative e gli account figli non possono usare operatori nelle policy. Puoi utilizzare questo operatore per bloccare efficacemente i valori definiti in una policy padre in modo che le policy figlio non possano aggiungere, integrare o rimuovere tali valori.

> **Note**
>
> Se un operatore di controllo figlio ereditato limita l'utilizzo di un operatore, non è possibile invertire tale regola in una policy figlio. Se includi operatori di controllo figlio in una policy padre, essi limitano gli operatori di impostazione del valore in tutti le policy figlio.

Esempi di ereditarietà

Questi esempi mostrano come funziona l'ereditarietà della policy mostrando come le policy di tag padre e figlio vengono unite in una policy di tag operativa di un account.

Gli esempi presuppongono che la struttura dell'organizzazione sia quella mostrata nel diagramma seguente.



Esempi

- Esempio 1: consente alle policy figlio di sovrascrivere solo i valori dei tag
- Esempio 2: aggiungere nuovi valori ai tag ereditati
- Esempio 3: rimuovere i valori dai tag ereditati
- Esempio 4: limitare le modifiche alle policy figlio
- Esempio 5: conflitti con gli operatori di controllo figlio

- Esempio 6: conflitti con l'aggiunta di valori allo stesso livello di gerarchia

Esempio 1: consente alle policy figlio di sovrascrivere solo i valori dei tag

La seguente policy di tag definisce la chiave di tag `CostCenter` e due valori ammissibili, `Development` e `Support`. Se la si collega alla radice dell'organizzazione, la policy di tag è attiva per tutti gli account dell'organizzazione.

Policy A – Policy di tag del root dell'organizzazione

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

Supponi che gli utenti nell'unità organizzativa OU1 utilizzino un valore di tag diverso per una chiave e che tu voglia applicare la policy di tag per tipi di risorse specifici. Poiché la policy A non specifica quali operatori di controllo figlio sono consentiti, tutti gli operatori sono consentiti. Puoi utilizzare l'operatore `@@assign` e creare una policy di tag come la seguente da collegare a OU1.

Policy B – Policy di tag dell'unità organizzativa 1

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Sandbox"
```

```
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

Specificando l'operatore `@@assign` per il tag, quando la policy A e la policy B si uniscono per formare la policy di tag operativa per un account:

- La policy B sovrascrive i due valori di tag specificati nella policy padre, la policy A. Il risultato è che `Sandbox` è l'unico valore ammissibile per la chiave di tag `CostCenter`.
- L'aggiunta di `enforced_for` specifica che il tag `CostCenter` deve essere il valore di tag specificato su tutte le risorse Amazon Redshift e le tabelle Amazon DynamoDB.

Come illustrato nel diagramma, OU1 comprende due account: 111111111111 e 222222222222.

Policy di tag operativa risultante per gli account 111111111111 e 222222222222.

> **Note**
>
> Non è possibile utilizzare direttamente il contenuto di una policy effettiva visualizzata come contenuto di una nuova policy. La sintassi non include gli operatori necessari per controllare l'unione con altre policy figlie e padri. La presentazione della policy efficace serve unicamente per comprendere i risultati della fusione.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Sandbox"
            ],
            "enforced_for": [
```

```
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

Esempio 2: aggiungere nuovi valori ai tag ereditati

In alcuni casi si desidera che tutti gli account dell'organizzazione specifichino una chiave di tag con un breve elenco di valori accettabili. Per gli account di un'unità organizzativa, puoi consentire un valore aggiuntivo che solo tali account possono specificare durante la creazione di risorse. Questo esempio specifica come eseguire questa operazione utilizzando l'operatore `@@append`. L'operatore `@@append` è una caratteristica avanzata.

Come l'esempio 1, questo esempio inizia con la policy A per la policy del tag root dell'organizzazione.

Policy A – Policy di tag del root dell'organizzazione

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

In questo esempio, colleghi la policy C a OU2. La differenza in questo esempio consiste nel fatto che l'utilizzo dell'operatore `@@append` nella policy C aggiunge, anziché sovrascrivere, l'elenco dei valori accettabili e la regola `enforced_for`.

Policy C – Policy di tag dell'unità organizzativa 2 per l'aggiunta di valori

```
{
```

```
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@append": [
                    "Marketing"
                ]
            },
            "enforced_for": {
                "@@append": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

Il collegamento della policy C a OU2 ha i seguenti effetti quando le policy A e C si uniscono per formare la policy tag operativa di un account:

- Poiché la policy C include l'operatore `@@append`, consente di aggiungere, non sovrascrivere, l'elenco dei valori di tag accettabili specificati nella policy A.
- Come nella policy B, l'aggiunta di `enforced_for` specifica che il tag `CostCenter` deve essere utilizzato come valore di tag specificato su tutte le risorse Amazon Redshift e le tabelle Amazon DynamoDB. La sovrascrittura (`@@assign`) e l'aggiunta (`@@append`) hanno lo stesso effetto se la policy padre non include un operatore di controllo figlio che limita ciò che una policy figlio può specificare.

Come mostrato nel diagramma, OU2 include un account: 999999999999. Le policy A e C si uniscono per creare la policy di tag operativa per l'account 999999999999.

Policy di tag operativa per l'account 999999999999

> **Note**
>
> Non è possibile utilizzare direttamente il contenuto di una policy effettiva visualizzata come contenuto di una nuova policy. La sintassi non include gli operatori necessari per controllare

l'unione con altre policy figlie e padri. La presentazione della policy efficace serve unicamente per comprendere i risultati della fusione.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Development",
                "Support",
                "Marketing"
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

Esempio 3: rimuovere i valori dai tag ereditati

In alcuni casi, la policy di tag collegata all'organizzazione definisce più valori di tag di quelli che si desidera vengano utilizzati da un account. In questo esempio viene illustrato come modificare una policy di tag utilizzando l'operatore `@@remove`. `@@remove` è una caratteristica avanzata.

Come gli altri esempi, anche questo esempio inizia con la policy A per la policy di tag root dell'organizzazione.

Policy A – Policy di tag del root dell'organizzazione

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
```

```
                ]
            }
        }
    }
}
```

In questo esempio, collega la policy D all'account 999999999999.

Policy D – Policy di tag dell'account 999999999999 per la rimozione divalori

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@remove": [
                    "Development",
                    "Marketing"
                ],
                "enforced_for": {
                    "@@remove": [
                        "redshift:*",
                        "dynamodb:table"
                    ]
                }
            }
        }
    }
}
```

L'associazione della policy D all'account 999999999999 ha i seguenti effetti quando le policy A, C e D si uniscono per formare la policy di tag operativa:

- Supponendo che siano stati eseguiti tutti gli esempi precedenti, le policy B, C e C sono policy figlio di A. La policy B è solo collegata all'unità organizzativa 1, quindi non ha alcun effetto sull'account 9999999999999.
- Per l'account 9999999999999, l'unico valore accettabile per la chiave di tag `CostCenter` è `Support`.
- La conformità non viene applicata per la chiave di tag `CostCenter`.

Nuova policy di tag operativa per l'account 999999999999

> **Note**
>
> Non è possibile utilizzare direttamente il contenuto di una policy effettiva visualizzata come contenuto di una nuova policy. La sintassi non include gli operatori necessari per controllare l'unione con altre policy figlie e padri. La presentazione della policy efficace serve unicamente per comprendere i risultati della fusione.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Support"
            ]
        }
    }
}
```

Se in seguito aggiungi altri account a OU2, le policy di tag operative sarebbero diverse da quelle dell'account 999999999999. Questo perché la policy D più restrittiva è collegata solo a livello di account e non all'unità organizzativa.

Esempio 4: limitare le modifiche alle policy figlio

Ci possono essere casi in cui vuoi limitare le modifiche nelle policy figlio. Questo esempio spiega come eseguire questa operazione utilizzando gli operatori di controllo figlio.

Questo esempio inizia con una nuova policy di tag root dell'organizzazione e presuppone che le policy di tag non siano ancora collegate alle entità dell'organizzazione.

Policy E - Policy di tag root dell'organizzazione per limitare le modifiche nelle policy figlio

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": ["@@none"],
```

```
                "@@assign": "Project"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance",
                    "Escalations"
                ]
            }
        }
    }
}
```

Quando associ la policy E alla root dell'organizzazione, questa impedisce alle policy figlio di modificare la chiave del tag `Project`. Tuttavia, le policy figlio possono sovrascrivere o aggiungere valori di tag.

Supponi quindi di associare la seguente policy F a un'unità organizzativa.

Policy F – Policy di tag dell'unità organizzativa

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": [
                    "Escalations - research"
                ]
            }
        }
    }
}
```

L'unione della policy E e della policy F ha i seguenti effetti sugli account dell'unità organizzativa:

- La policy F è una policy figlio per la policy E.
- La policy F tenta di cambiare il trattamento lettere maiuscole o minuscole, ma non può. Questo perché la policy E include l'operatore `"@@operators_allowed_for_child_policies": ["@@none"]` per la chiave di tag.

- Tuttavia, la policy F può aggiungere valori di tag per la chiave. Questo perché la policy E include `"@@operators_allowed_for_child_policies": ["@@append"]` per il valore del tag.

Policy operativa per gli account nell'unità organizzativa

> **Note**
>
> Non è possibile utilizzare direttamente il contenuto di una policy effettiva visualizzata come contenuto di una nuova policy. La sintassi non include gli operatori necessari per controllare l'unione con altre policy figlie e padri. La presentazione della policy efficace serve unicamente per comprendere i risultati della fusione.

```
{
    "tags": {
        "project": {
            "tag_key": "Project",
            "tag_value": [
                "Maintenance",
                "Escalations",
                "Escalations - research"
            ]
        }
    }
}
```

Esempio 5: conflitti con gli operatori di controllo figlio

Gli operatori di controllo figlio possono esistere nelle policy di tag collegate allo stesso livello nella gerarchia organizzativa. In questo caso, l'intersezione degli operatori consentiti viene utilizzata quando le policy si uniscono per formare la policy operativa per gli account.

Supponi che le policy G e H siano collegate alla root dell'organizzazione.

Policy G – Policy di tag del root dell'organizzazione 1

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
```

```
                "@@assign": [
                    "Maintenance"
                ]
            }
        }
    }
}
```

Policy H – Policy di tag del root dell'organizzazione 2

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append", "@@remove"]
            }
        }
    }
}
```

In questo esempio, una policy nella root dell'organizzazione definisce che i valori per la chiave di tag possono solo essere aggiunti. L'altra policy collegata alla root dell'organizzazione consente alle policy figlio di aggiungere e rimuovere valori. L'intersezione di queste due autorizzazioni viene utilizzata per le policy figlio. Il risultato è che le policy figlio possono aggiungere valori, ma non rimuovere valori. Pertanto, la policy figlio può aggiungere un valore all'elenco dei valori di tag, ma non può rimuovere il valore `Maintenance`.

Esempio 6: conflitti con l'aggiunta di valori allo stesso livello di gerarchia

Puoi collegare più policy di tag a ciascuna entità dell'organizzazione. Quando si esegue questa operazione, le policy di tag collegate alla stessa entità dell'organizzazione possono includere informazioni in conflitto. Le policy vengono valutate in base all'ordine in cui sono state associate all'entità dell'organizzazione. Per modificare l'ordine di valutazione delle policy, puoi scollegare e ricollegare una policy.

Supponi che la policy J sia collegata alla root dell'organizzazione e che poi la policy K venga collegata alla root dell'organizzazione.

Policy J – Prima policy di tag collegata al root dell'organizzazione

```
{
    "tags": {
```

```
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": ["Maintenance"]
            }
        }
    }
}
```

Policy K – Seconda policy di tag collegata al root dell'organizzazione

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "project"
            }
        }
    }
}
```

In questo esempio, la chiave di tag `PROJECT` viene utilizzata nella policy di tag operativa perché la policy che l'ha definita è stata collegata per prima alla root dell'organizzazione.

Policy JK – Policy di tag effettiva per l'account

La policy operativa per l'account è la seguente.

> **Note**
>
> Non è possibile utilizzare direttamente il contenuto di una policy effettiva visualizzata come contenuto di una nuova policy. La sintassi non include gli operatori necessari per controllare l'unione con altre policy figlie e padri. La presentazione della policy efficace serve unicamente per comprendere i risultati della fusione.

```
{
    "tags": {
        "project": {
```

```
            "tag_key": "PROJECT",
            "tag_value": [
                "Maintenance"
            ]
        }
    }
}
```

Policy di rifiuto dei servizi di IA

I servizi di intelligenza artificiale (IA) di AWS, tra cui Amazon Rekognition, Amazon CodeWhisperer, Amazon Transcribe e Contact Lens per Amazon Connect, potrebbero archiviare e utilizzare i contenuti dei clienti elaborati in vista dello sviluppo e del miglioramento continuo di altri servizi AWS. Come cliente AWS, è possibile decidere di rinunciare all'archiviazione e all'utilizzo dei tuoi contenuti per migliorare il servizio.

> **Note**
>
> I servizi di intelligenza artificiale (IA) di AWS potrebbero dover archiviare i contenuti dell'utente per fornire i servizi, anche se l'utente non vuole che AWS utilizzi i suoi dati per migliorare i servizi. Per ulteriori informazioni, consulta la documentazione relativa al servizio IA che utilizzi.

Invece di configurare questa impostazione singolarmente per ogni Account AWS utilizzato dall'organizzazione, è possibile configurare una policy dell'organizzazione che applichi le impostazioni desiderate a tutti gli account membri dell'organizzazione. Puoi scegliere di rifiutare l'archiviazione e l'utilizzo dei contenuti per un singolo servizio di IA o per tutti i servizi coperti contemporaneamente. È possibile eseguire una query sulla policy effettiva applicabile a ciascun account per visualizzare gli effetti delle scelte di impostazione.

> **Important**
>
> - Quando specifichi una preferenza di accettazione o rifiuto per un servizio, tale impostazione è globale e viene applicata a tutte le Regioni AWS. L'impostazione del valore da una Regione AWS si replica in tutte le altre Regioni.
> - Quando rifiuti l'utilizzo del contenuto da parte di un servizio di IA di AWS, tale servizio elimina tutto il contenuto cronologico associato che è stato condiviso con AWS prima di

impostare l'opzione. Questa eliminazione dovrebbe essere limitata ai dati archiviati che non sono necessari per fornire funzioni di servizio.

Guida introduttiva alle policy di rifiuto dei servizi di IA

Attieniti alla seguente procedura per iniziare a utilizzare le policy di rifiuto dei servizi di intelligenza artificiale (IA).

1. Abilita le policy di rifiuto dei servizi di IA per l'organizzazione.
2. Crea una policy di rifiuto dei servizi di IA.
3. Collega la policy di rifiuto dei servizi di IA al root, all'unità organizzativa o all'account dell'organizzazione.
4. Visualizza la policy di rifiuto dei servizi di IA effettiva combinata applicabile a un account.

Per tutte queste fasi, è possibile accedere come utente AWS Identity and Access Management (IAM), assumere un ruolo IAM o accedere come utente root (scelta non consigliata) nell'account di gestione dell'organizzazione.

Altre informazioni

- Scopri la sintassi delle policy per le policy di rifiuto dei servizi di IA e consulta esempi di policy

Creazione, aggiornamento ed eliminazione delle policy di rifiuto dei servizi di IA

In questo argomento:

- Dopo avere abilitato le policy di rifiuto dei servizi di IA per l'organizzazione, puoi creare una policy.
- Quando i requisiti di rifiuto cambiano, puoi aggiornare una policy esistente.
- Quando una policy non è più necessaria, dopo averla scollegata da tutte le unità organizzative (UO) e da tutti gli account la puoi eliminare.

Creazione di una policy di rifiuto dei servizi di IA

Autorizzazioni minime

Per creare una policy di rifiuto dei servizi di IA, è necessaria l'autorizzazione per eseguire l'operazione seguente:

- `organizations:CreatePolicy`

AWS Management Console

Per creare una policy di rifiuto dei servizi di IA

1. Accedere 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. Nella pagina AI services opt-out policies (Policy di rifiuto dei servizi di IA), scegli Create policy (Crea policy).
3. Nella pagina Create new AI services opt-out policy (Crea nuova policy di rifiuto dei servizi di IA, inserisci un Nome policy e facoltativamente una Descrizione per la policy.
4. (Facoltativo) Per aggiungere uno o più tag alla policy, scegli Add tag (Aggiungi tag) e quindi inserisci una chiave e un valore facoltativo. Lasciando vuoto il valore, questo viene impostato su una stringa vuota; non è `null`. Puoi associare fino a 50 tag a una policy. Per ulteriori informazioni, consultare Tagging delle risorse AWS Organizations.
5. Inserisci o incolla il testo della policy nella scheda JSON. Per informazioni sulla sintassi della policy di rifiuto dei servizi di IA, consulta Sintassi ed esempi di policy di rifiuto dei servizi di IA. Per esempi di policy che puoi utilizzare come punto di partenza, consulta Esempi di policy di rifiuto dei servizi di IA.
6. Al termine delle modifica della policy, seleziona Create policy (Crea policy nell'angolo in basso a destra della pagina.

AWS CLI & AWS SDKs

Per creare una policy di rifiuto dei servizi di IA

Puoi utilizzare una delle seguenti opzioni per creare una policy di tag:

- AWS CLI: create-policy

1. Crea una policy di rifiuto dei servizi di IA come la seguente e archiviala in un file di testo. Nota: "`optOut`" e "`optIn`" fanno distinzione tra lettere maiuscole e minuscole.

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

   Questa policy di rifiuto dei servizi di IA specifica che tutti gli account interessati dalla policy sono esclusi da tutti i servizi di IA, ad eccezione di Amazon Rekognition.

2. Importa il file di policy JSON per creare una nuova policy nell'organizzazione. In questo esempio, il file JSON precedente è stato denominato `policy.json`.

```
$ aws organizations create-policy \
    --type AISERVICES_OPT_OUT_POLICY \
    --name "MyTestPolicy" \
    --description "My test policy" \
    --content file://policy.json
{
    "Policy": {
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":{\"@@assign
\":\"optOut\"}},\"rekognition\":{\"opt_out_policy\":{\"@@assign\":\"optIn
\"}}}}",
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5"
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Description": "My test policy",
            "Name": "MyTestPolicy",
            "Type": "AISERVICES_OPT_OUT_POLICY"
```

```
        }
    }
}
```

- SDK AWS: CreatePolicy

Cosa fare in seguito

Dopo avere creato una policy di rifiuto dei servizi di IA, puoi applicare le scelte di rifiuto. A tale scopo, puoi collegare la policy al root dell'organizzazione, alle unità organizzative, agli Account AWS all'interno dell'organizzazione o a una combinazione di tutte queste entità.

Aggiornamento di una policy di rifiuto dei servizi di IA

> **Autorizzazioni minime**
>
> Per aggiornare una policy di rifiuto dei servizi di IA, è necessario disporre dell'autorizzazione per le seguenti operazioni:
>
> - `organizations:UpdatePolicy` con un elemento `Resource` nella stessa istruzione di policy che includa l'ARN della policy specificata (oppure "*")
> - `organizations:DescribePolicy` con un elemento `Resource` nella stessa istruzione di policy che includa l'Amazon Resource Name (ARN) della policy specificata (oppure "*")

AWS Management Console

Per aggiornare una policy di rifiuto dei servizi di IA

1. Accedere 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. Nella pagina AI services opt-out policies (Policy di rifiuto dei servizi di IA), scegli il nome della policy che vuoi aggiornare.
3. Nella pagina dei dettagli della policy, seleziona Edit policy (Modifica policy).
4. È possibile inserire un nuovo Policy name (Nome policy), una nuova Policy description (Descrizione della policy) o modificare il testo della policy JSON. Per informazioni sulla sintassi della policy di rifiuto dei servizi di IA, consulta Sintassi ed esempi di policy di rifiuto

dei servizi di IA. Per esempi di policy che puoi utilizzare come punto di partenza, consulta Esempi di policy di rifiuto dei servizi di IA.

5. Al termine dell'aggiornamento della policy, scegliere Salva modifiche.

AWS CLI & AWS SDKs

Per aggiornare una policy

Per aggiornare una policy, puoi utilizzare una delle seguenti opzioni:

- AWS CLI: update-policy

Nell'esempio seguente viene rinominata una policy di rifiuto dei servizi di IA.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

Nell'esempio seguente viene aggiunta o modificata la descrizione di una policy di rifiuto dei servizi di IA.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
```

```
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

Nell'esempio seguente viene modificato il documento della policy JSON collegato a una policy di rifiuto dei servizi di IA. In questo esempio, il contenuto viene preso da un file denominato `policy.json` con il testo seguente:

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
```

```
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
         "Content": "{\n\"services\": {\n\"default\": {\n\"   ....TRUNCATED FOR
 BREVITY....    ": \"optIn\"\n}\n}\n}\n}\n"}
}
```

- SDK AWS: UpdatePolicy

Modifica dei tag collegati a una policy di rifiuto dei servizi di IA

Quando effettui l'accesso all'account di gestione della tua organizzazione, puoi aggiungere o rimuovere i tag associati a una policy di rifiuto dei servizi di IA. Per ulteriori informazioni sul tagging, consultare Tagging delle risorse AWS Organizations.

Autorizzazioni minime

Per modificare i tag associati a una policy di rifiuto dei servizi di IA nella tua organizzazione AWS, è necessario disporre delle seguenti autorizzazioni:

- `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations
- `organizations:DescribePolicy` - Obbligatorio solo quando si utilizza la console Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Per modificare i tag collegati a una policy di rifiuto dei servizi di IA

1. Accedere 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. Nella pagina AI services opt-out policies (Policy di rifiuto dei servizi di IA), scegli il nome della policy con i tag che vuoi modificare.
3. Nella pagina dei dettagli della policy, scegli la scheda Tags, quindi scegli Manage tags (Gestisci tag).
4. In questa pagina puoi eseguire le seguenti operazioni:
   - Modifica il valore di un tag inserendo un nuovo valore rispetto a quello precedente. Non è possibile modificare la chiave. Per cambiare una chiave, devi eliminare il tag con la vecchia chiave e aggiungere un tag con la nuova chiave.
   - Rimuovi eventuali tag esistenti scegliendo Remove (Rimuovi).
   - Aggiungi una nuova coppia chiave e valore di tag. Scegli Add tag (Aggiungi tag), quindi inserisci il nuovo nome della chiave e il valore facoltativo nelle caselle fornite. Se lasci vuota la casella Value (Valore), il valore è una stringa vuota; non è `null`.
5. Scegli Save changes (Salva le modifiche) dopo avere apportato tutte le aggiunte, le rimozioni e le modifiche opportune.

AWS CLI & AWS SDKs

Per modificare i tag collegati a una policy di rifiuto dei servizi di IA

Per modificare i tag collegati a una policy di rifiuto dei servizi di IA puoi utilizzare uno dei seguenti comandi:

- AWS CLI: tag-resource e untag-resource
- SDK AWS: TagResource e UntagResource

Eliminazione di una policy di rifiuto dei servizi di IA

Quando effettui l'accesso all'account di gestione della tua organizzazione, puoi eliminare una policy di cui non hai più bisogno nella tua organizzazione.

Prima di poter eliminare una policy, devi distaccarla da tutte le entità collegate.

> **Autorizzazioni minime**
>
> Per eliminare una policy, è necessaria l'autorizzazione per la seguente operazione:
>
> - `organizations:DescribePolicy` (solo console - per passare alla policy)
> - `organizations:DeletePolicy`

AWS Management Console

Per eliminare una policy di rifiuto dei servizi di IA

1. Accedere 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. Nella pagina AI services opt-out policies (Policy di rifiuto dei servizi di IA), scegli il nome della policy che vuoi eliminare.
3. È necessario che la policy da scollegare venga prima eliminata da tutti i root, le UO e gli account. Seleziona la scheda Targets (Destinazioni), scegli il pulsante di opzione accanto a ciascun root, UO o account visualizzato nell'elenco Targets e scegli Detach (Scollega). Nella finestra di dialogo di conferma, scegli Detach (Scollega). Ripeti finché non hai rimosso tutti i target.
4. Nella parte superiore della pagina, seleziona Delete (Elimina).
5. Nella finestra di dialogo di conferma, inserisci il nome della policy, quindi scegli Delete (Elimina).

AWS CLI & AWS SDKs

Per eliminare una policy di rifiuto dei servizi di IA

Per eliminare una policy, puoi utilizzare una delle seguenti opzioni:

- AWS CLI: delete-policy

  Nell'esempio seguente viene eliminata la policy specificata. Funziona solo se la policy non è collegata a un root, un'UO o un account.

```
$ aws organizations delete-policy \
    --policy-id p-i9j8k7l6m5
```

Questo comando non produce alcun output se ha esito positivo.

- SDK AWS: DeletePolicy

Collegamento e scollegamento delle policy di rifiuto dei servizi di IA

Puoi utilizzare le policy di rifiuto dei servizi di intelligenza artificiale (IA) su un'intera organizzazione, sulle unità organizzative e sui singoli account. L'ambito di applicazione della policy di rifiuto dei servizi di IA dipende dall'elemento dell'organizzazione a cui lo si collega:

- Quando colleghi una policy di rifiuto dei servizi di IA al root dell'organizzazione, la policy si applica a tutte le unità organizzative e agli account membri del root.
- Quando colleghi una policy di rifiuto dei servizi di IA a un'unità organizzativa, tale policy si applica agli account appartenenti all'unità organizzativa o a una qualsiasi delle unità organizzative figlie. Questi account sono soggetti anche a qualsiasi policy collegata alla root dell'organizzazione.
- Quando colleghi una policy di rifiuto dei servizi di IA a un account, tale policy si applica solo a tale account. L'account è inoltre soggetto a qualsiasi policy collegata alla root dell'organizzazione e a qualsiasi unità organizzativa a cui appartiene l'account.

L'aggregazione di eventuali policy di rifiuto dei servizi di IA che l'account eredita dal root e dalle unità organizzative padre, nonché le eventuali policy collegate direttamente all'account, formano la policy effettiva. Per informazioni sull'unione delle policy alla policy effettiva, consulta Comprendere l'ereditarietà delle policy di gestione.

> **Autorizzazioni minime**
>
> Per collegare le policy di rifiuto dei servizi di IA, è necessario disporre dell'autorizzazione per le seguenti operazioni:
>
> - `organizations:AttachPolicy`

AWS Management Console

Per collegare una policy di rifiuto dei servizi di IA, puoi accedere alla policy oppure al root, all'unità organizzativa o all'account a cui vuoi collegare la policy.

Per collegare una policy di rifiuto dei servizi di IA passando dal root, dall'unità organizzativa o dall'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. Nella pagina Account AWS, individua e scegli il nome del root, dell'unità organizzativa o dell'account a cui desideri collegare una policy. Potrebbe essere necessario espandere le UO (scegli l'opzione ▶) per individuare l'UO o l'account desiderato.
3. Nella scheda Policies (Policy), alla voce per AI service opt-out policies (Policy di rifiuto dei servizi di IA), scegli Attach (Collega).
4. Individua la policy desiderata e scegli Attach policy (Collega policy).

   L'elenco delle policy di rifiuto dei servizi di IA collegate nella scheda Policies (Policy) viene aggiornato per includere la nuova aggiunta. La modifica della policy diventa immediatamente effettiva.

Per collegare una policy di rifiuto dei servizi di IA passando dalla policy

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. Nella pagina AI services opt-out policies (Policy di rifiuto dei servizi di IA), scegli il nome della policy che vuoi collegare.
3. Nella scheda Targets (Destinazioni), scegli Attach (Collega).
4. Scegli il pulsante di opzione accanto al root, all'unità organizzativa o all'account a cui vuoi collegare la policy. Potrebbe essere necessario espandere le UO (scegli l'opzione ▶) per individuare l'UO o l'account desiderato.
5. Scegli Attach policy (Collega policy).

L'elenco delle policy di rifiuto dei servizi di IA collegate nella scheda Targets (Destinazioni) viene aggiornato per includere la nuova aggiunta. La modifica della policy diventa immediatamente effettiva.

AWS CLI & AWS SDKs

Per collegare la policy di rifiuto dei servizi di IA al root, all'unità organizzativa o all'account dell'organizzazione.

Per collegare una policy di rifiuto dei servizi di IA puoi utilizzare uno dei seguenti comandi:

- AWS CLI: attach-policy

  Nell'esempio seguente una policy viene collegata a un'UO.

  ```
  $ aws organizations attach-policy \
      --target-id ou-a1b2-f6g7h222 \
      --policy-id p-i9j8k7l6m5
  ```

  Questo comando non produce alcun output se ha esito positivo.
- SDK AWS: AttachPolicy

La modifica della policy diventa immediatamente effettiva.

Scollegamento di una policy di rifiuto dei servizi di IA

Quando effettui l'accesso all'account di gestione della tua organizzazione, puoi scollegare una policy dal root, dall'unità organizzativa o dall'account a cui è collegata. Dopo avere scollegato una policy di rifiuto dei servizi di IA da un'entità, quella policy non si applica più ad alcun account interessato in precedenza dall'entità ora scollegata. Per distaccare una policy, completa le fasi seguenti.

Autorizzazioni minime

Per scollegare una policy di rifiuto dei servizi di IA dalla root dell'organizzazione, dall'unità organizzativa o dall'account, è necessaria l'autorizzazione per la seguente operazione:

- `organizations:DetachPolicy`

AWS Management Console

Per scollegare una policy di rifiuto dei servizi di IA, puoi accedere alla policy oppure al root, all'unità organizzativa o all'account da cui vuoi scollegare la policy.

Per scollegare una policy di rifiuto dei servizi di IA passando dal root, dall'unità organizzativa o dall'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. Nella pagina Account AWS individua il root, l'unità organizzativa o l'account da cui desideri scollegare una policy. Potrebbe essere necessario espandere le UO (scegli l'opzione ▶) per individuare l'UO o l'account desiderato. Scegli il nome del root, dell'unità organizzativa o dell'account.
3. Nella scheda Policies (Policy), scegli il pulsante di opzione accanto alla policy di rifiuto dei servizi di IA che desideri scollegare, quindi scegli Detach (Scollega).
4. Nella finestra di dialogo di conferma, scegli Detach policy (Scollega policy).

   L'elenco delle policy di rifiuto dei servizi di IA collegate viene aggiornato. La modifica della policy diventa immediatamente effettiva.

Per scollegare una policy di rifiuto dei servizi di IA passando dalla policy

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. Nella pagina AI services opt-out policies (Policy di rifiuto dei servizi di IA), scegli il nome della policy che vuoi scollegare da un root, un'UO o un account.
3. Nella scheda Targets (Destinazioni), scegli il pulsante di opzione accanto al root, all'unità organizzativa o all'account da cui vuoi scollegare la policy. Potrebbe essere necessario espandere le UO (scegli l'opzione ▶) per individuare l'UO o l'account desiderato.
4. Seleziona Detach (Scollega).
5. Nella finestra di dialogo di conferma, scegli Detach (Scollega).

L'elenco delle policy di rifiuto dei servizi di IA collegate viene aggiornato. La modifica della policy diventa immediatamente effettiva.

AWS CLI & AWS SDKs

Per scollegare la policy di rifiuto dei servizi di IA dal root, dall'unità organizzativa o dall'account dell'organizzazione.

Per scollegare una policy di rifiuto dei servizi di IA puoi utilizzare una delle seguenti opzioni:

- AWS CLI: detach-policy

  Nell'esempio seguente, una policy viene scollegata da un'unità organizzativa.

  ```
  $ aws organizations detach-policy \
      --target-id ou-a1b2-f6g7h222 \
      --policy-id p-i9j8k7l6m5
  ```

  Questo comando non produce alcun output se ha esito positivo.
- SDK AWS: DetachPolicy

La modifica della policy diventa immediatamente effettiva.

Visualizzazione delle policy di rifiuto dei servizi di IA effettivi

Determina la policy di rifiuto dei servizi di intelligenza artificiale (IA) per un account nell'organizzazione.

Qual è la policy di rifiuto dei servizi di IA effettiva?

La policy di rifiuto dei servizi di IA effettiva specifica le regole finali che si applicano a un Account AWS. Si tratta dell'aggregazione di tutte le policy di rifiuto dei servizi di IA ereditate dall'account e di qualsiasi policy di rifiuto dei servizi di IA direttamente collegata all'account. Quando colleghi una policy di rifiuto dei servizi di IA al root dell'organizzazione, questa si applica a tutti gli account dell'organizzazione. Quando colleghi una policy di rifiuto dei servizi di IA a un'unità organizzativa, questa si applica a tutti gli account e alle unità organizzative appartenenti all'unità organizzativa. Quando colleghi una policy direttamente a un account, questa si applica solo a tale Account AWS.

Ad esempio, la policy di rifiuto dei servizi di IA collegata al root dell'organizzazione potrebbe specificare che tutti gli account dell'organizzazione si oppongono all'utilizzo dei contenuti da parte di tutti i servizi di machine learning di AWS. Una policy separata di rifiuto dei servizi di IA collegata direttamente a un account membro specifica che consente di utilizzare il contenuto solo per Amazon Rekognition. La combinazione di queste policy di rifiuto dei servizi di IA costituisce la policy di rifiuto dei servizi di IA effettiva. Il risultato è che tutti gli account dell'organizzazione rifiutano tutti i servizi di AWS, ad eccezione di un account che sceglie di accettare Amazon Rekognition.

Per informazioni su come le policy vengono combinate nella policy effettiva finale, consulta Comprendere l'ereditarietà delle policy di gestione.

Come visualizzare la policy di rifiuto dei servizi di IA effettiva

Puoi visualizzare la policy di rifiuto dei servizi di IA effettiva per un account dalla AWS Management Console, dall'API AWS o l'AWS Command Line Interface.

> **Autorizzazioni minime**
>
> Per visualizzare la policy di rifiuto dei servizi di IA effettiva per un account, è necessario disporre dell'autorizzazione per le seguenti operazioni:
>
> - `organizations:DescribeEffectivePolicy`
> - `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations

AWS Management Console

Per visualizzare la policy di rifiuto dei servizi di IA effettiva per un 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. Nella pagina Account AWS, scegli il nome dell'account per il quale desideri visualizzare la policy di rifiuto dei servizi di IA effettiva. Potrebbe essere necessario espandere le UO (scegli l'opzione ▶) per individuare l'account desiderato.

3. Nella scheda Policies (Policy), nella sezione AI services opt-out policies (policy di rifiuto dei servizi di IA), scegli View the effective AI policy for this (Visualizza la policy di rifiuto dei servizi di IA effettiva per questo) Account AWS.

   Nella console viene visualizzata la policy effettiva applicata all'account specificato.

   > **Note**
   >
   > Non è possibile copiare e incollare una policy effettiva e utilizzarla come JSON per un'altra policy di rifiuto dei servizi di IA senza modifiche significative. I documenti della policy di rifiuto dei servizi di IA devono includere gli operatori di ereditarietà che specificano la modalità di unione di ciascuna impostazione nella policy effettiva finale.

AWS CLI & AWS SDKs

Per visualizzare la policy di rifiuto dei servizi di IA effettiva per un account

Puoi utilizzare una delle seguenti opzioni per visualizzare la policy di rifiuto dei servizi di IA effettiva:

- AWS CLI: describe-effective-policy

  Nell'esempio seguente viene illustrata la policy di rifiuto dei servizi di IA effettiva per un account.

```
$ aws organizations describe-effective-policy \
    --policy-type AISERVICES_OPT_OUT_POLICY \
    --target-id 123456789012
{
    "EffectivePolicy": {
        "PolicyContent": "{\"services\":{\"comprehend\":{\"opt_out_policy\":
\"optOut\"},   ....TRUNCATED FOR BREVITY....   "opt_out_policy\":\"optIn\"}}}",
        "LastUpdatedTimestamp": "2020-12-09T12:58:53.548000-08:00",
        "TargetId": "123456789012",
        "PolicyType": "AISERVICES_OPT_OUT_POLICY"
    }
}
```

- SDK AWS: DescribeEffectivePolicy

Sintassi ed esempi di policy di rifiuto dei servizi di IA

In questo argomento viene descritta la sintassi delle policy di rifiuto dei servizi di intelligenza artificiale (IA) e vengono forniti esempi.

Sintassi per le policy di rifiuto dei servizi di IA

Una policy di rifiuto dei servizi di IA è un file di testo normale strutturato in base alle regole di JSON. La sintassi per le policy di rifiuto dei servizi di IA segue la sintassi per tutti i tipi di policy di gestione. Per una discussione completa di tale sintassi, consulta Comprendere l'ereditarietà delle policy di gestione. Questo argomento è incentrato sull'applicazione della sintassi generale ai requisiti specifici del tipo di policy di rifiuto dei servizi di IA.

> **Important**
>
> L'uso di minuscole e maiuscole dei valori trattati in questa sezione è importante. Inserisci i valori con lettere maiuscole e minuscole come illustrato in questo argomento. Le policy non funzionano se si utilizzano maiuscole e minuscole impreviste.

La policy seguente mostra la sintassi delle policy di rifiuto dei servizi di IA di base. Se questo esempio fosse stato applicato direttamente a un account, tale account avrebbe esplicitamente rifiutato un servizio e accettato un altro servizio. Altri servizi possono essere accettati o rifiutati dalle policy ereditate da livelli superiori (policy di UO o root).

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

Immagina la seguente policy di esempio collegata al root dell'organizzazione. Imposta il rifiuto di tutti i servizi di IA come impostazione predefinita per l'organizzazione. Ciò include automaticamente tutti i servizi di IA non altrimenti esplicitamente esclusi, inclusi i servizi di IA che AWS potrebbe implementare in futuro. Puoi collegare policy figlie alle unità organizzative o direttamente agli account per ignorare questa impostazione per qualsiasi servizio di IA ad eccezione di Amazon Comprehend. La seconda voce dell'esempio seguente utilizza `@@operators_allowed_for_child_policies` impostato su `none` per evitare che venga sovrascritto. La terza voce nell'esempio imposta un'esenzione a livello di organizzazione per Amazon Rekognition. La policy accetta il servizio per tutta l'organizzazione, ma consente alle policy figlie di ignorarla se appropriato.

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

La sintassi della policy di rifiuto dei servizi di IA include i seguenti elementi:

- L'elemento `services`. Una policy di rifiuto dei servizi di IA è identificato da questo nome fisso come elemento contenente JSON più esterno.

  Una policy di rifiuto dei servizi di IA può avere una o più istruzioni sotto l'elemento `services`. Ogni istruzione contiene i seguenti elementi:

  - Una chiave del nome del servizio che identifica un servizio di IA di AWS. I seguenti nomi di chiave sono i valori validi per questo campo:

- **`default`** - Rappresenta tutti i servizi di IA attualmente disponibili e include implicitamente e automaticamente tutti i servizi di IA che potrebbero essere aggiunti in futuro.
- `awssupplychain`
- `chimesdkvoiceanalytics`
- `cloudwatch`
- `codeguruprofiler`
- `codewhisperer`
- `comprehend`
- `connectamd`
- `connectoptimization`
- `contactlens`
- `datazone`
- `frauddetector`
- `guardduty`
- `lex`
- `polly`
- `q`
- `quicksightq`
- `rekognition`
- `securitylake`
- `textract`
- `transcribe`
- `translate`

Ogni istruzione di policy identificata da una chiave di nome servizio può contenere i seguenti elementi:

- La chiave `opt_out_policy`. Questa chiave deve essere presente. Questa è l'unica chiave che puoi inserire sotto una chiave di nome del servizio.

  La chiave `opt_out_policy` può contenere solo l'operatore `@@assign` con uno dei seguenti valori:

  - `optOut` - Scegli di rifiutare l'utilizzo del contenuto per il servizio di IA specificato.

- `optIn` - Scegli di accettare l'utilizzo del contenuto per il servizio di IA specificato.

> **Note**
>
> - Non è possibile utilizzare gli operatori di ereditarietà `@@append` e `@@remove` nelle policy di rifiuto dei servizi di IA.
> - Non è possibile utilizzare l'operatore `@@enforced_for` nelle policy di rifiuto dei servizi di IA.

- A qualsiasi livello, è possibile specificare l'operatore `@@operators_allowed_for_child_policies` per controllare che cosa possono fare le policy figlie per sovrascrivere le impostazioni imposte dalle policy padre. È possibile specificare uno dei seguenti valori:
  - `@@assign` - Le policy figlie di questa policy possono utilizzare l'operatore `@@assign` per sovrascrivere il valore ereditato con un valore diverso.
  - `@@none` - Le policy figlie di questa policy non possono modificare il valore.

  Il comportamento di `@@operators_allowed_for_child_policies` dipende da dove lo posizioni. Puoi utilizzare le posizioni seguenti:
  - Sotto la chiave `services` - Controlla se una policy figlia può integrare o modificare l'elenco dei servizi nella policy effettiva.
  - Sotto la chiave per un servizio di IA specifico o la chiave `default` - Controlla se una policy figlia può integrare o modificare l'elenco di chiavi in questa voce specifica.
  - Sotto la chiave `opt_out_policies` per un servizio specifico - Controlla se una policy figlia può modificare soltanto le impostazioni di questo servizio specifico.

Esempi di policy di rifiuto dei servizi di IA

Le policy di esempio che seguono sono solo a scopo informativo.

Esempio 1: disattivazione di tutti i servizi di IA per tutti gli account dell'organizzazione

Nell'esempio seguente viene illustrata una policy che è possibile collegare alla directory principale dell'organizzazione per disattivare i servizi di IA per gli account dell'organizzazione.

> **Tip**
>
> Se copi l'esempio seguente utilizzando il pulsante Copia nell'angolo superiore destro dell'esempio, la copia non include i numeri di riga. È pronta per essere incollata.

```
    | {
    |     "services": {
[1] |         "@@operators_allowed_for_child_policies": ["@@none"],
    |         "default": {
[2] |             "@@operators_allowed_for_child_policies": ["@@none"],
    |             "opt_out_policy": {
[3] |                 "@@operators_allowed_for_child_policies": ["@@none"],
    |                 "@@assign": "optOut"
    |             }
    |         }
    |     }
    | }
```

- [1] - `"@@operators_allowed_for_child_policies": ["@@none"]` in `services` impedisce alle policy figlie di aggiungere nuove sezioni per i servizi individuali diverse dalla sezione `default` già presente. `Default` è il segnaposto che rappresenta "tutti i servizi di IA".
- [2] - `"@@operators_allowed_for_child_policies": ["@@none"]` in `default` impedisce alle policy figlie di aggiungere nuove sezioni diverse dalla sezione `opt_out_policy` già presente.
- [3] - `"@@operators_allowed_for_child_policies": ["@@none"]` in `opt_out_policy` impedisce alle policy figlie di modificare il valore dell'impostazione di `optOut` o di aggiungere ulteriori impostazioni.

Esempio 2: creazione di un'impostazione predefinita dell'organizzazione per tutti i servizi, consentendo alle policy figlie di ignorare l'impostazione per i singoli servizi

La policy di esempio seguente imposta un valore predefinito a livello di organizzazione per tutti i servizi di IA. Il valore per `default` impedisce a una policy figlia di modificare il valore `optOut` per il servizio `default`, il segnaposto per tutti i servizi di IA. Se questa policy viene applicata come policy padre collegandola al root o a un'unità organizzativa, le policy figlie possono comunque modificare l'impostazione di rifiuto dei singoli servizi, come illustrato nella seconda policy.

- Perché non è presente `"@@operators_allowed_for_child_policies": ["@@none"]` sotto la chiave `services`, le policy figlie possono aggiungere nuove sezioni per i singoli servizi.
- `"@@operators_allowed_for_child_policies": ["@@none"]` in `default` impedisce alle policy figlie di aggiungere nuove sezioni diverse dalla sezione `opt_out_policy` già presente.
- `"@@operators_allowed_for_child_policies": ["@@none"]` in `opt_out_policy` impedisce alle policy figlie di modificare il valore dell'impostazione di `optOut` o di aggiungere ulteriori impostazioni.

Policy padre di rifiuto esplicito dei servizi di IA per l'utente root dell'organizzazione

```
{
    "services": {
        "default": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        }
    }
}
```

La seguente policy di esempio presuppone che la policy dell'esempio precedente sia collegata al root dell'organizzazione o a un'unità organizzativa padre e che questo esempio venga collegato a un account interessato dalla policy padre. Sovrascrive l'impostazione di rifiuto di default e sceglie esplicitamente solo il servizio Amazon Lex.

Policy figlia di rifiuto esplicito dei servizi di IA - Intelligenza Artificiale

```
{
    "services": {
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

La policy effettiva risultante per l'Account AWS è che l'account accetta solo il servizio Amazon Lex e rifiuta tutti gli altri servizi di IA di AWS a causa dell'impostazione di rifiuto `default` ereditata dalla policy padre.

Esempio 3: definizione di una policy di disattivazione dei servizi di IA a livello di organizzazione per un singolo servizio

Nell'esempio seguente viene illustrata una policy di rifiuto dei servizi di IA che definisce un'impostazione `optOut` per un singolo servizio di IA. Se questa policy è collegata al root dell'organizzazione, impedisce a qualsiasi policy figlia di sovrascrivere l'impostazione `optOut` per questo servizio. Altri servizi non sono trattati da questa policy, ma potrebbero essere influenzati dalle policy figlie in altre unità organizzative o account.

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

Policy di backup

AWS Backup consente di creare piani di backup che definiscono le modalità di backup delle risorse AWS. Le regole nel piano includono diverse impostazioni, ad esempio la frequenza di backup, la finestra temporale durante la quale si verifica il backup, la Regione AWS contenente le risorse di cui eseguire il backup e il vault in cui archiviare il backup. Puoi quindi applicare un piano di backup a gruppi di risorse AWS identificati utilizzando i tag. Devi inoltre identificare un ruolo AWS Identity and Access Management (IAM) che concede a AWS Backup l'autorizzazione per eseguire l'operazione di backup per tuo conto.

Le policy di backup AWS Organizations combinano tutti questi elementi in documenti di testo JSON. Puoi collegare una policy di backup a qualsiasi elemento nella struttura dell'organizzazione, ad esempio il root, le unità organizzative e i singoli account. Organizations applica le regole di ereditarietà per combinare le policy nel root dell'organizzazione, eventuali unità organizzative padre o collegate all'account. Ciò si traduce in una policy di backup effettiva per ogni account. Questa policy effettiva indica a AWS Backup come eseguire automaticamente il backup delle risorse AWS.

Le policy di backup offrono un controllo granulare sul backup delle risorse a qualsiasi livello richiesto dall'organizzazione. Ad esempio, in una policy collegata al root dell'organizzazione puoi specificare che è necessario eseguire il backup di tutte le tabelle Amazon DynamoDB. Tale policy può includere una frequenza di backup predefinita. Puoi quindi collegare una policy di backup alle unità organizzative che sovrascrivono la frequenza di backup in base ai requisiti di ciascuna unità organizzativa. Ad esempio, l'unità organizzativa `Developers` potrebbe specificare una frequenza di backup di una volta alla settimana, mentre l'unità organizzativa `Production` specifica una frequenza di una volta al giorno.

Puoi creare policy di backup parziali che includano singolarmente solo una parte delle informazioni necessarie per eseguire correttamente il backup delle risorse. Puoi collegare queste policy a diverse parti della struttura dell'organizzazione, ad esempio il root o un'unità organizzativa padre, con l'intenzione di ereditare tali policy parziali dalle unità organizzative e dagli account di livello inferiore. Quando Organizations combina tutte le policy per un account utilizzando le regole di ereditarietà, la policy effettiva risultante deve disporre di tutti gli elementi richiesti. In caso contrario, AWS Backup considera la policy non valida e non esegue il backup delle risorse interessate.

> **Important**
>
> AWS Backup può eseguire un backup solo quando viene richiamato da una policy effettiva completa che dispone di tutti gli elementi richiesti.
> Sebbene una strategia di policy parziale descritta in precedenza possa funzionare, se una policy effettiva per un account risulta incompleta, si generano errori o risorse di cui non viene eseguito il backup. Come strategia alternativa, si consiglia di richiedere che tutti le policy di backup siano complete e convalidate autonomamente. Utilizza i valori predefiniti forniti dalle policy collegate più in alto nella gerarchia e sostituirli dove necessario nelle policy figlio includendo gli operatori di controllo figlio di ereditarietà.

Il piano di backup effettivo per ogni Account AWS dell'organizzazione viene visualizzato nella console AWS Backup come un piano immutabile per tale account. Puoi visualizzarlo, ma non modificarlo.

Quando AWS Backup avvia un backup basato su un piano di backup creato dalla policy, puoi visualizzare lo stato del processo di backup nella console AWS Backup. Un utente di un account membro può visualizzare lo stato e gli eventuali errori relativi ai processi di backup in tale account membro. Se abiliti anche l'accesso al servizio attendibile con AWS Backup, un utente nell'account di gestione dell'organizzazione può visualizzare lo stato e gli errori di tutti i processi di backup

nell'organizzazione. Per ulteriori informazioni, consulta Abilitazione della gestione di più account nella Guida per gli sviluppatori di AWS Backup.

Nozioni di base sulle policy di backup

Segui queste fasi per iniziare a utilizzare le policy di backup.

1. Ulteriori informazioni sulle autorizzazioni necessarie per eseguire attività delle policy di backup
2. Ulteriori informazioni su alcune best practice consigliate per l'utilizzo delle policy di backup.
3. Abilitare le policy di backup per l'organizzazione.
4. Creare una policy di backup.
5. Collegare la policy di backup alla root dell'organizzazione, all'unità organizzativa o all'account.
6. Visualizzare la policy di backup effettiva combinata applicabile a un account.

Per tutte queste fasi, è possibile accedere come utente IAM, assumere un ruolo IAM o accedere come utente root (scelta non consigliata) nell'account di gestione dell'organizzazione.

Altre informazioni

- Ulteriori informazioni sulla sintassi delle policy di backup e policy di esempio

Prerequisiti e autorizzazioni per la gestione delle policy di backup

In questa pagina vengono descritti i prerequisiti e le autorizzazioni richieste per la gestione delle policy di backup in AWS Organizations.

Argomenti

- Prerequisiti per la gestione delle policy di backup
- Autorizzazioni per la gestione delle policy di backup

Prerequisiti per la gestione delle policy di backup

Per gestire le policy di backup in un'organizzazione è necessario quanto segue:

- L'organizzazione deve avere tutte le caratteristiche abilitate.
- È necessario accedere all'account di gestione dell'organizzazione.

- L'utente o il ruolo AWS Identity and Access Management (IAM) richiede le autorizzazioni elencate nella sezione seguente.

Autorizzazioni per la gestione delle policy di backup

La policy IAM di esempio seguente fornisce le autorizzazioni per gestire tutti gli aspetti delle policy di backup in un'organizzazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageBackupPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:DetachPolicy",
                "organizations:DisableAWSServiceAccess",
                "organizations:DisablePolicyType",
                "organizations:EnableAWSServiceAccess",
                "organizations:EnablePolicyType",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListCreateAccountStatus",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:ListTargetsForPolicy",
                "organizations:UpdatePolicy"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Per ulteriori informazioni su policy e autorizzazioni IAM, consulta la Guida per l'utente di IAM.

Best practice per l'utilizzo delle policy di backup

AWS consiglia le seguenti best practice per l'utilizzo delle policy di backup:

Scelta di una strategia delle policy di backup

Puoi creare policy di backup in parti incomplete che vengono ereditate e unite per creare una policy completa per ogni account membro. In questo caso, se si apporta una modifica a un livello senza considerare attentamente l'impatto di tale modifica su tutti gli account al di sotto di tale livello c'è il rischio di ottenere una policy effettiva incompleta. Per evitare ciò, consigliamo di verificare che le policy di backup implementate a tutti i livelli siano complete autonomamente. Considera le policy padre come policy predefinite che possono essere sovrascritte dalle impostazioni specificate nelle policy figlie. In questo modo, anche se non esiste una policy figlio, la policy ereditata è completa e utilizza i valori predefiniti. Puoi controllare quali impostazioni possono essere aggiunte, modificate o rimosse da policy figlio utilizzando gli operatori di ereditarietà del controllo figlio.

Convalida delle modifiche al controllo delle policy di backup mediante **`GetEffectivePolicy`**

Dopo aver apportato una modifica a una policy di backup, controllare le policy effettive per gli account rappresentativi al di sotto del livello in cui è stata apportata la modifica. È possibile visualizzare la policy effettiva utilizzando la AWS Management Console o mediante l'operazione API GetEffectivePolicy o una delle relative varianti della AWS CLI o dell'SDK AWS. Assicurati che l'impatto della modifica apportata sulla policy effettiva sia quello previsto.

Iniziare semplicemente e apportare piccole modifiche

Per semplificare il debug, inizia con policy semplici e apporta modifiche un elemento alla volta. Convalida il comportamento e l'impatto di ogni modifica prima di apportare la modifica successiva. Questo approccio riduce il numero di variabili da tenere in considerazione quando si verifica un errore o un risultato imprevisto.

Memorizzare copie dei backup in altre Regioni AWS e account nell'organizzazione

Per migliorare la posizione di disaster recovery, è possibile archiviare copie dei backup.

- Una Regione diversa - Se si memorizzano copie del backup in Regioni AWS aggiuntive, è possibile proteggere il backup contro il danneggiamento accidentale o l'eliminazione nella Regione originale.

Utilizza la sezione `copy_actions` della policy per specificare un vault in una o più Regioni dello stesso account in cui viene eseguito il piano di backup. A tale scopo, identifica l'account utilizzando la variabile `$account` quando specifichi l'ARN del vault di backup in cui archiviare la copia del backup. La variabile `$account` viene automaticamente sostituita in fase di esecuzione con l'ID account in cui è in esecuzione la policy di backup.

- Un account diverso - Se memorizzi copie del backup in Account AWS, aggiungi una barriera di sicurezza che aiuta a proteggerti dall'eventualità che un soggetto malintenzionato possa compromettere uno dei tuoi account. Utilizza la sezione `copy_actions` della policy per specificare un vault in uno o più account dell'organizzazione, separati dall'account in cui viene eseguito il piano di backup. A tale scopo, identifica l'account utilizzando il numero ID account effettivo quando specifichi l'ARN del vault di backup in cui archiviare la copia del backup.

Limitare il numero di piani per policy

Le policy che contengono più piani sono più complicate da risolvere a causa del maggior numero di output che devono essere tutti convalidati. Fare invece in modo che ogni policy contenga un solo piano di backup per semplificare il debug e la risoluzione dei problemi. Puoi quindi aggiungere altre policy con altri piani per soddisfare altri requisiti. Questo approccio consente di mantenere tutti i problemi relativi a un piano isolati per una policy e impedisce a tali problemi di complicare la risoluzione dei problemi relativi ad altre policy e ai relativi piani.

Utilizza gli stack set per creare i vault di backup e i ruoli IAM richiesti

Utilizza l'integrazione AWS CloudFormation StackSets con Organizations per creare automaticamente i vault di backup e i ruoli AWS Identity and Access Management (IAM) richiesti in ciascuno degli account membri dell'organizzazione. Puoi creare uno stack set che include le risorse che devono essere automaticamente disponibili in ogni Account AWS dell'organizzazione. Questo approccio ti consente di eseguire i piani di backup assicurando che le dipendenze siano già soddisfatte. Per ulteriori informazioni, consulta Creazione di uno stack set con autorizzazioni gestite dal cliente nella Guida per l'utente di AWS CloudFormation.

Controllare i risultati esaminando il primo backup creato in ogni account

Quando apportati una modifica a una policy, controlla il backup successivo creato dopo tale modifica per assicurarti che l'impatto della modifica sia quello desiderato. Questa fase va oltre la ricerca della policy effettiva e garantisce che AWS Backup interpreti le policy e implementi i piani di backup nel modo desiderato.

Creazione, aggiornamento ed eliminazione di policy di backup

In questo argomento:

- Dopo avere abilitato le policy di backup per l'organizzazione, puoi creare una policy.
- Quando i requisiti di backup cambiano, puoi aggiornare una policy esistente.
- Quando una policy non è più necessaria, dopo averla scollegata da tutte le unità organizzative (UO) e da tutti gli account la puoi eliminare.

Creazione di una policy di backup

Autorizzazioni minime

Per creare una policy di backup, è necessaria l'autorizzazione per eseguire l'operazione seguente:

- `organizations:CreatePolicy`

AWS Management Console

Puoi creare una policy di backup nella AWS Management Console in uno dei due modi seguenti:

- Un editor visivo che consente di scegliere le opzioni e generare automaticamente il testo della policy JSON.
- Un editor di testo che consente di creare automaticamente il testo della policy JSON.

L'editor visivo semplifica il processo, ma limita la flessibilità. È ottimo per creare le prime policy e iniziare a utilizzarle. Dopo aver compreso il funzionamento e aver rilevato le limitazioni alle capacità dell'editor visivo, puoi aggiungere caratteristiche avanzate alle policy modificando personalmente il testo della policy JSON. L'editor visivo utilizza solo l'operatore di impostazione del valore @@assign e non fornisce alcun accesso agli operatori di controllo figli. Puoi aggiungere gli operatori di controlli figli solo se modifichi manualmente il testo della policy JSON.

Per creare una policy di backup

1. Accedere 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. Nella pagina Backup policies (Policy di backup), scegli Create policy (Crea policy).
3. Nella pagina Create policy (Crea policy), inserisci un Nome policy e una Descrizione policy (facoltativa).
4. (Facoltativo) Per aggiungere uno o più tag alla policy, scegli Add tag (Aggiungi tag) e quindi inserisci una chiave e un valore facoltativo. Lasciando vuoto il valore, questo viene impostato su una stringa vuota; non è `null`. Puoi associare fino a 50 tag a una policy. Per ulteriori informazioni sul tagging, consultare Tagging delle risorse AWS Organizations.
5. È possibile creare la policy utilizzando l'editor visivo come descritto in questa procedura. Puoi anche inserire o incollare il testo della policy nella scheda JSON. Per informazioni sulla sintassi della policy di backup, consulta Sintassi ed esempi delle policy di backup.

   Se si sceglie di utilizzare Editor visivo, selezionare le opzioni di backup appropriate per lo scenario. Un piano di backup è composto da tre parti. Per ulteriori informazioni su questi elementi del piano di backup, consulta Creazione di un piano di backup e Assegnazione di risorse nella Guida per gli sviluppatori di AWS Backup.

   a. Dettagli generali del piano di backup
      - Il Nome del piano di Backup può essere costituito solo da caratteri alfanumerici, trattini e caratteri di sottolineatura.
      - È necessario selezionare almeno una regione del piano di Backup dall'elenco. Il piano può eseguire il backup delle risorse solo nelle Regioni AWS selezionate.
   b. Una o più regole di backup che specificano come e quando AWS Backup deve funzionare. Ogni regola di backup definisce i seguenti elementi:
      - Una pianificazione che include la frequenza del backup e la finestra temporale in cui può verificarsi il backup.
      - Il nome del vault di backup da utilizzare. Il Nome del vault di Backup può essere costituito solo da caratteri alfanumerici, trattini e caratteri di sottolineatura. Per poter eseguire correttamente il piano, il vault di backup deve esistere già. Creare il vault utilizzando la console AWS Backup o i comandi AWS CLI.

- (Facoltativo) Una o più regole Copia in Regione per copiare il backup anche nei vault in altre Regioni AWS.
- Una o più coppie di valori e chiavi di tag da collegare ai punti di ripristino di backup creati ogni volta che si esegue questo piano di backup.
- Opzioni del ciclo di vita che specificano quando il backup passa allo storage a freddo e quando il backup scade.

Scegli Add rule (Aggiungi regola) per aggiungere ogni regola necessaria al piano.

Per ulteriori informazioni sulle regole di backup, consulta Regole di backup nella Guida per gli sviluppatori di AWS Backup.

c. Un'assegnazione di risorse che specifica le risorse di cui AWS Backup deve eseguire il backup con questo piano. L'assegnazione viene effettuata specificando coppie di tag che AWS Backup utilizza per trovare e abbinare le risorse

- Il nome dell'assegnazione risorsa può essere costituito solo da caratteri alfanumerici, trattini e caratteri di sottolineatura.
- Specifica il ruolo IAM che AWS Backup può utilizzare per eseguire il backup in base al suo nome.

  Nella console, non specificare l'intero Amazon Resource Name (ARN). È necessario includere il nome del ruolo e il relativo prefisso che specifica il tipo di ruolo. I prefissi sono in genere `role` o `service-role` e sono separati dal nome del ruolo da una barra ('/'). Ad esempio, è possibile immettere `role/MyRoleName` o `service-role/MyManagedRoleName`. Questo viene convertito automaticamente in un ARN completo quando viene archiviato nel JSON sottostante.

  > **Important**
  >
  > Il ruolo IAM specificato deve esistere già nell'account a cui viene applicata la policy. In caso contrario, il piano di backup potrebbe avviare correttamente i processi di backup, ma questi non andranno a buon fine.

- Specifica uno o più valori per Resource tag key (Chiave di tag risorsa) e Tag values (Valori di tag) per identificare le risorse di cui vuoi far eseguire il backup. Se sono presenti più valori di tag, separa i valori con virgole.

Scegli Add assignment (Aggiungi un'assegnazione) per aggiungere ogni assegnazione di risorse configurata al piano di backup.

Per ulteriori informazioni, consulta Assegnazione di risorse a un piano di backup nella Guida per gli sviluppatori di AWS Backup.

6. Al termine della creazione della policy, scegli Create policy (Crea policy). La policy viene visualizzata nell'elenco delle policy di backup disponibili.

AWS CLI & AWS SDKs

Per creare una policy di backup

Per creare una policy di backup, puoi utilizzare una delle seguenti opzioni:

- AWS CLI: create-policy

  Crea un piano di backup come testo JSON simile al seguente e archivialo in un file di testo. Per le regole complete per la sintassi, consulta Sintassi ed esempi delle policy di backup.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" }
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
```

```
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII" ] }
                    }
                }
            }
        }
    }
}
```

Questa policy di backup specifica che AWS deve eseguire il backup di tutte le risorse negli Account AWS interessati che si trovano nelle Regioni AWS specificate e che hanno il tag `dataType` con un valore pari a `PII`.

Quindi, importa il piano di backup del file di policy JSON per creare una nuova policy di backup nell'organizzazione. Prendere nota dell'ID policy alla fine dell'ARN della policy nell'output.

```
$ aws organizations create-policy \
    --name "MyBackupPolicy" \
    --type BACKUP_POLICY \
    --description "My backup policy" \
    --content file://policy.json{
    "Policy": {
        "PolicySummary": {
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/backup_policy/p-
i9j8k7l6m5",
            "Description": "My backup policy",
            "Name": "MyBackupPolicy",
            "Type": "BACKUP_POLICY"
        }
        "Content": "...a condensed version of the JSON policy document you
 provided in the file...",
    }
```

```
}
```

- SDK AWS: CreatePolicy

Cosa fare in seguito

Dopo aver creato una policy di backup, puoi applicarla. A tale scopo, puoi collegare la policy al root dell'organizzazione, alle unità organizzative, agli Account AWS all'interno dell'organizzazione o a una combinazione di tutte queste entità.

Aggiornamento di una policy di backup

Quando effettui l'accesso all'account di gestione dell'organizzazione, puoi modificare una policy che richiede modifiche all'organizzazione.

> **Autorizzazioni minime**
>
> Per aggiornare una policy di backup, è necessario disporre dell'autorizzazione per le seguenti operazioni:
>
> - `organizations:UpdatePolicy` con un elemento `Resource` nella stessa istruzione di policy che includa l'ARN della policy da aggiornare (oppure "*")
> - `organizations:DescribePolicy` con un elemento `Resource` nella stessa istruzione di policy che includa l'ARN della policy da aggiornare (oppure "*")

AWS Management Console

Per aggiornare una policy di backup

1. Accedere 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. Nella pagina Backup policies (Policy di backup), scegli la policy che desideri aggiornare.
3. Selezionare Edit policy (Modifica policy).
4. È possibile inserire nuovi valori per Policy name (Nome policy) e Policy descritpion (Descrizione della policy). È possibile modificare il contenuto della policy utilizzando Visual editor (Editor visivo) o modificando direttamente il JSON.
5. Al termine dell'aggiornamento della policy, scegliere Salva modifiche.

AWS CLI & AWS SDKs

Per aggiornare una policy di backup

Per aggiornare una policy di backup, puoi utilizzare una delle seguenti opzioni:

- AWS CLI: update-policy

Nell'esempio seguente viene rinominata una policy di backup.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

Nell'esempio seguente viene aggiunta o modificata la descrizione di una policy di backup.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
```

```
        },
       "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

Nell'esempio seguente viene modificato il documento della policy JSON collegato a una policy di backup. In questo esempio, il contenuto viene preso da un file denominato `policy.json` con il testo seguente:

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" }
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                            "tag_key": { "@@assign": "dataType" },
```

```
                        "tag_value": { "@@assign": [ "PII" ] }
                    }
                }
            }
        }
    }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
}
```

- SDK AWS: UpdatePolicy

Modifica dei tag collegati a una policy di backup

Quando effettui l'accesso all'account di gestione dell'organizzazione, puoi aggiungere o rimuovere i tag collegati a una policy di backup. Per ulteriori informazioni sul tagging, consultare Tagging delle risorse AWS Organizations.

Autorizzazioni minime

Per modificare i tag associati a una policy di backup nella tua organizzazione AWS, è necessario disporre delle seguenti autorizzazioni:

- `organizations:DescribeOrganization` (solo console - per passare alla policy)
- `organizations:DescribePolicy` (solo console - per passare alla policy)

- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Per modificare i tag associati a una policy di backup

1. Accedere 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. Pagina Backup policies (Policy di backup)
3. Seleziona il nome della policy con i tag che desideri modificare.

   Viene visualizzata la pagina dei dettagli della policy.
4. Nella scheda Tags (Tag) scegliere Manage tags (Gestisci tag).
5. In questa pagina puoi eseguire le seguenti operazioni:

   - Modifica il valore di un tag inserendo un nuovo valore rispetto a quello precedente. Non è possibile modificare la chiave. Per cambiare una chiave, devi eliminare il tag con la vecchia chiave e aggiungere un tag con la nuova chiave.
   - Rimuovi eventuali tag esistenti scegliendo Remove (Rimuovi).
   - Aggiungi una nuova coppia chiave e valore di tag. Scegli Add tag (Aggiungi tag), quindi inserisci il nuovo nome della chiave e il valore facoltativo nelle caselle fornite. Se lasci vuota la casella Value (Valore), il valore è una stringa vuota; non è `null`.
6. Scegli Save changes (Salva le modifiche) dopo avere apportato tutte le aggiunte, le rimozioni e le modifiche opportune.

AWS CLI & AWS SDKs

Per modificare i tag associati a una policy di backup

Per modificare i tag associati a una policy di backup puoi utilizzare uno dei seguenti comandi:

- AWS CLI: tag-resource e untag-resource
- SDK AWS: TagResource e UntagResource

Eliminazione di una policy di backup

Quando effettui l'accesso all'account di gestione della tua organizzazione, puoi eliminare una policy di cui non hai più bisogno nella tua organizzazione.

Prima di poter eliminare una policy, devi distaccarla da tutte le entità collegate.

> **Autorizzazioni minime**
>
> Per eliminare una policy, è necessaria l'autorizzazione per la seguente operazione:
>
> - `organizations:DeletePolicy` con un elemento `Resource` nella stessa istruzione di policy che includa l'ARN della policy da eliminare (oppure "*")

AWS Management Console

Per eliminare una policy di backup

1. Accedere 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. Nella pagina Backup policies (Policy di backup), scegli la policy che desideri eliminare.
3. È necessario che la policy di backup da scollegare venga prima eliminata da tutti i root, le UO e gli account. Seleziona la scheda Targets (Destinazioni), scegli il pulsante di opzione accanto a ciascun root, UO o account visualizzato nell'elenco Targets e scegli Detach (Scollega). Nella finestra di dialogo di conferma, scegli Detach (Scollega). Ripeti finché non hai rimosso tutti i target.
4. Nella parte superiore della pagina, seleziona Delete (Elimina).
5. Nella finestra di dialogo di conferma, inserisci il nome della policy, quindi scegli Delete (Elimina).

AWS CLI & AWS SDKs

Per eliminare una policy di backup

Per eliminare una policy, puoi utilizzare una delle seguenti opzioni:

- AWS CLI: delete-policy

Nell'esempio seguente viene eliminata la policy specificata. Funziona solo se la policy non è collegata a un root, un'UO o un account.

```
$ aws organizations delete-policy \
    --policy-id p-i9j8k7l6m5
```

Questo comando non produce alcun output se ha esito positivo.

- SDK AWS: DeletePolicy

Allegare e distaccare policy di backup

Puoi utilizzare le policy di backup su un'intera organizzazione, sulle unità organizzative e sui singoli account. Tieni presente quanto segue:

- Quando colleghi una policy di backup alla root dell'organizzazione, la policy si applica a tutte le unità organizzative e agli account membri della root.
- Quando colleghi una policy di backup ad un' unità organizzativa, tale policy si applica agli account appartenenti all'unità organizzativa o a una qualsiasi delle unità organizzative figlio. Questi account sono soggetti anche a qualsiasi policy collegata alla root dell'organizzazione.
- Quando colleghi una policy di backup a un account, tale policy si applica solo a tale account. L'account è inoltre soggetto a qualsiasi policy collegata alla root dell'organizzazione e a qualsiasi unità organizzativa a cui appartiene l'account.

L'aggregazione di eventuali policy di backup che l'account eredita dal root e dalle unità organizzative padri, nonché le eventuali policy collegate direttamente all'account, formano la policy effettiva. Per informazioni sull'unione delle policy alla policy effettiva, consulta Comprendere l'ereditarietà delle policy di gestione.

Collegamento di una policy di backup

Quando effettui l'accesso all'account di gestione dell'organizzazione, puoi collegare una policy di backup al root, all'unità organizzativa o direttamente a un account dell'organizzazione.

> **Autorizzazioni minime**
>
> Per collegare le policy di backup, è necessaria l'autorizzazione per la seguente operazione:

- `organizations:AttachPolicy`

AWS Management Console

Puoi collegare una policy di backup accedendo alla policy oppure al root, all'unità organizzativa o all'account a cui vuoi collegare la policy.

Per collegare una policy di backup passando da un root, un'unità organizzativa o un account

1. Accedere 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. Nella pagina Account AWS, individua e scegli il nome del root, dell'unità organizzativa o dell'account a cui desideri collegare una policy. Potrebbe essere necessario espandere le UO (scegli l'opzione ) per individuare l'UO o l'account desiderato.
3. Nella scheda Policies (Policy), alla voce per Backup policies (Policy di backup), scegli Attach (Collega).
4. Individua la policy desiderata e scegli Attach policy (Collega policy).

   L'elenco delle policy di backup collegate nella scheda Policies (Policy) viene aggiornato per includere la nuova aggiunta. La modifica della policy diventa immediatamente effettiva.

Per collegare una policy di backup passando dalla policy

1. Accedere 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. Nella pagina Backup policies (Policy di backup), scegli il nome della policy che desideri collegare.
3. Nella scheda Targets (Destinazioni), scegli Attach (Collega).
4. Scegli il pulsante di opzione accanto al root, all'unità organizzativa o all'account a cui vuoi collegare la policy. Potrebbe essere necessario espandere le UO (scegli l'opzione

)

per individuare l'UO o l'account desiderato.

5. Scegli Attach policy (Collega policy).

   L'elenco delle policy di backup collegate nella scheda Targets (Destinazioni) viene aggiornato per includere la nuova aggiunta. La modifica della policy diventa immediatamente effettiva.

AWS CLI & AWS SDKs

Per collegare una policy di backup al root dell'organizzazione, a un'unità organizzativa o a un account

Per collegare una policy di backup, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: attach-policy

```
$ aws organizations attach-policy \
    --target-id 123456789012 \
    --policy-id p-i9j8k7l6m5
```

- SDK AWS: AttachPolicy

La modifica della policy diventa immediatamente effettiva.

Distaccare una policy di backup

Quando effettui l'accesso all'account di gestione della tua organizzazione, puoi scollegare una policy di backup dal root, dall'unità organizzativa o dall'account dell'organizzazione a cui è collegata. Dopo avere distaccato una policy di backup da un'entità, quella policy non si applica più ad alcun account interessato in precedenza dall'entità ora scollegata. Per distaccare una policy, completa le fasi seguenti.

Autorizzazioni minime

Per distaccare una policy di backup dalla root dell'organizzazione, dall'unità organizzativa o dall'account, è necessaria l'autorizzazione per la seguente operazione:

- `organizations:DetachPolicy`

AWS Management Console

Per scollegare una policy di backup, puoi accedere alla policy oppure al root, all'unità organizzativa o all'account da cui vuoi scollegare la policy.

Per scollegare una policy di backup passando dal root, dall'unità organizzativa o da un account

1. Accedere 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. Nella pagina Account AWS individua il root, l'unità organizzativa o l'account da cui desideri scollegare una policy. Potrebbe essere necessario espandere le UO (scegli l'opzione ) per individuare l'UO o l'account desiderato. Scegli il nome del root, dell'unità organizzativa o dell'account.
3. Nella scheda Policies (Policy), scegli il pulsante di opzione accanto alla policy di backup che desideri scollegare, quindi scegli Detach (Scollega).
4. Nella finestra di dialogo di conferma, scegli Detach policy (Scollega policy).

   L'elenco delle policy di backup collegate viene aggiornato. La modifica della policy diventa immediatamente effettiva.

Per scollegare una policy di backup passando dalla policy

1. Accedere 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. Nella pagina Backup policies (Policy di backup), scegli il nome della policy che vuoi scollegare da un root, un'UO o un account.
3. Nella scheda Targets (Destinazioni), scegli il pulsante di opzione accanto al root, all'unità organizzativa o all'account da cui vuoi scollegare la policy. Potrebbe essere necessario espandere le UO (scegli l'opzione ) per individuare l'UO o l'account desiderato.
4. Seleziona Detach (Scollega).
5. Nella finestra di dialogo di conferma, scegli Detach (Scollega).

L'elenco delle policy di backup collegate viene aggiornato. La modifica della policy diventa immediatamente effettiva.

AWS CLI & AWS SDKs

Per scollegare una policy di backup dal root dell'organizzazione, da un'unità organizzativa o da un account

Per scollegare una policy di backup, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: detach-policy

  Nell'esempio seguente, una policy viene scollegata da un'unità organizzativa.

  ```
  $ aws organizations detach-policy \
      --target-id ou-a1b2-f6g7h222 \
      --policy-id p-i9j8k7l6m5
  ```

  Questo comando non produce alcun output se ha esito positivo.
- SDK AWS: DetachPolicy

La modifica della policy diventa immediatamente effettiva.

Visualizzazione delle policy di backup effettive

Puoi visualizzare la policy di backup effettiva per un account dalla console di gestione AWS, tramite l'API AWS o l'interfaccia a riga di comando AWS. Nella sezione seguente viene fornita una breve panoramica della policy di backup effettiva, incluso un esempio.

Che cos'è la policy di backup effettiva?

La policy di backup effettiva specifica le impostazioni finali del piano di backup che si applicano a un Account AWS. Si tratta dell'aggregazione di tutte le policy di backup ereditate dall'account e di qualsiasi policy di backup direttamente collegata all'account. Quando colleghi una policy di backup al root dell'organizzazione, questa si applica a tutti gli account dell'organizzazione. Quando colleghi una policy di backup a un'unità organizzativa (UO), questa si applica a tutti gli account e alle unità organizzative appartenenti all'UO. Quando colleghi una policy direttamente a un account, questa si applica solo a tale Account AWS.

Ad esempio, la policy di backup collegata al root dell'organizzazione potrebbe specificare che tutti gli account dell'organizzazione eseguono il backup di tutte le tabelle Amazon DynamoDB con una frequenza di backup predefinita pari a una volta alla settimana. Una policy di backup separata collegata direttamente a un account membro con informazioni critiche in una tabella può sovrascrivere la frequenza con un valore di una volta al giorno. La combinazione di queste policy di backup comprende la policy di backup effettiva. Questa policy di backup effettiva è determinata individualmente per ogni account nell'organizzazione. In questo esempio, il risultato è che tutti gli account dell'organizzazione eseguono il backup delle tabelle DynamoDB una volta alla settimana, ad eccezione di un account che esegue il backup delle tabelle ogni giorno.

Per informazioni su come le policy di backup vengono combinate nella policy di backup effettiva finale, consulta Comprendere l'ereditarietà delle policy di gestione.

Visualizzazione della policy di backup effettiva

Puoi visualizzare la policy di backup effettiva per un account utilizzando la AWS Management Console, l'API AWS o la AWS Command Line Interface.

> **Autorizzazioni minime**
>
> Per visualizzare la policy di backup effettiva per un account, è necessario disporre dell'autorizzazione per le seguenti operazioni:
>
> - `organizations:DescribeEffectivePolicy`
> - `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations

AWS Management Console

Per visualizzare la policy di backup effettiva per un account

1. Accedere 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. Nella pagina Account AWS, scegli il nome dell'account per il quale desideri visualizzare la policy di backup effettiva. Potrebbe essere necessario espandere le UO (scegli l'opzione ▶) per individuare l'account desiderato.

3. Nella scheda Policies (Policy), nella sezione Backup policies (Policy di backup), scegli View the effective backup policy for this (Visualizza la policy di backup effettiva per questo) Account AWS.

   Nella console viene visualizzata la policy effettiva applicata all'account specificato.

   > **Note**
   >
   > Non è possibile copiare e incollare una policy effettiva e utilizzarla come JSON per un'altra policy di backup senza modifiche significative. I documenti della policy di backup devono includere gli operatori di ereditarietà che specificano la modalità di unione di ciascuna impostazione nella policy effettiva finale.

AWS CLI & AWS SDKs

Per visualizzare la policy di backup effettiva per un account

Puoi utilizzare uno dei seguenti comandi per visualizzare la policy di backup effettiva:

- AWS CLI: describe-effective-policy

  L'esempio seguente mostra i dettagli di una policy di backup.

```
$ aws organizations describe-effective-policy \
--policy-type BACKUP_POLICY \
--target-id 123456789012{
    "EffectivePolicy": {
        "LastUpdatedTimestamp": "2020-06-22T14:31:50.748000-07:00",
        "TargetId": "123456789012",
        "PolicyType": "BACKUP_POLICY",
        "PolicyContent": "{\"plans\":{\"pii_backup_plan\":{\"regions\":[\"ap-
northeast-2\",\"us-east-1\",\"eu-north-1\"],\
"selections\":{\"tags\":{\"datatype\":{\"iam_role_arn\":\"arn:aws:iam::
$account:role/MyIamRole\",\"tag_value\":[\"PII\"],\
"tag_key\":\"dataType\"}}},\"rules\":{\"hourly\":{\"complete_backup_window_minutes
\":\"10080\",\"target_backup_vault_name\
":\"FortKnox\",\"start_backup_window_minutes\":\"480\",\"schedule_expression\":
\"cron(0 5/1 ? * * *)\",\"lifecycle\":{\"mo
ve_to_cold_storage_after_days\":\"180\",\"delete_after_days\":\"270\"},
\"copy_actions\":{\"arn:aws:backup:us-east-1:$accou
```

```
nt:backup-vault:secondary-vault\":{\"lifecycle\":
{\"move_to_cold_storage_after_days\":\"10\",\"delete_after_days\":\"100\"
}}}}}}}"
    }
}
```

- SDK AWS: DescribeEffectivePolicy

Utilizzo degli eventi AWS CloudTrail per monitorare le policy di backup nell'organizzazione

È possibile utilizzare gli eventi AWS CloudTrail per monitorare quando le policy di backup vengono create, aggiornate o eliminate da qualsiasi account dell'organizzazione AWS o quando esiste un piano di backup organizzativo non valido. Per ulteriori informazioni, consulta Registrazione degli eventi per la gestione di più account nella Guida per gli sviluppatori di AWS Backup.

Sintassi ed esempi delle policy di backup

In questa pagina viene descritta la sintassi delle policy di backup e vengono forniti esempi.

Sintassi per le policy di backup

Una policy di backup è un file di testo normale strutturato in base alle regole di JSON. La sintassi per le policy di backup segue la sintassi per tutti i tipi di policy di gestione. Per una discussione completa di tale sintassi, consulta Policy syntax and inheritance for management policy types. Questo argomento è incentrato sull'applicazione della sintassi generale ai requisiti specifici del tipo di policy di backup.

La parte sostanziale di una policy di backup è costituita dal piano di backup con le relative regole. La sintassi per il piano di backup all'interno di una policy di AWS Organizations backup è strutturalmente identica alla sintassi utilizzata da AWS Backup, ma i nomi delle chiavi sono diversi. Nelle descrizioni dei nomi delle chiavi delle policy riportate di seguito, ognuno include il nome chiave del piano equivalente AWS Backup . Per ulteriori informazioni sui AWS Backup piani, consulta CreateBackupPlanla Guida perAWS Backup gli sviluppatori.

> **Note**
>
> Quando si utilizza JSON, i nomi di chiave duplicati verranno rifiutati. Se desideri includere più piani, regole o selezioni in un'unica politica, assicurati che il nome di ogni chiave sia univoco.

Per essere completa e funzionale, una policy di backup efficace deve includere più piani di backup con la relativa pianificazione e regole. La policy deve inoltre identificare le Regioni AWS risorse da sottoporre a backup e il ruolo AWS Identity and Access Management (IAM) che è AWS Backup possibile utilizzare per eseguire il backup.

La seguente policy funzionalmente completa mostra la sintassi della policy di backup di base. Se questo esempio fosse collegato direttamente a un account, AWS Backup eseguirebbe il backup di tutte le risorse relative a quell'account nelle `eu-north-1` regioni `us-east-1` e nelle regioni che hanno il tag `dataType` con un valore pari `PII` o`RED`. Esegue il backup di tali risorse ogni giorno alle 5:00 in `My_Backup_Vault` e archivia anche una copia in `My_Secondary_Vault`. Entrambi i vault si trovano nello stesso account della risorsa. Memorizza inoltre una copia del backup nel `My_Tertiary_Vault` in un account diverso, esplicitamente specificato. Le casseforti devono già esistere in ciascuna delle casseforti specificate Regioni AWS per ognuna di esse Account AWS che riceve la politica effettiva. Se una delle risorse di cui è stato eseguito il backup sono istanze EC2, il supporto per Microsoft Volume Shadow Copy Service (VSS) è abilitato per i backup di tali istanze. Il backup applica il tag `Owner:Backup` a ciascun punto di ripristino.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "rules": {
                "My_Hourly_Rule": {
                    "schedule_expression": {"@@assign": "cron(0 5 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "complete_backup_window_minutes": {"@@assign": "604800"},
                    "enable_continuous_backup": {"@@assign": false},
                    "target_backup_vault_name": {"@@assign": "My_Backup_Vault"},
                    "recovery_point_tags": {
                        "Owner": {
                            "tag_key": {"@@assign": "Owner"},
                            "tag_value": {"@@assign": "Backup"}
                        }
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "180"},
                        "delete_after_days": {"@@assign": "270"}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault": {
                            "target_backup_vault_arn": {
```

```
                                "@@assign": "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"}
                            }
                        },
                        "arn:aws:backup:us-east-1:$account:backup-
vault:My_Tertiary_Vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
east-1:111111111111:backup-vault:My_Tertiary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"}
                            }
                        }
                    }
                }
            },
            "regions": {
                "@@append": [
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "selections": {
                "tags": {
                    "My_Backup_Assignment": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
```

```
                "ec2": {
                    "windows_vss": {"@@assign": "enabled"}
                }
            },
            "backup_plan_tags": {
                "stage": {
                    "tag_key": {"@@assign": "Stage"},
                    "tag_value": {"@@assign": "Beta"}
                }
            }
        }
    }
}
```

La sintassi della policy di backup include i seguenti componenti:

- Variabili `$account` - In alcune stringhe di testo nelle policy, è possibile utilizzare la variabile `$account` per rappresentare l' Account AWScorrente. Quando AWS Backup esegue un piano nella politica effettiva, sostituisce automaticamente questa variabile con la politica corrente Account AWS in cui vengono eseguiti la politica effettiva e i relativi piani.

  > **Important**
  >
  > Puoi utilizzare la variabile `$account` solo negli elementi della policy che possono includere un Amazon Resource Name (ARN), ad esempio quelli che specificano il vault di backup in cui archiviare il backup o il ruolo IAM con autorizzazioni per eseguire il backup.

  Ad esempio, quanto segue richiede che `My_Vault` esista un archivio denominato in ogni archivio a Account AWS cui si applica la politica.

  ```
  arn:aws:backup:us-west-2:$account:vault:My_Vault"
  ```

  Ti consigliamo di utilizzare i set di AWS CloudFormation stack e la relativa integrazione con Organizations per creare e configurare automaticamente gli archivi di backup e i ruoli IAM per ogni account membro dell'organizzazione. Per ulteriori informazioni, consulta Creazione di uno stack set con autorizzazioni gestite dal cliente nella Guida per l'utente diAWS CloudFormation .

- Operatori di ereditarietà - Le policy di backup possono utilizzare sia gli operatori di impostazione del valore di ereditarietà sia gli operatori di controllo figlio.

- `plans`

  In corrispondenza della chiave di livello superiore della policy si trova la chiave `plans`. Una policy di backup deve sempre iniziare con questo nome chiave fissa nella parte superiore del file di policy. Sotto questa chiave puoi avere uno o più piani di backup.

- Ogni piano sotto la chiave di livello superiore `plans` ha un nome chiave costituito dal nome del piano di backup assegnato dall'utente. Nell'esempio precedente, il nome del piano di backup è `PII_Backup_Plan`. Puoi includere più piani in una policy, ognuno con `rules`, `regions`, `selections` e `tags` specifici.

  Questo nome chiave del piano di backup in una policy di backup corrisponde al valore della `BackupPlanName` chiave in un AWS Backup piano.

  Ogni oggetto può contenere i seguenti elementi:

  - `rules` - Questa chiave contiene una raccolta di regole. Ogni regola si traduce in un'attività pianificata, con un'ora di inizio e una finestra in cui eseguire il backup delle risorse identificate dagli elementi `selections` e `regions` nella policy di backup effettiva.
  - `regions`— Questa chiave contiene un elenco di matrici delle risorse di Regioni AWS cui è possibile eseguire il backup mediante questa politica.
  - `selections` - Questa chiave contiene una o più raccolte di risorse (all'interno delle `regions` specificate) di cui viene eseguito il backup in base alle `rules` specificate.
  - `advanced_backup_settings` - Questa chiave contiene impostazioni specifiche per i backup in esecuzione su determinate risorse.
  - `backup_plan_tags` - Specifica i tag collegati al piano di backup stesso.

- `rules`

  La chiave di policy `rules` viene mappata alla chiave `Rules` di un piano AWS Backup . Sotto la chiave `rules` possono essere presenti una o più regole. Ogni regola diventa un'attività pianificata per eseguire un backup delle risorse selezionate.

  Ogni regola contiene una chiave il cui nome chiave è il nome della regola. Nell'esempio precedente, il nome della regola è «My_Hourly_Rule». Il valore della chiave della regola è la seguente raccolta di elementi della regola:

  - `schedule_expression`— Questa chiave politica corrisponde alla `ScheduleExpression` chiave di un AWS Backup piano.

Specifica l'ora di inizio del backup. Questa chiave contiene l'operatore del valore di `@@assign` ereditarietà e un valore di stringa con un'espressione CRON che specifica quando AWS Backup avviare un processo di backup. Il formato generale della stringa CRON è: "cron( )". Ciascun elemento è un numero o un carattere jolly. Ad esempio, `cron(0 5 ? * 1,3,5 *)` avvia il backup alle 5 di ogni lunedì, mercoledì e venerdì. `cron(0 0/1 ? * * *)` avvia il backup ogni ora ad un orario prestabilito, ogni giorno della settimana.

- `target_backup_vault_name`— Questa chiave politica corrisponde alla chiave di un piano. `TargetBackupVaultName` AWS Backup

  Specifica il nome del vault di backup in cui archiviare il backup. Il valore viene creato utilizzando AWS Backup. Questa chiave contiene l'operatore del valore di ereditarietà `@@assign` e un valore stringa con un nome vault.

  > **Important**
  >
  > Il vault deve esistere già la prima volta che sia avvia il piano di backup. Ti consigliamo di utilizzare i set di AWS CloudFormation stack e la relativa integrazione con Organizations per creare e configurare automaticamente gli archivi di backup e i ruoli IAM per ogni account membro dell'organizzazione. Per ulteriori informazioni, consulta Creazione di uno stack set con autorizzazioni gestite dal cliente nella Guida per l'utente diAWS CloudFormation .

- `start_backup_window_minutes`— Questa chiave di policy corrisponde alla `StartWindowMinutes` chiave di un AWS Backup piano.

  (Facoltativo) Specifica il numero di minuti di attesa prima di annullare un processo che non viene avviato correttamente. Questa chiave contiene l'operatore del valore di ereditarietà `@@assign` e un valore con un numero intero di minuti.

- `complete_backup_window_minutes` - Questa chiave di policy viene mappata alla chiave `CompletionWindowMinutes` in un piano AWS Backup .

  (Facoltativo) Specifica il numero di minuti dopo l'avvio corretto di un processo di backup prima che venga completato o venga annullato da AWS Backup. Questa chiave contiene l'operatore del valore di ereditarietà `@@assign` e un valore con un numero intero di minuti.

- `enable_continuous_backup`— Questa chiave politica corrisponde alla `EnableContinuousBackup` chiave di un AWS Backup piano.

(Facoltativo) Specificate se vengono AWS Backup creati backup continui. `True`causa AWS Backup la creazione di backup continui in grado di point-in-time ripristinare (PITR). `False`(o non specificate) sono le cause della creazione AWS Backup di copie di backup istantanee.

> **Note**
>
> Poiché i backup abilitati per il PITR possono essere conservati per un massimo di 35 giorni, è necessario scegliere `False` o non specificare un valore se viene impostata una delle seguenti opzioni:
>
> - Imposta `delete_after_days` su un valore maggiore di 35.
> - Imposta `move_to_cold_storage_after_days` su qualsiasi valore.

Per ulteriori informazioni sui backup continui, consulta P oint-in-time recovery nella Developer Guide.AWS Backup

- `lifecycle`— Questa chiave politica corrisponde alla `Lifecycle` chiave di un AWS Backup piano.

  (Facoltativo) Specifica quando AWS Backup trasferisce questo backup alla conservazione a freddo e quando scade.

  - `move_to_cold_storage_after_days` — Questa chiave politica corrisponde alla chiave di un `MoveToColdStorageAfterDays` piano. AWS Backup

    Specifica il numero di giorni dopo l'esecuzione del backup prima che AWS Backup sposti il punto di ripristino nello storage a freddo. Questa chiave contiene l'operatore del valore di ereditarietà `@@assign` e un valore con un numero intero di giorni.

  - `delete_after_days`— Questa chiave politica corrisponde alla `DeleteAfterDays` chiave di un AWS Backup piano.

    Specifica il numero di giorni dopo l'esecuzione del backup prima che AWS Backup elimini il punto di ripristino. Questa chiave contiene l'operatore del valore di ereditarietà `@@assign` e un valore con un numero intero di giorni. Se si esegue la transizione di un backup nello storage a freddo, deve rimanere almeno 90 giorni, pertanto questo valore deve essere un minimo di 90 giorni maggiore del valore `move_to_cold_storage_after_days`.

- `copy_actions`— Questa chiave politica corrisponde alla `CopyActions` chiave di un AWS Backup piano.

(Facoltativo) Specifica che AWS Backup deve copiare il backup in una o più posizioni aggiuntive. Ogni percorso di copia di backup è descritto come segue:

- Una chiave il cui nome identifica in modo univoco questa operazione di copia. Al momento, il nome della chiave deve essere l'Amazon Resource Name (ARN) del vault di backup. Questa chiave contiene due voci.
  - `target_backup_vault_arn` - Questa chiave di policy viene mappata alla chiave `DestinationBackupVaultArn` in un piano AWS Backup .

    (Facoltativo) Specifica l'archivio in cui viene AWS Backup archiviata una copia aggiuntiva del backup. Il valore di questa chiave contiene l'operatore del valore di ereditarietà `@@assign` e l'ARN del vault.
    - Per fare riferimento a un vault in Account AWS cui è in esecuzione la policy di backup, usa la `$account` variabile nell'ARN al posto del numero ID dell'account. Quando AWS Backup esegue il piano di backup, sostituisce automaticamente la variabile con il numero ID dell'account Account AWS in cui viene eseguita la policy. Ciò consente di eseguire correttamente il backup quando la policy di backup si applica a più account di un'organizzazione.
    - Per fare riferimento a un vault in un Account AWS nella stessa organizzazione, utilizza il numero di ID dell'account effettivo nell'ARN.

    > **Important**
    >
    > - Se questa chiave è assente, viene utilizzata una versione in minuscolo dell'ARN nel nome della chiave padre. Poiché gli ARN fanno distinzione tra maiuscole e minuscole, questa stringa potrebbe non corrispondere all'ARN effettivo dell'errore e il piano non riesce. Per questo motivo, ti consigliamo di fornire sempre questa chiave e questo valore.
    > - La prima volta che si avvia il piano di backup, il vault di backup su cui vuoi copiare il backup deve già esistere. Si consiglia di utilizzare gli stack set AWS CloudFormation e la relativa integrazione con Organizations per creare e configurare automaticamente i vault di backup e i ruoli IAM per ogni account membro nell'organizzazione. Per ulteriori informazioni, consulta Creazione di uno stack set con autorizzazioni gestite dal cliente nella Guida per l'utente diAWS CloudFormation .

- `lifecycle`— Questa chiave di policy corrisponde alla `Lifecycle` chiave contenuta nella `CopyAction` chiave di un AWS Backup piano.

  (Facoltativo) Speciifica quando AWS Backup trasferisce questa copia di un backup alla conservazione a freddo e quando scade.

  - `move_to_cold_storage_after_days` - Questa chiave di policy viene mappata alla chiave `MoveToColdStorageAfterDays` in un piano AWS Backup .

    Speciifica il numero di giorni dopo l'esecuzione del backup prima dello AWS Backup spostamento del punto di ripristino nella cella frigorifera. Questa chiave contiene l'operatore del valore di ereditarietà `@@assign` e un valore con un numero intero di giorni.

  - `delete_after_days` - Questa chiave di policy viene mappata alla chiave `DeleteAfterDays` in un piano AWS Backup .

    Speciifica il numero di giorni dopo l'esecuzione del backup prima dell' AWS Backup eliminazione del punto di ripristino. Questa chiave contiene l'operatore del valore di ereditarietà `@@assign` e un valore con un numero intero di giorni. Se si esegue la transizione di un backup nello storage a freddo, deve rimanere almeno 90 giorni, pertanto questo valore deve essere un minimo di 90 giorni maggiore del valore `move_to_cold_storage_after_days`.

- `recovery_point_tags`— Questa chiave politica corrisponde alla `RecoveryPointTags` chiave di un AWS Backup piano.

  (Facoltativo) Specifica i tag da AWS Backup allegare a ogni backup creato da questo piano. Il valore di questa chiave contiene uno o più dei seguenti elementi:

  - Un identificatore per la coppia nome chiave e valore di questa chiave. Questo nome per ogni elemento in `recovery_point_tags` è il nome della chiave del tag in lettere minuscole, anche se `tag_key` ha un trattamento diverso per caso. Questo identificatore non distingue tra maiuscole e minuscole. Nell'esempio precedente, questa coppia di chiavi è stata identificata dal nome `Owner`. Ogni coppia di chiavi contiene i seguenti elementi:

    - `tag_key` - Specifica il nome della chiave di tag da collegare al piano di backup. Questa chiave contiene l'operatore del valore di ereditarietà `@@assign` e un valore stringa. Il valore prevede la distinzione tra lettere maiuscole e minuscole.

    - `tag_value`: specifica il valore collegato al piano di backup e associato alla `tag_key`. Questa chiave contiene uno qualsiasi degli operatori del valore di ereditarietà e uno o

più valori da sostituire, aggiungere o rimuovere dalla policy effettiva. Questi valori fanno distinzione tra maiuscole e minuscole.

- `regions`

  La chiave `regions` politica specifica quali risorse vengono Regioni AWS AWS Backup cercate per trovare le risorse che soddisfano le condizioni della chiave. `selections` Questa chiave contiene uno qualsiasi degli operatori di valori di ereditarietà e uno o più valori di stringa per i Regione AWS codici, ad esempio:. `["us-east-1", "eu-north-1"]`

- `selections`

  La chiave di policy `selections` specifica le risorse di cui viene eseguito il backup dalle regole del piano in questa policy. Questa chiave corrisponde all'incirca all'BackupSelectionoggetto in. AWS BackupLe risorse sono specificate da una query per la corrispondenza dei nomi e dei valori delle chiavi di tag. La chiave `selections` contiene una chiave: `tags`.

  - `tags` - Specifica i tag che identificano le risorse e il ruolo IAM che dispone dell'autorizzazione per eseguire la query e il backup delle risorse. Il valore di questa chiave contiene uno o più dei seguenti elementi:

    - Un identificatore per questo elemento del tag. Questo identificatore in `tags` è il nome della chiave di tag tutto in lettere minuscole, anche se il tag di cui eseguire la query da interrogare viene trattato in modo diverso ai fini della distinzione tra maiuscole e minuscole. Questo identificatore non distingue tra maiuscole e minuscole. Nell'esempio precedente, un elemento è stato identificato dal nome `My_Backup_Assignment`. Ogni identificatore in `tags` contiene i seguenti elementi:

      - `iam_role_arn` - Specifica il ruolo IAM che dispone dell'autorizzazione per accedere alle risorse identificate dalla query di tag nelle Regioni AWS specificate dalla chiave `regions`. Questo valore contiene l'operatore del valore di `@@assign` ereditarietà e un valore stringa che contiene l'ARN del ruolo. AWS Backup utilizza questo ruolo per interrogare e scoprire le risorse ed eseguire il backup.

        Puoi utilizzare la variabile `$account` nell'ARN al posto del numero ID dell'account. Quando il piano di backup viene eseguito AWS Backup, sostituisce automaticamente la variabile con l'effettivo numero ID dell'account Account AWS in cui viene eseguita la policy.

        > **Important**
        >
        > La prima volta che si avvia il piano di backup, il ruolo deve esistere già. Ti consigliamo di utilizzare i set di AWS CloudFormation stack e la relativa integrazione

con Organizations per creare e configurare automaticamente gli archivi di backup e i ruoli IAM per ogni account membro dell'organizzazione. Per ulteriori informazioni, consulta Creazione di uno stack set con autorizzazioni gestite dal cliente nella Guida per l'utente diAWS CloudFormation .

- `tag_key` - Specifica il nome della chiave di tag da cercare. Questa chiave contiene l'operatore del valore di ereditarietà `@@assign` e un valore stringa. Il valore prevede la distinzione tra lettere maiuscole e minuscole.
- `tag_value`— Speciifica il valore che deve essere associato a un nome di chiave corrispondente. `tag_key` AWS Backup include la risorsa nel backup solo se entrambe le opzioni `tag_key` e `tag_value` coincidono. Questa chiave contiene uno qualsiasi degli operatori del valore di ereditarietà e uno o più valori da sostituire, aggiungere o rimuovere dalla policy effettiva. Questi valori fanno distinzione tra maiuscole e minuscole.

- `advanced_backup_settings` - Specifica le impostazioni per scenari di backup specifici. Questa chiave contiene una o più impostazioni. Ogni impostazione è una stringa di oggetto JSON con i seguenti elementi:
  - Nome chiave oggetto - Una stringa che specifica il tipo di risorsa a cui si applicano le seguenti impostazioni avanzate.
  - Valore oggetto - Una stringa di oggetto JSON che contiene una o più impostazioni di backup specifiche per il tipo di risorsa associato.

  Al momento, l'unica impostazione di backup avanzata supportata abilita i backup di Microsoft Volume Shadow Copy Service (VSS) per Windows o SQL Server in esecuzione su un'istanza Amazon EC2. Il nome della chiave deve essere il tipo di risorsa `"ec2"`, mentre il valore specifica che il supporto `"windows_vss"` è `enabled` o `disabled` per i backup eseguiti su tali istanze Amazon EC2. Per ulteriori informazioni su questa caratteristica, consulta Creazione di un backup Windows abilitato per VSS nella Guida per gli sviluppatori diAWS Backup .

```
"advanced_backup_settings": {
    "ec2": {
        "windows_vss": {
            "@@assign": "enabled"
        }
    }
}
```

- `backup_plan_tags` - Specifica i tag collegati al piano di backup stesso. Ciò non influisce sui tag specificati nelle regole o nelle selezioni.

(Facoltativo) Puoi collegare i tag ai piani di backup. Il valore di questa chiave è una raccolta di elementi.

Il nome della chiave per ogni elemento in `backup_plan_tags` è il nome della chiave di tag tutta in lettere minuscole, anche se il tag di cui effettuare la query viene trattato in modo diverso ai fini della distinzione tra maiuscole e minuscole. Questo identificatore non distingue tra maiuscole e minuscole. Il valore per ciascuna di queste voci è costituito dalle seguenti chiavi:

- `tag_key` - Specifica il nome della chiave di tag da collegare al piano di backup. Questa chiave contiene l'operatore del valore di ereditarietà `@@assign` e un valore stringa. Questo valore prevede la distinzione tra lettere maiuscole e minuscole.
- `tag_value`: specifica il valore collegato al piano di backup e associato alla `tag_key`. Questa chiave contiene l'operatore del valore di ereditarietà `@@assign` e un valore stringa. Questo valore prevede la distinzione tra lettere maiuscole e minuscole.

Esempi di policy di backup

Le policy di backup di esempio che seguono sono solo a scopo informativo. In alcuni degli esempi seguenti, la formattazione degli spazi bianchi JSON potrebbe essere compressa per risparmiare spazio.

Esempio 1: policy assegnata a un nodo padre

Nell'esempio seguente viene illustrata una policy di backup assegnata a uno dei nodi padre di un account.

Policy padre - Questa policy può essere collegata al root dell'organizzazione o a qualsiasi unità organizzativa che è un padre di tutti gli account previsti.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "ap-northeast-2",
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "rules": {
```

```
                "Hourly": {
                    "schedule_expression": {
                        "@@assign": "cron(0 5/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@assign": "480"
                    },
                    "complete_backup_window_minutes": {
                        "@@assign": "10080"
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {
                            "@@assign": "180"
                        },
                        "delete_after_days": {
                            "@@assign": "270"
                        }
                    },
                    "target_backup_vault_name": {
                        "@@assign": "FortKnox"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                }
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
                            },
                            "lifecycle": {
```

```
                            "move_to_cold_storage_after_days": {
                                "@@assign": "30"
                            },
                            "delete_after_days": {
                                "@@assign": "120"
                            }
                        }
                    }                   }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {
                            "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                        },
                        "tag_key": {
                            "@@assign": "dataType"
                        },
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": {
                        "@@assign": "enabled"
                    }
                }
            }
        }
    }
}
```

Se nessun altro criterio viene ereditato o associato agli account, la politica effettiva resa in ciascuna delle politiche applicabili è Account AWS simile all'esempio seguente. L'espressione CRON implica che il backup venga eseguito una volta all'ora. L'ID account 123456789012 sarà l'ID account effettivo per ogni account.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "to_delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180"
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "to_delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
```

```
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": "enabled"
                }
            }
        }
    }
}
```

Esempio 2: una policy padre viene unita a una policy figlio

Nell'esempio seguente, una politica ereditata per i genitori e una politica per i figli sono ereditate o direttamente collegate a un' Account AWS unione per formare la politica effettiva.

Policy padre - Questa policy può essere collegata al root dell'organizzazione o a qualsiasi unità organizzativa padre.

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": { "@@append":[ "us-east-1", "ap-northeast-3", "eu-north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 0/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "60" },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "28" },
                        "to_delete_after_days": { "@@assign": "180" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
```

```
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "28" },
                                "to_delete_after_days": { "@@assign": "180" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII", "RED" ] }
                    }
                }
            }
        }
    }
}
```

Policy figlia - Questa policy può essere collegata direttamente all'account o a un'unità organizzativa che si trova a un livello inferiore qualsiasi a quello della policy padre cui è collegata.

```
{
    "plans": {
       "Monthly_Backup_Plan": {
            "regions": {
                "@@append":[ "us-east-1", "eu-central-1" ] },
            "rules": {
                "Monthly": {
                    "schedule_expression": { "@@assign": "cron(0 5 1 * ? *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "target_backup_vault_name": { "@@assign": "Default" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "30" },
                        "to_delete_after_days": { "@@assign": "365" }
                    },
```

```
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:Default" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "30" },
                                "to_delete_after_days": { "@@assign": "365" }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "MonthlyDatatype": {
                            "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyMonthlyBackupIamRole" },
                            "tag_key": { "@@assign": "BackupType" },
                            "tag_value": { "@@assign": [ "MONTHLY", "RED" ] }
                        }
                    }
                }
            }
        }
```

Policy effettiva risultante - La policy effettiva applicata agli account contiene due piani, ciascuno con un proprio set di regole e un set di risorse a cui applicare le regole.

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": [ "us-east-1", "ap-northeast-3", "eu-north-1" ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
```

```
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "to_delete_after_days": "180"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [ "PII", "RED" ]
                    }
                }
            }
        },
        "Monthly_Backup_Plan": {
            "regions": [ "us-east-1", "eu-central-1" ],
            "rules": {
                "monthly": {
                    "schedule_expression": "cron(0 5 1 * ? *)",
                    "start_backup_window_minutes": "480",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "to_delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:Default" : {
                            "target_backup_vault_arn": {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:Default"
                            },
                            "lifecycle": {
```

```
                                "move_to_cold_storage_after_days": "30",
                                "to_delete_after_days": "365"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "monthlydatatype": {
                        "iam_role_arn": "arn:aws:iam::&ExampleAWSAccountNo3;:role/
MyMonthlyBackupIamRole",
                        "tag_key": "BackupType",
                        "tag_value": [ "MONTHLY", "RED" ]
                    }
                }
            }
        }
    }
}
```

Esempio 3: una policy padre impedisce qualsiasi modifica da parte di una policy figlio

Nell'esempio seguente, una policy padre ereditata utilizza gli operatori di controllo figlio per imporre tutte le impostazioni e impedisce che vengano modificate o sostituite da una policy figlio.

Policy padre - Questa policy può essere collegata al root dell'organizzazione o a qualsiasi unità organizzativa padre. La presenza di `"@@operators_allowed_for_child_policies": ["@@none"]` in ogni nodo della policy significa che una policy figlio non può apportare modifiche di alcun tipo al piano. Né una policy figlio può aggiungere altri piani alla policy effettiva. Questa policy diventa la policy effettiva per ogni unità organizzativa e account nell'unità organizzativa cui è collegata.

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@none"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@append": [
                    "us-east-1",
```

```
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "Hourly": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "schedule_expression": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "cron(0 0/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "60"
                    },
                    "target_backup_vault_name": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "FortKnox"
                    },
                    "lifecycle": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "move_to_cold_storage_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "28"
                        },
                        "to_delete_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "180"
                        }
                    },
                    "copy_actions": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:
$account:vault:secondary_vault",
                                "@@operators_allowed_for_child_policies": ["@@none"]
                            },
                            "lifecycle": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "to_delete_after_days": {
```

```
                                    "@@operators_allowed_for_child_policies":
["@@none"],
                                    "@@assign": "28"
                                },
                                "move_to_cold_storage_after_days": {
                                    "@@operators_allowed_for_child_policies":
["@@none"],
                                    "@@assign": "180"
                                }
                            }
                        }
                    }
                },
                "selections": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "tags": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "datatype": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "iam_role_arn": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                            },
                            "tag_key": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "@@assign": "dataType"
                            },
                            "tag_value": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "@@assign": [
                                    "PII",
                                    "RED"
                                ]
                            }
                        }
                    }
                },
                "advanced_backup_settings": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "ec2": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "windows_vss": {
                            "@@assign": "enabled",
```

```
                        "@@operators_allowed_for_child_policies": ["@@none"]
                    }
                }
            }
        }
    }
}
```

Policy effettiva risultante - Se esistono policy di backup figlio, queste vengono ignorate e la policy padre diventa la policy effettiva.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "target_backup_vault_arn": "arn:aws:backup:us-
east-1:123456789012:vault:secondary_vault",
                        "lifecycle": {
                            "move_to_cold_storage_after_days": "28",
                            "to_delete_after_days": "180"
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
```

```
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {"windows_vss": "enabled"}
            }
        }
    }
}
```

Esempio 4: una policy padre impedisce modifiche a un piano di backup da parte di una policy figlio

Nell'esempio seguente, una policy padre ereditata utilizza gli operatori di controllo figlio per imporre le impostazioni per un singolo piano e impedisce che vengano modificate o sostituite da una policy figlio. La policy figlio può comunque aggiungere altri piani.

Policy padre - Questa policy può essere collegata al root dell'organizzazione o a qualsiasi unità organizzativa padre. Questo esempio è simile all'esempio precedente con tutti gli operatori di ereditarietà figlio bloccati, ad eccezione del livello superiore `plans`. L'impostazione `@@append` a tale livello consente alle policy figlio di aggiungere altri piani alla raccolta nella policy effettiva. Le eventuali modifiche apportate al piano ereditato sono ancora bloccate.

Le sezioni del piano vengono troncate per chiarezza.

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@append"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        }
    }
}
```

Policy figlia - Questa policy può essere collegata direttamente all'account o a un'unità organizzativa che si trova a un livello inferiore qualsiasi a quello della policy padre cui è collegata. Questa policy figlio definisce un nuovo piano.

Le sezioni del piano vengono troncate per chiarezza.

```
{
    "plans": {
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

Policy effettiva risultante - La policy effettiva include entrambi i piani.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        },
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

Esempio 5: una policy figlio sostituisce le impostazioni in una policy padre

Nell'esempio seguente, una policy figlia utilizza operatori di impostazione del valore per sovrascrivere alcune delle impostazioni ereditate da una policy padre.

Policy padre - Questa policy può essere collegata al root dell'organizzazione o a qualsiasi unità organizzativa padre. Qualsiasi impostazione può essere sovrascritta da una policy figlio perché il comportamento predefinito, in assenza di un operatore di controllo figlio che lo impedisce, è quello di

consentire alla policy figlio di `@@assign`, `@@append` o `@@remove`. La policy padre contiene tutti gli elementi necessari per un piano di backup valido, quindi esegue correttamente il backup delle risorse se viene ereditata così com'è.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/1 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "target_backup_vault_name": {"@@assign": "FortKnox"},
                    "lifecycle": {
                        "to_delete_after_days": {"@@assign": "2"},
                        "move_to_cold_storage_after_days": {"@@assign": "180"}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:t2": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:vault:t2"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "28"},
                                "to_delete_after_days": {"@@assign": "180"}
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
```

```
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            }
        }
    }
}
```

Policy figlia - La policy figlia include solo le impostazioni che devono essere diverse dalla policy padre ereditata. È necessario disporre di una policy padre ereditata che fornisca le altre impostazioni necessarie quando viene unita in una policy effettiva. In caso contrario, la policy di backup effettiva contiene un piano di backup che non è valido e non esegue il backup delle risorse come previsto.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "us-west-2",
                    "eu-central-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/2 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "80"},
                    "target_backup_vault_name": {"@@assign": "Default"},
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "30"},
                        "to_delete_after_days": {"@@assign": "365"}
                    }
                }
            }
        }
    }
}
```

Policy effettiva risultante - La policy effettiva include le impostazioni di entrambe le policy, con le impostazioni fornite dalla policy figlio che sovrascrivono le impostazioni ereditate dal padre. In questo esempio, si verificano le seguenti modifiche:

- L'elenco delle regioni viene sostituito con un elenco completamente diverso. Se desideri aggiungere una Regione all'elenco ereditato, utilizza `@@append` anziché `@@assign` nella policy figlia.
- AWS Backup viene eseguito ogni due ore anziché ogni ora.
- AWS Backup consente l'avvio del backup per 80 minuti anziché 60 minuti.
- AWS Backup utilizza il `Default` vault invece di. `FortKnox`
- Il ciclo di vita viene esteso sia per il trasferimento nello storage a freddo sia per l'eliminazione finale del backup.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-west-2",
                "eu-central-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/2 ? * * *)",
                    "start_backup_window_minutes": "80",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "to_delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:vault:secondary_vault"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "to_delete_after_days": "180"
                            }
                        }
                    }
                }
```

```
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            }
        }
    }
}
```

Policy di tag

Puoi utilizzare le policy di tag per mantenere i tag coerenti, incluso il trattamento lettere maiuscole o minuscole preferito delle chiavi e dei valori di tag.

Cosa sono i tag?

I tag sono etichette di attributi personalizzate che assegni o che AWS assegna alle risorse AWS. Ogni tag è costituito da due parti:

- Una chiave del tag (ad esempio, `CostCenter`, `Environment` o `Project`). Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.
- Un campo facoltativo noto come valore del tag (ad esempio, `111122223333` o `Production`). Non specificare il valore del tag equivale a utilizzare una stringa vuota. Analogamente alle chiavi dei tag, i valori dei tag prevedono una distinzione tra lettere maiuscole e minuscole.

Il resto di questa pagina descrive le policy di tag. Per ulteriori informazioni sui tag, consulta i seguenti argomenti:

- Per informazioni generali sull'etichettatura, incluse le convenzioni di denominazione e utilizzo, consulta la AWSTagging Resources User Guide.
- Per un elenco dei servizi che supportano l'utilizzo dei tag, consulta l'argomento della documentazione di riferimento delle API per l'applicazione di tag a Resource Groups.

- Per informazioni sull'utilizzo dei tag per classificare le risorse, consultate il white paper sulle migliori pratiche per l'etichettatura delle risorse. AWS
- Per informazioni sull'assegnazione di tag alle risorse di Organizations, consulta Tagging delle risorse AWS Organizations.
- Per informazioni sull'etichettatura delle risorse in altri AWS servizi, consulta la documentazione relativa a tale servizio.

Che cosa sono le policy di tag?

Le policy di tag sono un tipo di policy che può semplificare la standardizzazione dei tag tra le risorse degli account dell'organizzazione. In una policy di tag specifichi le regole di tag applicabili alle risorse quando vengono taggate.

Ad esempio, una policy di tag può specificare che quando il tag `CostCenter` è collegato a una risorsa, deve utilizzare i valori di trattamento lettere maiuscole o minuscole e di tag definiti dalla policy di tag. Una policy di tag può anche specificare che le operazioni di tag non conformi vengono applicate su tipi di risorse specifici. In altre parole, le richieste di tag non conformi su tipi di risorse specifici non possono essere completate. Le risorse senza tag o i tag non sono definiti nella policy di tag non vengono valutati per la conformità con la policy di tag.

L'utilizzo delle policy di tag comporta l'utilizzo di più servizi AWS:

- Utilizza AWS Organizations per gestire le policy di tag. Quando effettui l'accesso all'account di gestione dell'organizzazione, puoi usare Organizations per abilitare la caratteristica delle policy di tag. È necessario accedere come utente IAM, assumere un ruolo IAM o accedere come utente root (non consigliato) nell'account di gestione dell'organizzazione. Quindi, puoi creare le policy di tag e collegarle alle entità dell'organizzazione per rendere effettive tali regole di tag.
- Utilizza AWS Resource Groups per gestire la conformità con le policy di tag. Quando effettui l'accesso a un account dell'organizzazione, puoi utilizzare Resource Groups per trovare tag non conformi nelle risorse dell'account. Puoi correggere i tag non conformi nel servizio AWS in cui è stata creata la risorsa.

  Se accedi all'account di gestione nell'organizzazione, puoi visualizzare le informazioni di conformità per tutti gli account dell'organizzazione.

Le policy di tag sono disponibili solo nelle organizzazioni in cui sono abilitate tutte le caratteristiche. Per ulteriori informazioni sui requisiti per utilizzare le policy di tag, consulta Prerequisiti e autorizzazioni per la gestione delle policy di tag.

> **Important**
>
> Per iniziare a usare le policy di tag, AWS consiglia vivamente di seguire il flusso di lavoro di esempio descritto in Nozioni di base sulle policy di tag prima di passare a policy di tag più avanzate. È meglio comprendere gli effetti del collegamento di una policy di tag semplice a un singolo account prima di espandere le policy di tag a un'intera unità organizzativa o a un'organizzazione. È particolarmente importante comprendere gli effetti di una policy di tag prima di applicare la conformità a qualsiasi policy di tag. Le tabelle della pagina Nozioni di base sulle policy di tag forniscono anche i collegamenti alle istruzioni per le attività più avanzate relative alle policy.

Prerequisiti e autorizzazioni per la gestione delle policy di tag

In questa pagina vengono descritti i prerequisiti e le autorizzazioni necessarie per la gestione delle policy di tag in AWS Organizations.

Argomenti

- Prerequisiti per la gestione delle policy di tag
- Autorizzazioni per la gestione delle policy di tag

Prerequisiti per la gestione delle policy di tag

Per utilizzare le policy di tag:

- L'organizzazione deve avere tutte le caratteristiche abilitate.
- È necessario accedere all'account di gestione dell'organizzazione.
- Sono necessarie le autorizzazioni elencate in Autorizzazioni per la gestione delle policy di tag.

Per valutare la conformità con le policy di tag utilizzi AWS Resource Groups. Per informazioni sui requisiti per la valutazione della conformità, consulta l'argomento relativo a prerequisiti e autorizzazioni nella Guida per l'utente di AWS Resource Groups.

Autorizzazioni per la gestione delle policy di tag

La policy IAM di esempio riportata di seguito fornisce le autorizzazioni per la gestione delle policy di tag.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageTagPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribePolicy",
                "organizations:ListRoots",
                "organizations:DisableAWSServiceAccess",
                "organizations:DetachPolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
                "organizations:DisablePolicyType",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListPolicies",
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListCreateAccountStatus",
                "organizations:DescribeOrganization",
                "organizations:UpdatePolicy",
                "organizations:EnablePolicyType",
                "organizations:DescribeOrganizationalUnit",
                "organizations:AttachPolicy",
                "organizations:ListParents",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:CreatePolicy",
                "organizations:DescribeCreateAccountStatus"
            ],
            "Resource": "*"
        }
    ]
}
```

Per ulteriori informazioni sulle policy e le autorizzazioni in IAM, consulta la Guida per l'utente di IAM.

Best practice per l'utilizzo delle policy di tag

AWS consiglia le seguenti best practice per l'utilizzo delle policy di tag.

Decidi una strategia di capitalizzazione dei tag

Determina come desideri capitalizzare i tag e implementa in modo coerente tale strategia in tutti i tipi di risorse. Ad esempio, puoi decidere se utilizzare `Costcenter`, `costcenter` o `CostCenter` e utilizzare la stessa convenzione per tutti i tag. Per risultati coerenti nei report di conformità, evita di utilizzare tag simili con un trattamento lettere maiuscole o minuscole incoerente. Questa strategia consente di definire le policy di tag per l'organizzazione.

Utilizza il flusso di lavoro consigliato

Inizia in piccolo creando una semplice policy di tag. Quindi collegala a un account membro che puoi usare a scopo di test. Utilizza i flussi di lavoro descritti in Nozioni di base sulle policy di tag.

Determina le regole di tagging

Questo dipenderà dalle esigenze dell'organizzazione. Ad esempio, è possibile specificare che quando un tag `CostCenter` è collegato ai segreti AWS Secrets Manager, deve utilizzare il trattamento lettere maiuscole o minuscole specificato. Crea le policy di tag che definiscono tag conformi e collegali alle entità dell'organizzazione in cui vuoi che tali regole di tag siano in vigore.

Istruire gli amministratori degli account

Quando sei pronto a espandere l'utilizzo delle policy di tag, istruisci gli amministratori degli account come segue:

- Comunica la tua strategia di tag.
- Sottolinea che gli amministratori devono utilizzare i tag su tipi di risorse specifici.

  Questo è importante perché le risorse senza tag non vengono visualizzate come non conformi nei risultati di conformità.
- Fornisci le indicazioni per verificare la conformità con le policy di tag. Indica agli amministratori di trovare e correggere i tag non conformi sulle risorse del proprio account utilizzando la procedura descritta nell'argomento relativo alla valutazione della conformità per un account nella Guida per l'utente di AWS Resource Groups. Indica la frequenza con cui desideri che verifichino la conformità.

Usa cautela nell'applicare la conformità

L'applicazione della conformità potrebbe impedire agli utenti degli account dell'organizzazione di applicare i tag alle risorse necessarie. Rivedi le informazioni in Informazioni sull'applicazione. Consulta anche i flussi di lavoro descritti in Nozioni di base sulle policy di tag.

Considera la possibilità di creare una SCP per impostare dei limiti attorno alle richieste di creazione di risorse

Le risorse a cui non sono mai stati associati tag non vengono visualizzate come non conformi nei report. Gli amministratori dell'account possono comunque creare risorse senza tag. In alcuni casi, è possibile utilizzare una policy di controllo dei servizi per impostare i guardrail attorno alle richieste di creazione delle risorse. Per un esempio di policy di controllo dei servizi, consulta Richiedere un tag sulle risorse create specificate. Per sapere se un servizio AWS supporta il controllo dell'accesso tramite tag, consultare Servizi AWS supportati da IAM nella Guida per l'utente di IAM. Cerca i servizi che hanno Yes (Sì) nella colonna Authorization based on tags (Autorizzazione basata su tag). Scegli il nome del servizio per visualizzarne la documentazione sul controllo degli accessi e delle autorizzazioni.

Nozioni di base sulle policy di tag

L'utilizzo delle policy di tag comporta l'utilizzo di più servizi AWS: Per iniziare, esamina le pagine seguenti. Segui quindi i flussi di lavoro in questa pagina per familiarizzare con le policy di tag e i loro effetti.

- Prerequisiti e autorizzazioni per la gestione delle policy di tag
- Best practice per l'utilizzo delle policy di tag

Utilizzo delle policy di tag per la prima volta

Attieniti alla seguente procedura per iniziare a utilizzare le policy di tag per la prima volta.

Processo	Account a cui accedere	Console del servizio AWS da utilizzare
Fase 1: abilita le policy di tag per l'organizzazione.	Account di gestione dell'organizzazione.[1]	AWS Organizations

Processo	Account a cui accedere	Console del servizio AWS da utilizzare
Fase 2: crea una policy di tag. Mantieni semplice la tua prima policy di tag. Inserisci una chiave di tag nel trattamento lettere maiuscole o minuscole che desideri utilizzare e lascia tutte le altre opzioni sulle impostazioni predefinite.	Account di gestione dell'organizzazione.[1]	AWS Organizations
Fase 3: collega una policy di tag a un singolo account membro che è possibile utilizzare per il test. Dovrai accedere a questo account nella prossima fase.	Account di gestione dell'organizzazione.[1]	AWS Organizations
Fase 4: crea alcune risorse con tag conformi e alcune con tag non conformi.	L'account membro che stai utilizzando a scopo di test.	Un servizio AWS che desideri. Ad esempio, puoi utilizzare AWS Secrets Manager e seguire la procedura in Creazione di un segreto di base per creare segreti con segreti conformi e non conformi.

Processo	Account a cui accedere	Console del servizio AWS da utilizzare
Fase 5: visualizza le policy di tag operative e valutare lo stato di conformità dell'account.	L'account membro che stai utilizzando a scopo di test.	Resource Groups e il servizio AWS in cui è stata creata la risorsa. Se sono state create risorse con tag conformi e non conformi, i tag non conformi vengono visualizzati nei risultati.
Fase 6: ripeti il processo di individuazione e correzione dei problemi di conformità fino a quando le risorse dell'account di test non siano conformi alla policy di tag.	L'account membro che stai utilizzando a scopo di test.	Resource Groups e il servizio AWS in cui è stata creata la risorsa.
In qualsiasi momento, puoi valutare la conformità a livello di organizzazione.	Account di gestione dell'organizzazione.[1]	Gruppi di risorse

[1] È necessario accedere come utente IAM, assumere un ruolo IAM o accedere come utente root (non consigliato) nell'account di gestione dell'organizzazione.

Espansione dell'uso delle policy di tag

Per espandere l'utilizzo delle policy di tag puoi eseguire le seguenti attività in qualsiasi ordine.

Attività avanzata	Account a cui accedere	Console del servizio AWS da utilizzare
Creare policy di tag avanzate. Segui lo stesso processo degli utenti inesperti, ma prova altre	Account di gestione dell'organizzazione.[1]	AWS Organizations

Attività avanzata	Account a cui accedere	Console del servizio AWS da utilizzare
attività. Ad esempio, definisci chiavi o valori aggiuntivi o specifica un trattamento lettere maiuscole o minuscole diverso per una chiave di tag. Puoi utilizzare le informazioni in Comprendere l'ereditarietà delle policy di gestione e Sintassi delle policy di tag per creare policy di tag più dettagliate.		
Collega le policy di tag ad account o unità organizzative aggiuntivi. Controlla la policy di tag operativa per un account dopo aver collegato altre policy all'account o a qualsiasi unità organizzativa in cui l'account è membro.	Account di gestione dell'organizzazione.[1]	AWS Organizations
Crea una policy di controllo dei servizi per richiedere i tag quando vengono create nuove risorse. Per un esempio, consulta Richiedere un tag sulle risorse create specificate.	Account di gestione dell'organizzazione.[1]	AWS Organizations

Attività avanzata	Account a cui accedere	Console del servizio AWS da utilizzare
Continua a valutare lo stato di conformità dell'account rispetto alla policy di tag operativa man mano che cambia. Correggi i tag non conformi.	Un account membro con una policy di tag attiva.	Resource Groups e il servizio AWS in cui è stata creata la risorsa.
Valuta la conformità a livello di organizzazione.	Account di gestione dell'organizzazione.[1]	Gruppi di risorse

[1] È necessario accedere come utente IAM, assumere un ruolo IAM o accedere come utente root (non consigliato) nell'account di gestione dell'organizzazione.

Applicazione delle policy di tag per la prima volta

Per applicare le policy di tag per la prima volta, segui un flusso di lavoro simile all'utilizzo delle policy di tag per la prima volta e utilizza un account di test.

> **Warning**
>
> Usa cautela nell'applicare la conformità. Assicurati di aver compreso gli effetti dell'utilizzo delle policy di tag e segui il flusso di lavoro raccomandato. Verifica il funzionamento dell'applicazione in un account di test prima di espanderla a più account. In caso contrario, potresti impedire agli utenti degli account dell'organizzazione di applicare i tag alle risorse necessarie. Per ulteriori informazioni, consulta Informazioni sull'applicazione.

Attività di applicazione	Account a cui accedere	Console del servizio AWS da utilizzare
Fase 1: crea una policy di tag. Mantieni semplice la tua prima policy di tag applicata . Immetti una chiave di	Account di gestione dell'organizzazione.[1]	AWS Organizations

Attività di applicazione	Account a cui accedere	Console del servizio AWS da utilizzare
tag nel trattamento lettere maiuscole o minuscole che desideri utilizzare e scegli l'opzione Prevent noncompli ant operations for this tag (Impedisci operazioni non conformi per questo tag). Quindi specifica un tipo di risorsa su cui applicarla. Continuando con l'esempio precedente, puoi scegliere di applicarla sui segreti Secrets Manager.		
Fase 2: collega una policy di tag a un singolo account di test.	Account di gestione dell'orga nizzazione.[1]	AWS Organizations
Fase 3: prova a creare alcune risorse con tag conformi e alcune con tag non conformi. Non ti è consentito creare un tag per una risorsa del tipo specificato nella policy di tag con un tag non conforme.	L'account membro che stai utilizzando a scopo di test.	Un servizio AWS che desideri. Ad esempio, puoi utilizzar e AWS Secrets Manager e seguire la procedura in Creazione di un segreto di base per creare segreti con segreti conformi e non conformi.
Fase 4: valuta lo stato di conformità dell'account rispetto alla policy di tag operativa e correggi i tag non conformi.	L'account membro che stai utilizzando a scopo di test.	Resource Groups e il servizio AWS in cui è stata creata la risorsa.

Attività di applicazione	Account a cui accedere	Console del servizio AWS da utilizzare
Fase 5: ripeti il processo di individuazione e correzione dei problemi di conformità fino a quando le risorse dell'acco unt di test non siano conformi alla policy di tag.	L'account membro che stai utilizzando a scopo di test.	Resource Groups e il servizio AWS in cui è stata creata la risorsa.
In qualsiasi momento, puoi valutare la conformità a livello di organizzazione.	Account di gestione dell'orga nizzazione.[1]	Gruppi di risorse

[1] È necessario accedere come utente IAM, assumere un ruolo IAM o accedere come utente root (non consigliato) nell'account di gestione dell'organizzazione.

Creazione, aggiornamento ed eliminazione delle policy di tag

In questo argomento:

- Dopo avere abilitato le policy di tag per l'organizzazione, puoi creare una policy.
- Quando i requisiti di assegnazione di tag cambiano, puoi aggiornare una policy esistente.
- Quando una policy non è più necessaria, dopo averla scollegata da tutte le unità organizzative (UO) e da tutti gli account la puoi eliminare.

> **Important**
>
> Le risorse senza tag non appaiono nei risultati come non conformi.

Creazione di una policy di tag

> **Autorizzazioni minime**
>
> Per creare le policy di tag, è necessaria l'autorizzazione per la seguente operazione:

- `organizations:CreatePolicy`

Puoi creare una policy di tag nella AWS Management Console in uno dei due modi seguenti:

- Un editor visivo che consente di scegliere le opzioni e generare automaticamente il testo della policy JSON.
- Un editor di testo che consente di creare automaticamente il testo della policy JSON.

L'editor visivo semplifica il processo, ma limita la flessibilità. È ottimo per creare le prime policy e iniziare a utilizzarle. Dopo aver compreso il funzionamento e aver rilevato le limitazioni alle capacità dell'editor visivo, puoi aggiungere caratteristiche avanzate alle policy modificando personalmente il testo della policy JSON. L'editor visivo utilizza solo l'operatore di impostazione del valore @@assign e non fornisce alcun accesso agli operatori di controllo figli. Puoi aggiungere gli operatori di controlli figli solo se modifichi manualmente il testo della policy JSON.

AWS Management Console

Per creare una policy di tag

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. Nella pagina Tag policies (Policy di tag), scegli Create policy (Crea policy).
3. Nella pagina Create policy (Crea policy), inserisci un Nome policy e una Descrizione policy (facoltativa).
4. (Facoltativo) Puoi aggiungere uno o più tag per l'oggetto policy. Questi tag non fanno parte della policy. A questo scopo, scegli Add tag (Aggiungi tag) e inserisci una chiave e un valore facoltativo. Lasciando vuoto il valore, questo viene impostato su una stringa vuota; non è `null`. Puoi associare fino a 50 tag a una policy. Per ulteriori informazioni, consulta Tagging delle risorse AWS Organizations.
5. È possibile creare la policy di tag utilizzando l'editor visivo come descritto in questa procedura. È inoltre possibile digitare o incollare una policy di tag nella scheda JSON. Per informazioni sulla sintassi delle policy di tag, consulta Sintassi delle policy di tag.

Per New tag key 1 (Nuova chiave di tag 1), specifica il nome di una chiave di tag da aggiungere.

6. Per la conformità dell'uso delle maiuscole e delle minuscole della chiave di tag, lascia questa opzione deselezionata (impostazione predefinita) per specificare che la policy di tag padre ereditata, se presente, deve definire il trattamento delle lettere maiuscole o minuscole per la chiave di tag.

   Seleziona questa opzione se desideri impostare una norma specifica su minuscole e maiuscole per la chiave di tag utilizzando questa policy. Se si seleziona questa opzione, l'uso delle maiuscole e delle minuscole specificato per Tag Key (Chiave di tag) sostituisce il trattamento di lettere maiuscole o minuscole specificato in una policy padre ereditata.

   Se non esiste una policy padre e non abiliti questa opzione, solo le chiavi di tag in caratteri minuscoli sono considerate conformi. Per ulteriori informazioni sull'ereditarietà dai policy padre, consulta Comprendere l'ereditarietà delle policy di gestione.

   > **Tip**
   >
   > Puoi utilizzare la policy di tag di esempio mostrata in Esempio 1: definire l'uso delle maiuscole o minuscole per la chiave di tag a livello di organizzazione come guida per la creazione di una policy di tag che definisca le chiavi di tag e il relativo trattamento lettere maiuscole o minuscole. Collegala alla root dell'organizzazione. Successivamente, puoi creare e collegare ulteriori policy di tag alle unità organizzative o agli account per creare ulteriori regole di tag.

7. Per Tag value compliance (Conformità dei valori di tag), seleziona questa opzione se desideri aggiungere valori consentiti per questa chiave di tag a tutti i valori ereditati da una policy padre.

   Per impostazione predefinita, questa opzione è deselezionata, il che significa che solo i valori definiti in ed ereditati da una policy padre sono considerati conformi. Se una policy padre non esiste e non si specificano valori di tag, qualsiasi valore (incluso nessun valore) viene considerato conforme.

   Per aggiornare l'elenco dei valori di tag accettabili, seleziona Specify allowed values for this tag key (Specifica i valori consentiti per questa chiave di tag) quindi scegli Specify values

(Specifica valori). Quando richiesto, inserisci i nuovi valori (uno per casella) e scegli Save changes (Salva modifiche).

8. Per Prevent noncompliant operations for this tag (Impedisci operazioni non conformi per questo tag), consigliamo di lasciare questa opzione deselezionata (impostazione predefinita) a meno che non si abbia esperienza con l'utilizzo delle policy di tag. Assicurati di aver esaminato i suggerimenti in Informazioni sull'applicazione ed effettua test accurati. In caso contrario, potresti impedire agli utenti degli account dell'organizzazione di applicare i tag alle risorse necessarie.

   Se desideri applicare la conformità con questa chiave di tag, seleziona la casella di controllo e quindi Specify resource types (Specifica i tipi di risorsa). Quando richiesto, seleziona i tipi di risorsa da includere nella policy. Selezionare quindi Save changes (Salva modifiche).

   > **Important**
   >
   > Quando selezioni questa opzione, tutte le operazioni che manipolano i tag per le risorse dei tipi specificati hanno esito positivo solo se l'operazione genera tag conformi alla policy.

9. (Opzionale) Per aggiungere un'altra chiave di tag a questa policy di tag, scegliere Add tag key (Aggiungi chiave di tag). Quindi esegui i passaggi da 6 a 9 per definire la chiave di tag.
10. Al termine della creazione della policy di tag, scegliere Save changes (Salva modifiche).

AWS CLI & AWS SDKs

Per creare una policy di tag

Puoi utilizzare una delle seguenti opzioni per creare una policy di tag:

- AWS CLI: create-policy

  Puoi usare qualsiasi editor di testo per creare la policy di tag. Usa la sintassi JSON e salva la policy di tag come file con qualsiasi nome ed estensione in una posizione a tua scelta. Le policy di tag possono avere un massimo di 2.500 caratteri, spazi inclusi. Per informazioni sulla sintassi delle policy di tag, consulta Sintassi delle policy di tag.

  Per creare una policy di tag

  1. Crea una policy di tag in un file di testo simile alla seguente:

Contenuto di `testpolicy.json`.

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            }
        }
    }
}
```

Questa policy di tag definisce la chiave di tag `CostCenter`. Il tag può accettare qualsiasi valore o nessun valore. Una policy come questa determina che una risorsa a cui è associato il tag CostCenter con o senza valore è conforme.

2. Crea una policy che contenga il contenuto della policy dal file. Lo spazio bianco extra nell'output è stato troncato per motivi di leggibilità.

```
$ aws organizations create-policy \
    --name "MyTestTagPolicy" \
    --description "My Test policy" \
    --content file://testpolicy.json \
    --type TAG_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-a1b2c3d4e5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-a1b2c3d4e5",
            "Name": "MyTestTagPolicy",
            "Description": "My Test policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign
\":\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

- SDK AWS: CreatePolicy

Cosa fare in seguito

Dopo aver creato una policy di tag, puoi rendere effettive le regole di tag. A tale scopo, collega la policy al root dell'organizzazione, alle unità organizzative, agli Account AWS all'interno dell'organizzazione o a una combinazione di entità dell'organizzazione.

Aggiornamento di una policy di tag

> **Autorizzazioni minime**
>
> Per aggiornare una policy di tag, è necessario disporre dell'autorizzazione per le seguenti operazioni:
>
> - `organizations:UpdatePolicy` con un elemento `Resource` nella stessa istruzione di policy che includa l'ARN della policy specificata (oppure "*")
> - `organizations:DescribePolicy` con un elemento `Resource` nella stessa istruzione di policy che includa l'ARN della policy specificata (oppure "*")

AWS Management Console

Per aggiornare una policy di tag

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. Nella pagina Tag policies (Policy di tag), scegli la policy di tag che desideri aggiornare.
3. Selezionare Edit policy (Modifica policy).
4. È possibile inserire nuovi valori per Policy name (Nome policy) e Policy descritpion (Descrizione della policy). È possibile modificare il contenuto della policy utilizzando Visual editor (Editor visivo) o modificando il JSON.
5. Al termine dell'aggiornamento della policy dei tag, scegliere Save changes (Salva modifiche).

AWS CLI & AWS SDKs

Per aggiornare una policy

Per aggiornare una policy, puoi utilizzare una delle seguenti opzioni:

- AWS CLI: update-policy

  Nell'esempio seguente viene rinominata una policy di tag.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed tag policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

  Nell'esempio seguente viene aggiunta o modificata la descrizione di una policy di tag.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new tag policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
       "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

Nell'esempio seguente viene modificato il documento della policy JSON collegato a una policy di rifiuto dei servizi di IA. In questo esempio, il contenuto viene preso da un file denominato `policy.json` con il testo seguente:

```
{
  "tags": {
    "Stage": {
      "tag_key": {
        "@@assign": "Stage"
      },
      "tag_value": {
        "@@assign": [
          "Production",
          "Test"
        ]
      }
    }
  }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"tags\":{\"Stage\":{\"tag_key\":{\"@@assign\":\"Stage
\"},\"tag_value\":{\"@@assign\":[\"Production\",\"Test\"]},\"enforced_for\":
{\"@@assign\":[\"ec2:instance\"]}}}}"
}
```

- SDK AWS: UpdatePolicy

Modifica dei tag collegati a una policy di tag

Quando effettui l'accesso all'account di gestione dell'organizzazione, puoi aggiungere o rimuovere i tag collegati a una policy di tag. Per farlo, completa le seguenti fasi.

Autorizzazioni minime

Per modificare i tag associati a una policy di tag nella tua organizzazione AWS, è necessario disporre delle seguenti autorizzazioni:

- `organizations:DescribeOrganization` (solo console - per passare alla policy)
- `organizations:DescribePolicy` (solo console - per passare alla policy)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Per modificare i tag collegati a una policy di rifiuto dei servizi di IA

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. Nella pagina Tag policies (Policy di tag), scegli il nome della policy con i tag che vuoi modificare.
3. Nella pagina dei dettagli della policy, scegli la scheda Tags, quindi scegli Manage tags (Gestisci tag).
4. In questa pagina puoi eseguire le seguenti operazioni:
   - Modifica il valore di un tag inserendo un nuovo valore rispetto a quello precedente. Non è possibile modificare la chiave. Per cambiare una chiave, devi eliminare il tag con la vecchia chiave e aggiungere un tag con la nuova chiave.
   - Rimuovi eventuali tag esistenti scegliendo Remove (Rimuovi).
   - Aggiungi una nuova coppia chiave e valore di tag. Scegli Add tag (Aggiungi tag), quindi inserisci il nuovo nome della chiave e il valore facoltativo nelle caselle fornite. Se lasci vuota la casella Value (Valore), il valore è una stringa vuota; non è `null`.

5. Scegli Save changes (Salva le modifiche) dopo avere apportato tutte le aggiunte, le rimozioni e le modifiche opportune.

AWS CLI & AWS SDKs

Per modificare i tag associati a una policy di tag

Per modificare i tag associati a una policy di tag puoi utilizzare uno dei seguenti comandi:

- AWS CLI: tag-resource e untag-resource
- SDK AWS: TagResource e UntagResource

Eliminazione di una policy di tag

Quando effettui l'accesso all'account di gestione della tua organizzazione, puoi eliminare una policy di cui non hai più bisogno nella tua organizzazione.

Prima di poter eliminare una policy, devi distaccarla da tutte le entità collegate.

> **Autorizzazioni minime**
>
> Per eliminare una policy di tag, è necessaria l'autorizzazione per la seguente operazione:
>
> - `organizations:DeletePolicy`

AWS Management Console

Per eliminare una policy di tag

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.
3. Nella pagina Tag policies (Policy di tag), sceglie la policy di tag che desideri eliminare.
4. È necessario che la policy da scollegare venga prima eliminata da tutti i root, le UO e gli account. Seleziona la scheda Targets (Destinazioni), scegli il pulsante di opzione accanto a ciascun root, UO o account visualizzato nell'elenco Targets e scegli Detach (Scollega). Nella finestra di dialogo di conferma, scegli Detach (Scollega).

5. Nella parte superiore della pagina, seleziona Delete (Elimina).
6. Nella finestra di dialogo di conferma, inserisci il nome della policy, quindi scegli Delete (Elimina).

AWS CLI & AWS SDKs

Per eliminare una policy di tag

Per eliminare una policy, puoi utilizzare una delle seguenti opzioni:

- AWS CLI: delete-policy

  Nell'esempio seguente viene eliminata la policy specificata. Funziona solo se la policy non è collegata a un root, un'UO o un account.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Questo comando non produce alcun output se ha esito positivo.
- SDK AWS: DeletePolicy

Collegamento e scollegamento delle policy di tag

Puoi utilizzare le policy di tag su un'intera organizzazione, sulle unità organizzative e sui singoli account.

- Quando colleghi una policy di tag alla root dell'organizzazione, la policy di tag si applica a tutte le unità organizzative e agli account membri della root.
- Quando colleghi una policy di tag a un'unità organizzativa, la policy viene applicata agli account che appartengono all'unità organizzativa. Questi account sono soggetti anche a qualsiasi policy di tag collegata alla root dell'organizzazione.
- Quando colleghi una policy di tag a un account, la policy viene applicata all'account. Inoltre, l'account è soggetto a qualsiasi policy di tag collegata alla root dell'organizzazione, oltre a qualsiasi policy di tag collegata a un'unità organizzativa a cui appartiene l'account.

L'aggregazione di tutte le policy di tag ereditate dall'account, oltre a qualsiasi policy di tag direttamente collegata all'account è la policy di tag operativa. Per ulteriori informazioni, consulta Comprendere l'ereditarietà delle policy di gestione.

> **Important**
>
> Le risorse senza tag non appaiono nei risultati come non conformi.

> **Autorizzazioni minime**
>
> Per collegare le policy di tag, è necessaria l'autorizzazione per la seguente operazione:
>
> - `organizations:AttachPolicy`

AWS Management Console

Puoi collegare una policy di tag accedendo alla policy oppure al root, all'unità organizzativa o all'account a cui vuoi collegare la policy.

Per collegare una policy di tag passando dal root, un'unità organizzativa o un 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. Nella pagina Account AWS, individua e scegli il nome del root, dell'unità organizzativa o dell'account a cui desideri collegare una policy. Potrebbe essere necessario espandere le UO (scegli l'opzione ▶) per individuare l'UO o l'account desiderato.
3. Nella scheda Policies (Policy), alla voce per Tag policies (Policy di tag), scegli Attach (Collega).
4. Individua la policy desiderata e scegli Attach policy (Collega policy).

   L'elenco delle policy di tag collegate nella scheda Policies (Policy) viene aggiornato per includere la nuova aggiunta. La modifica della policy diventa immediatamente effettiva.

Per collegare una policy di tag passando dalla policy

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. Nella pagina Tag policies (Policy di tag), scegli il nome della policy che desideri collegare.
3. Nella scheda Targets (Destinazioni), scegli Attach (Collega).
4. Scegli il pulsante di opzione accanto al root, all'unità organizzativa o all'account a cui vuoi collegare la policy. Potrebbe essere necessario espandere le UO (scegli l'opzione ) per individuare l'UO o l'account desiderato.
5. Scegli Attach policy (Collega policy).

   L'elenco delle policy di tag collegate nella scheda Targets (Destinazioni) viene aggiornato per includere la nuova aggiunta. La modifica della policy diventa immediatamente effettiva.

AWS CLI & AWS SDKs

Per collegare una policy di tag al root dell'organizzazione, a un'unità organizzativa o un account

Per collegare una policy di tag, puoi utilizzare una delle seguenti opzioni:

- AWS CLI: attach-policy

  Nella procedura seguente viene illustrato come collegare la policy di tag appena creata a un singolo account di test.

  - Collega la policy di tag all'account di test eseguendo un comando simile al seguente:

    ```
    $ aws organizations attach-policy \
        --target-id <account-id> \
        --policy-id p-a1b2c3d4e5
    ```

    Questo comando non restituisce alcun output se ha esito positivo.
- SDK AWS: AttachPolicy

La modifica della policy diventa immediatamente effettiva.

Cosa fare in seguito

Dopo avere collegato una policy di tag, puoi verificare quanto le tue risorse sono conformi con la policy di tag. A tale scopo, utilizza la console Resource Groups. Per informazioni, consulta l'argomento relativo alla valutazione della conformità di un account nella Guida per l'utente di AWS Resource Groups.

Scollegamento di una policy di tag

Quando effettui l'accesso all'account di gestione della tua organizzazione, puoi scollegare una policy di tag dal root, dall'unità organizzativa o dall'account a cui è collegata. Dopo avere scollegato una policy di tag da un'entità, quella policy non si applica più ad alcun account interessato dall'entità ora scollegata. Per distaccare una policy, completa le fasi seguenti.

> **Autorizzazioni minime**
>
> Per scollegare una policy di tag dalla root dell'organizzazione, dall'unità organizzativa o dall'account, è necessaria l'autorizzazione per la seguente operazione:
>
> - `organizations:DetachPolicy`

AWS Management Console

Per scollegare una policy di tag, puoi accedere alla policy oppure al root, all'unità organizzativa o all'account da cui vuoi scollegare la policy.

Per scollegare una policy di tag passando dal root, dall'unità organizzativa o da un account a cui è collegata

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. Nella pagina Account AWS individua il root, l'unità organizzativa o l'account da cui desideri scollegare una policy. Potrebbe essere necessario espandere le UO (scegli l'opzione ▶) per individuare l'UO o l'account desiderato. Scegli il nome del root, dell'unità organizzativa o dell'account.
3. Nella scheda Policies (Policy), scegli il pulsante di opzione accanto alla policy di tag che desideri scollegare, quindi scegli Detach (Scollega).

4. Nella finestra di dialogo di conferma, scegli Detach policy (Scollega policy).

   L'elenco delle policy di tag collegate viene aggiornato. La modifica della policy diventa immediatamente effettiva.

Per scollegare una policy di tag passando dalla policy

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. Nella pagina Tag policies (Policy di tag), scegli il nome della policy che vuoi scollegare da un root, un'UO o un account.
3. Nella scheda Targets (Destinazioni), scegli il pulsante di opzione accanto al root, all'unità organizzativa o all'account da cui vuoi scollegare la policy. Potrebbe essere necessario espandere le UO (scegli l'opzione ) per individuare l'UO o l'account desiderato.
4. Seleziona Detach (Scollega).
5. Nella finestra di dialogo di conferma, scegli Detach (Scollega).

   L'elenco delle policy di tag collegate viene aggiornato. La modifica della policy diventa immediatamente effettiva.

AWS CLI & AWS SDKs

Per scollegare una policy di tag dal root dell'organizzazione, da un'unità organizzativa o da un account

Per scollegare una policy di tag, puoi utilizzare una delle seguenti opzioni:

- AWS CLI: detach-policy
- SDK AWS: DetachPolicy

La modifica della policy diventa immediatamente effettiva.

Visualizzazione delle policy di tag operative

Prima di iniziare a controllare lo stato di conformità per le risorse con tag in un account, è utile determinare innanzitutto la policy di tag operativa per un account.

Qual è la policy di tag operativa?

La policy di tag operativa specifica le regole di tag applicabili a un account. È l'aggregazione di tutte le policy di tag ereditate dall'account, oltre a qualsiasi policy di tag direttamente collegata all'account. Quando colleghi una policy di tag alla root dell'organizzazione, questa si applica a tutti gli account dell'organizzazione. Quando colleghi una policy di tag a un'unità organizzativa, questa si applica a tutti gli account e alle unità organizzative appartenenti all'unità organizzativa.

Ad esempio, la policy di tag collegata al root dell'organizzazione può definire un tag `CostCenter` con quattro valori conformi. Una policy di tag separata collegata all'account può limitare la chiave `CostCenter` a soli due dei quattro valori conformi. La combinazione di queste policy di tag costituisce la policy di tag operativa. Il risultato è che solo due dei quattro valori di tag conformi definiti nella policy del tag root dell'organizzazione sono conformi per l'account.

Per ulteriori informazioni ed esempi più avanzati di come vengono generate le policy di tag operative, consulta Comprendere l'ereditarietà delle policy di gestione.

Come visualizzare la policy di tag operativa

Puoi visualizzare la policy di tag operativa per un account dalla AWS Management Console, dall'API AWS o l'AWS Command Line Interface.

> **Autorizzazioni minime**
>
> Per visualizzare la policy di tag operativa per un account, è necessario disporre dell'autorizzazione per le seguenti operazioni:
>
> - `organizations:DescribeEffectivePolicy`
> - `organizations:DescribeOrganization`

AWS Management Console

Per visualizzare la policy di tag effettiva per un 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. Nella pagina Account AWS, scegli il nome dell'account per il quale desideri visualizzare la policy di tag effettiva. Potrebbe essere necessario espandere le UO (scegli l'opzione ▶) per individuare l'account desiderato.
3. Nella scheda Policies (Policy), nella sezione Tag policies (Policy di tag), scegli View the effective tag policy for this (Visualizza la policy di tag effettiva per questo) Account AWS.

   Nella console viene visualizzata la policy effettiva applicata all'account specificato.

   > **Note**
   >
   > Non è possibile copiare e incollare una policy effettiva e utilizzarla come JSON per un'altra policy di tag senza modifiche significative. I documenti della policy di tag devono includere gli operatori di ereditarietà che specificano la modalità di unione di ciascuna impostazione nella policy effettiva finale.

AWS CLI & AWS SDKs

Per visualizzare la policy di tag effettiva per un account

Puoi utilizzare una delle seguenti opzioni per visualizzare la policy di tag operativa:

- AWS CLI: describe-effective-policy

  Per determinare quali regole di assegnazione di tag sono ereditate da o collegate a un account, esegui le operazioni indicate di seguito dall'account e salva i risultati in un file:

```
$ aws organizations describe-effective-policy \
    --policy-type TAG_POLICY
{
    "EffectivePolicy": {
```

```
        "PolicyContent": "{\"tags\":{\"costcenter\":{\"tag_value\":[\"*\"],
\"tag_key\":\"CostCenter\"}}}",
        "LastUpdatedTimestamp": "2020-06-09T08:34:25.103000-07:00",
        "TargetId": "123456789012",
        "PolicyType": "TAG_POLICY"
    }
}
```

Se una policy di tag è collegata all'account e al root o una o più UO, la combinazione di tutte le policy ereditate definisce la policy di tag effettiva dell'account. In questi casi, l'esecuzione di `describe-effective-policy` dall'account restituisce il contenuto unito di tutte le policy di tag nella gerarchia dell'account.

- SDK AWS: DescribeEffectivePolicy

Utilizzo di Amazon EventBridge per monitorare i tag non conformi

Puoi utilizzare Amazon EventBridge, precedentemente Eventi Amazon CloudWatch per monitorare quando vengono introdotti tag non conformi. Nel seguente evento di esempio, il valore `"false"` per `tag-policy-compliant` indica che un nuovo tag non è conforme alla policy di tag operativa.

```
{
  "detail-type": "Tag Change on Resource",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "a-new-key"
    ],
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
    "tag-policy-compliant": "false",
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added"
    }
  }
}
```

Puoi sottoscrivere eventi e specificare stringhe o modelli da monitorare. Per ulteriori informazioni su EventBridge consulta la Guida per l'utente di Amazon EventBridge.

Informazioni sull'applicazione

Una policy di tag può specificare che le operazioni di tag non conformi vengono applicate su tipi di risorse specifici. In altre parole, le richieste di tag non conformi su tipi di risorse specifici non possono essere completate.

> **Important**
>
> L'applicazione non ha alcun effetto sulle risorse create senza tag.

Per applicare la conformità alle policy di tag, eseguire una delle seguenti operazioni quando si crea una policy di tag:

- Dalla scheda Visual editor (Editor visivo) selezionare Prevent noncompliant operations for this tag (Impedisci operazioni non conformi per questo tag).
- Dalla scheda JSON utilizzare il campo `enforced_for`. Per informazioni sulla sintassi delle policy di tag, consultare Sintassi ed esempi delle policy di tag.

Segui queste best practice per applicare la conformità alle policy di tag:

- Usa cautela nell'applicare la conformità - Assicurati di aver compreso gli effetti dell'utilizzo delle policy di tag e segui i flussi di lavoro raccomandati descritti in Nozioni di base sulle policy di tag. Verifica il funzionamento dell'applicazione in un account di test prima di espanderla a più account. In caso contrario, potresti impedire agli utenti degli account dell'organizzazione di applicare i tag alle risorse necessarie.
- Tieni presente a quali tipi di risorse è possibile applicare la conformità - Puoi applicare la conformità solo alle policy di tag per i tipi di risorse supportati. I tipi di risorse che supportano l'applicazione della conformità vengono elencati quando utilizzi l'editor visivo per creare una policy di tag.
- Comprendi le interazioni con alcuni servizi - Alcuni servizi AWS dispongono di raggruppamenti di risorse simili a container che creano automaticamente risorse per tuo conto, e i tag possono propagarsi da una risorsa in un servizio a un altro. Ad esempio, i tag nei gruppi Amazon EC2 Auto Scaling e nei cluster Amazon EMR possono essere propagati automaticamente nelle istanze Amazon EC2 contenute. Potresti avere policy di tag per Amazon EC2 più rigorose rispetto ai gruppi

Auto Scaling o ai cluster EMR. Se abiliti l'applicazione, la policy di tag impedisce l'applicazione di tag alle risorse e potrebbe bloccare il dimensionamento dinamico e il provisioning.

Nelle sezioni seguenti viene illustrato come trovare risorse non conformi e correggerle in modo che siano conformi.

Ricerca di risorse non conformi per un account

Per ogni account puoi ottenere le informazioni sulle risorse non conformi. Puoi eseguire questo comando da ogni regione in cui l'account dispone di risorse.

Per trovare le risorse non conformi per un account che utilizza la policy di tag, esegui quanto indicato di seguito quando effettui l'accesso all'account e salva i risultati in un file:

```
$ aws resourcegroupstaggingapi get-resources  --region us-east-1 \
    --include-compliance-details \
    --exclude-compliant-resources > outputfile.txt
```

Correzione di tag non conformi nelle risorse

Dopo aver trovato i tag non conformi, apporta le correzioni utilizzando uno dei metodi descritti di seguito. Devi accedere all'account con la risorsa con tag non conformi:

- Utilizza la console o le operazioni API del servizio AWS che hanno creato le risorse non conformi.
- Utilizza le operazioni di AWS Resource Groups TagResources e UntagResources per aggiungere i tag conformi con la policy effettiva o per rimuovere i tag non conformi.

Individuazione e correzione di ulteriori problemi di non conformità

L'individuazione e la correzione dei problemi di conformità è un processo iterativo. Ripeti i passaggi nelle due sezioni precedenti fino a quando le risorse che ti interessano non siano conformi con la policy di tag.

Generazione di un report di conformità a livello di organizzazione

In qualsiasi momento puoi generare un report che elenca tutte le risorse con tag negli Account AWS dell'organizzazione. Il report mostra se ogni risorsa è conforme alla policy di tag operativa. Tieni presente che le modifiche apportate a una policy di tag o alle risorse possono impiegare fino a 48 ore prima di essere riportate nel report di conformità a livello di organizzazione. Ad esempio, supponi di avere una policy di tag che definisce un nuovo tag standardizzato per un tipo di risorsa. Le risorse

di quel tipo che non dispongono di questo tag vengono mostrate come conformi nel report per un massimo di 48 ore.

Puoi generare il report dall'account di gestione dell'organizzazione nella Regione `us-east-1`, a condizione che abbia accesso a un bucket Amazon S3. Il bucket deve essere collegato a una policy di bucket, come descritto in Policy dei bucket Amazon S3 per l'archiviazione del report. Per generare il report, esegui il comando seguente:

```
$ aws resourcegroupstaggingapi get-compliance-summary --region us-east-1
{
    "SummaryList": [
        {
            "LastUpdated": "2020-06-09T18:40:46Z",
            "NonCompliantResources": 0
        }
    ]
}
```

Puoi generare un report alla volta.

Il completamento del report potrebbe richiedere del tempo. Puoi controllare lo stato eseguendo il seguente comando:

```
$ aws resourcegroupstaggingapi describe-report-creation --region us-east-1
{
    "Status": "SUCCEEDED"
}
```

Quando il comando precedente restituisce `SUCCEEDED`, puoi aprire il report dal bucket Amazon S3.

Servizi e tipi di risorse che supportano l'applicazione

I seguenti servizi e tipi di risorse supportano l'applicazione con le policy di tag:

Nome servizio	Tipo di risorsa	Sintassi JSON
Amazon API Gateway	• Chiavi API • Nomi di dominio • Operazioni REST API	• `"apigateway:apikeys"` • `"apigateway:domainnames"` • `"apigateway:restapis"` • `"apigateway:restapis/stages"`

Nome servizio	Tipo di risorsa	Sintassi JSON
	• Stage	
AWS Amplify	• Componente • Tema	• `"amplifyuibuilder:app/environment/components"` • `"amplifyuibuilder:app/environment/themes"`
AWS AppConfig	• Applicazione • Profilo di configurazione • Implementazione • Strategia di distribuzione • Ambiente	• `"appconfig:application"` • `"appconfig:application/configurationprofile"` • `"appconfig:application/environment/deployment"` • `"appconfig:deploymentstrategy"` • `"appconfig:application/environment"`
AWS App Mesh	• Tutti • Instradamento gateway • Mesh • Route • Gateway virtuale • Nodo virtuale • Router virtuale • Servizio virtuale	• `"appmesh:*"` • `"appmesh:mesh/virtualGateway/gatewayRoute"` • `"appmesh:mesh"` • `"appmesh:mesh/virtualRouter/route"` • `"appmesh:mesh/virtualGateway"` • `"appmesh:mesh/virtualNode"` • `"appmesh:mesh/virtualRouter"` • `"appmesh:mesh/virtualService"`
Amazon Athena	• Tutti • Gruppo di lavoro	• `"athena:*"` • `"athena:workgroup"`

Nome servizio	Tipo di risorsa	Sintassi JSON
AWS Audit Manager	• Valutazione • Framework della valutazione • Controllo	• `"auditmanager:assessment "` • `"auditmanager:assessmentFramework "` • `"auditmanager:control "`
AWS Backup	• Piano di backup • Vault • Gateway • Hypervisor • VM	• `"backup:backup-plan"` • `"backup:backup-vault"` • `"backup-gateway:gateway"` • `"backup-gateway:hypervisor"` • `"backup-gateway:vm"`
AWS Batch	• Processo • Definizione processo • Coda processo	• `"batch:job"` • `"batch:job-definition"` • `"batch:job-queue"`
AWS BugBust	• Evento	• `"bugbust:event"`
AWS Certificate Manager	• Tutti • Certificati • Private Certificate Authority	• `"acm:*"` • `"acm:certificate"` • `"acm-pca:certificate-authority"`

Nome servizio	Tipo di risorsa	Sintassi JSON
Amazon Chime	• Istanza dell'applicazione • Canale • Pipeline multimediale • Riunione • Applicazioni multimediali SIP • Istanza dell'applicazione dell'utente • Connettore vocale	• `"chime:app-instance"` • `"chime:app-instance/channel"` • `"chime:media-pipeline"` • `"chime:meeting"` • `"chime:sma"` • `"chime:app-instance/user"` • `"chime:vc"`
AWS Clean Rooms	• Collaborazione • Tabella configurata • Appartenenza • Associazione della tabella configurata	• `"cleanrooms:collaboration"` • `"cleanrooms:configuredtable"` • `"cleanrooms:membership"` • `"cleanrooms:membership/configuredtableassociation"`
AWS Cloud9	• Ambiente	• `"cloud9:environment"`
Amazon CloudFront	• Tutti • Distribuzione • Distribuzione in streaming	• `"cloudfront:*"` • `"cloudfront:distribution"` • `"cloudfront:streaming-distribution"`
AWS CloudTrail	• Tutti • Trail	• `"cloudtrail:*"` • `"cloudtrail:trail"`

Nome servizio	Tipo di risorsa	Sintassi JSON
Amazon CloudWatch	• Tutti • Allarme • Regole di Contributor Insights • Flusso del parametro	• `"cloudwatch:*"` • `"cloudwatch:alarm"` • `"cloudwatch:insight-rule"` • `"cloudwatch:metric-stream"`
Amazon CloudWatch Internet Monitor	• Monitoraggio	• `"internetmonitor:monitor"`
CloudWatch Registri Amazon	• Gruppo di log	• `"logs:log-group"`
Amazon CloudWatch Observability Access Manager	• Link • Sink	• `"oam:link"` • `"oam:sink"`
AWS CodeBuild	• Tutti • Progetto	• `"codebuild:*"` • `"codebuild:project"`
Amazon CodeCatalyst	• Connessioni	• `"codecatalyst:connections"`
AWS CodeCommit	• Tutti • Repository	• `"codecommit:*"` • `"codecommit:repository"`
AWS CodePipeline	• Tutti • Tipo di operazione • Pipeline • Webhook	• `"codepipeline:*"` • `"codepipeline:actiontype"` • `"codepipeline:pipeline"` • `"codepipeline:webhook"`
Amazon Cognito Identity	• Tutti • Pool di identità	• `"cognito-identity:*"` • `"cognito-identity:identitypool"`

Nome servizio	Tipo di risorsa	Sintassi JSON
Pool di utenti Amazon Cognito	• Tutti • Bacino d'utenza	• `"cognito-idp:*"` • `"cognito-idp:userpool"`
Amazon Comprehend	• Tutti • Classificatore di documenti • Riconoscimento delle entità	• `"comprehend:*"` • `"comprehend:document-classifier"` • `"comprehend:entity-recognizer"`
AWS Config	• Tutti • Autorizzazione dell'aggregazione • Aggregatore di configurazione • Regola di configurazione	• `"config:*"` • `"config:aggregation-authorization"` • `"config:config-aggregator"` • `"config:config-rule"`
CodeGuru Revisore Amazon	• Associazione	• `"codeguru-reviewer:association"`
CodeGuru Sicurezza Amazon	• Scan	• `"codeguru-security:scans"`
CodeConnections	• Connessione • Host	• `"codestar-connections:connection"` • `"codestar-connections:host"`

Nome servizio	Tipo di risorsa	Sintassi JSON
Amazon Connect	• Flusso di contatto • Associazione di integrazione • Queue • Connessione rapida • Profilo di routing • Utente	• `"connect:instance/contact-flow"` • `"connect:instance/integration-association"` • `"connect:instance/queue"` • `"connect:instance/transfer-destination"` • `"connect:instance/routing-profile"` • `"connect:instance/agent"`
Amazon Connect Wisdom	• Assistente • Associazione • Contenuti • Knowledge Base • Sessione	• `"wisdom:assistant"` • `"wisdom:association"` • `"wisdom:content"` • `"wisdom:knowledge-base"` • `"wisdom:session"`
AWS Database Migration Service	• Tutti • Endpoint • ES • Rep • Subgrp • Attività	• `"dms:*"` • `"dms:endpoint"` • `"dms:es"` • `"dms:rep"` • `"dms:subgrp"` • `"dms:task"`
Amazon Data Lifecycle Manager	• Policy	• `"dlm:policy"`
AWS Direct Connect	• Tutti • Dxcon • Dxlag • Dxvif	• `"directconnect:*"` • `"directconnect:dxcon"` • `"directconnect:dxlag"` • `"directconnect:dxvif"`

Nome servizio	Tipo di risorsa	Sintassi JSON
Amazon DynamoDB	• Tutti • Tabella	• `"dynamodb:*"` • `"dynamodb:table"`

Nome servizio	Tipo di risorsa	Sintassi JSON
Amazon EC2	• Prenotazione di capacità • Endpoint Client VPN • Gateway del cliente • Opzioni DHCP • IP elastico • Parco istanze • Immagine FPGA • Prenotazione host • Immagine • Istanza • Internet Gateway • Modello di avvio • Gateway NAT • Lista di controllo degli accessi di rete • Interfaccia di rete • Istanze riservate • Tabella di routing • Gruppo di sicurezza • Snapshot • Richiesta di istanze spot • Sottorete • Filtro di mirroring del traffico • Sessione di mirroring del traffico	• `"ec2:capacity-reservation"` • `"ec2:client-vpn-endpoint"` • `"ec2:customer-gateway"` • `"ec2:dhcp-options"` • `"ec2:elastic-ip"` • `"ec2:fleet"` • `"ec2:fpga-image"` • `"ec2:host-reservation"` • `"ec2:image"` • `"ec2:instance"` • `"ec2:internet-gateway"` • `"ec2:launch-template"` • `"ec2:natgateway"` • `"ec2:network-acl"` • `"ec2:network-interface"` • `"ec2:reserved-instances"` • `"ec2:route-table"` • `"ec2:security-group"` • `"ec2:snapshot"` • `"ec2:spot-instances-request"` • `"ec2:subnet"` • `"ec2:traffic-mirror-filter"` • `"ec2:traffic-mirror-session"` • `"ec2:traffic-mirror-target"` • `"ec2:volume"` • `"ec2:vpc"` • `"ec2:vpc-endpoint"` • `"ec2:vpc-endpoint-service"` • `"ec2:vpc-peering-connection"`

Nome servizio	Tipo di risorsa	Sintassi JSON
	• Destinazione di mirroring del traffico • Volume • VPC • Endpoint VPC • Servizio endpoint VPC • Connessione di peering di VPC • Connessione VPN • Gateway VPN	• `"ec2:vpn-connection"` • `"ec2:vpn-gateway"`
Cestino di riciclaggio Amazon EC2	• Regola	• `"rbin:rule"`
Amazon Elastic Container Registry	• Repository	• `"ecr:repository"`
AWS Elastic Beanstalk	• Applicazione • Versione dell'applicazione • Modello di configurazione • Piattaforma	• `"elasticbeanstalk:application"` • `"elasticbeanstalk:applicationversion"` • `"elasticbeanstalk:configurationtemplate"` • `"elasticbeanstalk:platform"`
Amazon Elastic Container Service	• Cluster • Servizio • Set di attività	• `"ecs:cluster"` • `"ecs:service"` • `"ecs:task-set"`
Amazon Elastic File System	• Tutti • File system	• `"elasticfilesystem:*"` • `"elasticfilesystem:file-system"`

Nome servizio	Tipo di risorsa	Sintassi JSON
Amazon Elastic Inference	• Accelerator	• `"elastic-inference:elastic-inference-accelerator"`
Amazon Elastic Kubernetes Service	• Cluster	• `"eks:cluster"`
Amazon Elastic Search	• Domain	• `"es:domain"`
Amazon EMR	• Cluster • Editor	• `"elasticmapreduce:cluster"` • `"elasticmapreduce:editor"`
Amazon EMR Serverless	• Applicazione	• `"emr-serverless:applications"`
AWS Risoluzione dell'entità	• Flusso di lavoro corrispondente • Mappatura dello schema	• `"entityresolution:matchingworkflow"` • `"entityresolution:schemamapping"`
Amazon ElastiCache	• Cluster	• `"elasticache:cluster"`
Amazon EventBridge	• Tutti • Router di eventi • Regola	• `"events:*"` • `"events:event-bus"` • `"events:rule"`
EventBridge Tubi Amazon	• Pipeline	• `"pipes:pipe"`
Amazon EventBridge Scheduler	• Gruppo di pianificazione	• `"scheduler:schedule-group"`

Nome servizio	Tipo di risorsa	Sintassi JSON
Amazon Fraud Detector	• Rilevatore • Versione del rilevatore • Modello • Regola • Variabile	• `"frauddetector:detector"` • `"frauddetector:detector-version"` • `"frauddetector:model"` • `"frauddetector:rule"` • `"frauddetector:variable"`
Amazon Global Accelerator	• Accelerator	• `"globalaccelerator:accelerator"`
Sistema di bilanciamento del carico elastico	• Tutti • Sistema di bilanciamento del carico (load balancer) • Gruppo di destinazione	• `"elasticloadbalancing:*"` • `"elasticloadbalancing:loadbalancer"` • `"elasticloadbalancing:targetgroup"`
Amazon FSx	• Tutti • Backup • File system	• `"fsx:*"` • `"fsx:backup"` • `"fsx:file-system"`
Amazon GuardDuty	• Rilevatore • Filtro • Set di IP • Set di intelligence delle minacce	• `"guardduty:detector"` • `"guardduty:detector/filter"` • `"guardduty:detector/ipset"` • `"guardduty:detector/threatintelset"`
AWS HealthLake	• Datastore	• `"healthlake:datastore  "`

Nome servizio	Tipo di risorsa	Sintassi JSON
AWS HealthOmics	• Archivio di annotazioni • Versione dell'archivio di annotazioni • Archivio di riferimenti • Documentazione di riferimento • Esecuzione • Gruppo di esecuzioni • Archivio di sequenze • Set di lettura • Archivio di varianti • Flusso di lavoro	• `"omics:annotationStore"` • `"omics:annotationStore/version"` • `"omics:referenceStore"` • `"omics:referenceStore/reference"` • `"omics:run"` • `"omics:runGroup"` • `"omics:sequenceStore"` • `"omics:sequenceStore/readSet"` • `"omics:variantStore"` • `"omics:workflow"`
Amazon Inspector	• Filtro	• `"inspector2:filter "`
AWS Identity and Access Management	• Profilo dell'istanza • MFA • Provider OIDC • Policy • Provider SAML • Certificato del server	• `"iam:instance-profile"` • `"iam:mfa"` • `"iam:oidc-provider"` • `"iam:policy"` • `"iam:saml-provider"` • `"iam:server-certificate"`

Nome servizio	Tipo di risorsa	Sintassi JSON
AWS IoT Analytics	• Tutti • Canale • Set di dati • Datastore • Pipeline	• `"iotanalytics:*"` • `"iotanalytics:channel"` • `"iotanalytics:dataset"` • `"iotanalytics:datastore"` • `"iotanalytics:pipeline"`
AWS IoT Events	• Tutti • Modello di rilevatore • Input	• `"iotevents:*"` • `"iotevents:detectorModel"` • `"iotevents:input"`
AWS IoT Fleet Hub	• Applicazione	• `"iotfleethub:application"`
AWS IoT SiteWise	• Asset • Modello di asset	• `"iotsitewise:asset"` • `"iotsitewise:asset-model  "`
AWS IoT Greengrass	• Distribuzione in blocco • Definizione di un connettore • Definizione di base • Definizione di dispositivo • Definizione della funzione • Definizione del logger • Definizioni di risorsa • Definizione di sottoscrizione	• `"greengrass:bulk"` • `"greengrass:connectorsDefinition"` • `"greengrass:coresDefinition"` • `"greengrass:devicesDefinition"` • `"greengrass:functionsDefinition"` • `"greengrass:loggersDefinition"` • `"greengrass:resourcesDefinition"` • `"greengrass:subscriptionsDefinition"`
AWS Key Management Service	• Tutti • Chiave	• `"kms:*"` • `"kms:key"`

Nome servizio	Tipo di risorsa	Sintassi JSON
Amazon Kinesis	• Tutti • Applicazione	• `"kinesisanalytics:*"` • `"kinesisanalytics:application"`
Amazon Data Firehose	• Tutti • Flusso di consegna	• `"firehose:*"` • `"firehose:deliverystream"`
AWS Lambda	• Tutti • Funzione	• `"lambda:*"` • `"lambda:function"`
Amazon Macie	• Identificatore dati personalizzato	• `"macie2:custom-data-identifier"`
Amazon MediaStore	• Container	• `"mediastore:container"`
Amazon MQ	• Broker • Configurazione	• `"mq:broker"` • `"mq:configuration"`
Amazon Network Firewall	• Firewall • Policy firewall • Gruppo di regole stateful • Gruppo di regole stateless	• `"network-firewall:firewall"` • `"network-firewall:firewall-policy"` • `"network-firewall:stateful-rulegroup"` • `"network-firewall:stateless-rulegroup"`
Amazon senza OpenSearch server	• Raccolta	• `"aoss:collection"`
AWS Organizations	• Account • Unità organizzativa • Policy • Root	• `"organizations:account"` • `"organizations:ou"` • `"organizations:policy"` • `"organizations:root"`

Nome servizio	Tipo di risorsa	Sintassi JSON
Amazon Pinpoint SMS Voice V2	• Set di configurazione • Elenco di esclusione • Numero di telefono • Pool • ID mittente	• `"sms-voice:configuration-set"` • `"sms-voice:opt-out-list"` • `"sms-voice:phone-number"` • `"sms-voice:pool"` • `"sms-voice:sender-id"`
Amazon RDS	• Cluster parameter group (Gruppo di parametri del cluster) • Endpoint del cluster • Sottoscrizione a eventi • Gruppo di opzioni database • DB parameter group (Gruppo di parametri database) • Proxy DB • Endpoint proxy DB • Istanza database riservata • Gruppo di sicurezza DB • DB subnet group (Gruppo di sottoreti DB) • Gruppo di destinazione	• `"rds:cluster-pg"` • `"rds:cluster-endpoint"` • `"rds:es"` • `"rds:og"` • `"rds:pg"` • `"rds:db-proxy"` • `"rds:db-proxy-endpoint"` • `"rds:ri"` • `"rds:secgrp"` • `"rds:subgrp"` • `"rds:target-group"`

Nome servizio	Tipo di risorsa	Sintassi JSON
Amazon Redshift	• Tutti • Cluster • Gruppo DB • Nome database • Utente DB • Sottoscrizione a eventi • Certificato client HSM • Configurazione HSM • Gruppo di parametri • Snapshot • Autorizzazione di copia degli snapshot • Pianificazione snapshot • Subnet group (Gruppo di sottoreti)	• `"redshift:*"` • `"redshift:cluster"` • `"redshift:dbgroup"` • `"redshift:dbname"` • `"redshift:dbuser"` • `"redshift:eventsubscription"` • `"redshift:hsmclientcertificate"` • `"redshift:hsmconfiguration"` • `"redshift:parametergroup"` • `"redshift:snapshot"` • `"redshift:snapshotcopygrant"` • `"redshift:snapshotschedule"` • `"redshift:subnetgroup"`
Amazon Redshift Serverless	• Spazio dei nomi • Gruppo di lavoro	• `"redshift-serverless:namespace"` • `"redshift-serverless:workgroup"`
AWS Resource Access Manager	• Tutti • Condivisione delle risorse	• `"ram:*"` • `"ram:resource-share"`
AWS Resource Groups	• Tutti • Group (Gruppo)	• `"resource-groups:*"` • `"resource-groups:group"`

Nome servizio	Tipo di risorsa	Sintassi JSON
Amazon Route 53	• Hosted zone	• `"route53:hostedzone"`
Amazon Route 53 Resolver	• Tutti • Endpoint del risolutore • Regola del risolutore	• `"route53resolver:*"` • `"route53resolver:resolver-endpoint"` • `"route53resolver:resolver-rule"`
Amazon S3	• Bucket • Storage Lens	• `"s3:bucket"` • `"s3:storage-lens"`
Amazon SageMaker	• App Image Config • Artifact • Context • Processo di formazione • Processo di elaborazione • Gruppo di pacchetti di modelli • UI delle attività umane • Pacchetto del modello • Azione • Pipeline • Esperimento • Definizione di flusso • Progetto	• `"sagemaker:app-image-config"` • `"sagemaker:artifact"` • `"sagemaker:context"` • `"sagemaker:training-job"` • `"sagemaker:processing-job "` • `"sagemaker:model-package-group"` • `"sagemaker:human-task-ui"` • `"sagemaker:model-package"` • `"sagemaker:action"` • `"sagemaker:pipeline"` • `"sagemaker:experiment"` • `"sagemaker:flow-definition"` • `"sagemaker:project"`
AWS Secrets Manager	• Tutti • Segreto	• `"secretsmanager:*"` • `"secretsmanager:secret"`

Nome servizio	Tipo di risorsa	Sintassi JSON
AWS Lago di sicurezza	• Data lake • Sottoscrittore	• `"securitylake:data-lake"` • `"securitylake:subscriber"`
AWS Service Catalog	• Applicazione • Gruppo di attributi • Portfolio • Product	• `"servicecatalog:applications"` • `"servicecatalog:attribute-groups "` • `"catalog:portfolio "` • `"catalog:product "`
Amazon Simple Notification Service (SNS)	• Argomento	• `"sns:topic"`
Amazon Simple Queue Service (SQS)	• Queue	• `"sqs:queue"`
Amazon States Language	• Tutti • Attività • Macchina a stati	• `"states:*"` • `"states:activity "` • `"states:stateMachine  "`
AWS Step Functions	• Attività	• `"states:activity"`
AWS Storage Gateway	• Tutti • Gateway • Condivisione • Nastro • Volume	• `"storagegateway:*"` • `"storagegateway:gateway"` • `"storagegateway:share"` • `"storagegateway:tape"` • `"storagegateway:gateway/volume"`

Nome servizio	Tipo di risorsa	Sintassi JSON
AWS Systems Manager	• Associazione • Esecuzione di automazione • Documento • Finestra di manutenzione • Istanza gestita • Elemento Ops • Base di patch • Sessione • Contatti	• `"ssm:association"` • `"ssm:automation-execution"` • `"ssm:document"` • `"ssm:maintenancewindow"` • `"ssm:managed-instance"` • `"ssm:opsitem"` • `"ssm:patchbaseline"` • `"ssm:session"` • `"ssm-contacts:contact"`
AWS Transfer Family	• Server • Utente • Flusso di lavoro	• `"transfer:server"` • `"transfer:user"` • `"transfer:workflow"`
Amazon Well-Arch itected	• Carico di lavoro	• `"wellarchitected:workload"`
AWS Wickr	• Rete	• `"wickr:network"`
Amazon WorkSpaces	• Tutti • Directory • WorkSpace • WorkSpaces pacchetto • WorkSpaces immagine • WorkSpaces gruppo IP	• `"workspaces:*"` • `"workspaces:directory"` • `"workspaces:workspace"` • `"workspaces:workspacebundle"` • `"workspaces:workspaceimage"` • `"workspaces:workspaceipgroup"`
Amazon WorkLink	• Parco istanze	• `"worklink:fleet"`

Sintassi ed esempi delle policy di tag

Questa pagina descrive la sintassi delle policy di tag e fornisce esempi.

Sintassi delle policy di tag

Una policy di tag è un file di testo normale strutturato in base alle regole di JSON. La sintassi per le policy di tag segue la sintassi per tutti i tipi di policy di gestione. Per una discussione completa di tale sintassi, consulta Comprendere l'ereditarietà delle policy di gestione. Questo argomento è incentrato sull'applicazione della sintassi generale ai requisiti specifici del tipo di policy di tag.

La seguente policy di tag mostra la sintassi della policy di tag di base:

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "100",
                    "200"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "secretsmanager:*"
                ]
            }
        }
    }
}
```

La sintassi della policy di tag include i seguenti elementi:

- Il nome della chiave di campo `tags`. Le policy di tag iniziano sempre con questo nome di chiave fisso. È la prima riga nella policy di esempio precedente.
- Una chiave della policy che identifica in modo univoco l'istruzione della policy. Deve corrispondere al valore per la chiave di tag, ad eccezione del trattamento lettere maiuscole o minuscole. A differenza della chiave di tag (descritta in seguito), il valore della policy non fa distinzione tra maiuscole e minuscole.

In questo esempio, `costcenter` è la chiave della policy.

- Almeno una chiave di tag che specifica la chiave di tag consentita con l'uso delle maiuscole e minuscole a cui desideri che le risorse siano conformi. Se il trattamento lettere maiuscole o minuscole non è definito, minuscole è il trattamento predefinito per le chiavi di tag. Il valore per la chiave di tag deve corrispondere al valore per la chiave della policy. Tuttavia, poiché il valore della chiave della policy non fa distinzione tra maiuscole e minuscole, l'uso delle maiuscole e delle minuscole può essere diverso.

  In questo esempio, `CostCenter` è la chiave di tag. Questo è il trattamento lettere maiuscole o minuscole che è richiesto per la conformità con la policy di tag. Le risorse con il trattamento alternativo lettere maiuscole o minuscole per questa chiave di tag non sono conformi con la policy di tag.

  In una policy di tag è possibile definire più chiavi di tag.

- (Facoltativo) Un elenco di uno o più valori di tag accettabili per la chiave di tag. Se la policy di tag non specifica un valore di tag per una chiave di tag, qualsiasi valore (incluso nessun valore) viene considerato conforme.

  In questo esempio, i valori accettabili per la chiave di tag `CostCenter` sono `100` e `200`.

- (Facoltativo) Un'opzione `enforced_for` che indica se impedire le operazioni di tag non conformi su servizi e risorse specificati. Nella console, questa è l'opzione Prevent noncompliant operations for this tag (Impedisci operazioni non conformi per questo tag) nell'editor visivo per la creazione di policy di tag. L'impostazione predefinita per questa opzione è null.

  La policy di tag di esempio specifica che tutte le risorse AWS Secrets Manager devono avere questo tag.

  > **Warning**
  >
  > Cambia l'impostazione predefinita di questa opzione solo se sei esperto dell'utilizzo delle policy di tag. In caso contrario, è possibile agli utenti degli account dell'organizzazione venga impedito di creare le risorse necessarie.

- Operatori che specificano il modo in cui la policy di tag si unisce con altre policy di tag all'interno dell'albero dell'organizzazione per creare la policy di tag operativa di un account. In questo esempio, `@@assign` viene utilizzato per assegnare le stringhe a `tag_key`, `tag_value` e `enforced_for`. Per ulteriori informazioni sugli operatori, consulta Operatori di ereditarietà.

- - Puoi utilizzare il carattere jolly * nei valori dei tag e nei campi `enforced_for`.
  - Puoi utilizzare solo un carattere jolly per ogni valore di tag. Ad esempio, `*@example.com` è consentito, mentre non lo è `*@*.com`.
  - Per `enforced_for`, è possibile utilizzare `<service>:*` con alcuni servizi per abilitare l'applicazione per tutte le risorse per tale servizio. Per un elenco dei servizi e dei tipi di risorse che supportano `enforced_for`, consultare Servizi e tipi di risorse che supportano l'applicazione.

    Non è possibile utilizzare un carattere jolly per specificare tutti i servizi o per specificare una risorsa per tutti i servizi.

Esempi di policy con tag

Le policy di tag di esempio che seguono sono solo a scopo informativo.

> **Note**
>
> Prima di tentare di utilizzare queste policy di tag di esempio nell'organizzazione, tieni presente quanto segue:
>
> - Assicurati di aver seguito il flusso di lavoro raccomandato per iniziare a utilizzare le policy di tag.
> - Esamina attentamente e personalizza queste policy di tag in base ai tuoi requisiti univoci.
> - Tutti i caratteri nella policy di tag sono soggetti a una dimensione massima. Gli esempi in questa guida mostrano le policy di tag formattate con spazio vuoto aggiuntivo per migliorarne la leggibilità. Tuttavia puoi eliminare qualsiasi spazio vuoto per risparmiare spazio, se la dimensione della policy si avvicina a quella massima. Esempi di spazio bianco includono gli spazi e le interruzioni di riga che sono al di fuori delle virgolette.
> - Le risorse senza tag non appaiono nei risultati come non conformi.

Esempio 1: definire l'uso delle maiuscole o minuscole per la chiave di tag a livello di organizzazione

Nell'esempio seguente viene illustrata una policy di tag che definisce solo due chiavi di tag e l'uso delle maiuscole e delle minuscole su cui si desidera che gli account dell'organizzazione vengano standardizzati.

Policy A: policy di tag della root dell'organizzazione

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        },
        "Project": {
            "tag_key": {
                "@@assign": "Project",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

Questa policy di tag definisce due chiavi tag: `CostCenter` e `Project`. Il collegamento di questa policy di tag alla root dell'organizzazione ha i seguenti effetti:

- Tutti gli account dell'organizzazione ereditano questa policy di tag.
- Tutti gli account dell'organizzazione devono utilizzare il trattamento lettere maiuscole o minuscole definito per la conformità. Le risorse con i tag `CostCenter` e `Project` sono conformi. Le risorse con il trattamento lettere maiuscole o minuscole alternativo per la chiave di tag (ad esempio `costcenter`, `Costcenter` o `COSTCENTER`) non sono conformi.
- Le righe `@@operators_allowed_for_child_policies": ["@@none"]` bloccano le chiavi di tag. Le policy di tag collegate a un livello inferiore nell'albero dell'organizzazione (policy figlio) non possono utilizzare gli operatori di impostazione del valore per modificare la chiave di tag, incluso il trattamento lettere maiuscole o minuscole.
- Nello stesso modo delle policy di tag, le risorse senza tag o i tag che non sono definiti nella policy di tag non vengono valutati per la conformità con la policy di tag.

AWS consiglia di utilizzare questo esempio come guida per la creazione di una policy di tag simile per le chiavi di tag che vuoi utilizzare. Collegala alla root dell'organizzazione. Quindi crea una policy di tag simile all'esempio successivo, che definisce solo i valori accettabili per le chiavi di tag definite.

Fase successiva: definizione dei valori

Supponiamo di aver collegato la policy di tag precedente alla root dell'organizzazione. Quindi ora è possibile creare un policy di tag come la seguente e collegarla a un account. Questa policy definisce i valori accettabili per le chiavi di tag `CostCenter` e `Project`.

Policy B: policy di tag dell'account

```
{
    "tags": {
        "CostCenter": {
            "tag_value": {
                "@@assign": [
                    "Production",
                    "Test"
                ]
            }
        },
        "Project": {
            "tag_value": {
                "@@assign": [
                    "A",
                    "B"
                ]
            }
        }
    }
}
```

Se colleghi la policy A alla root dell'organizzazione e la policy B a un account, le policy vengono combinate per creare la seguente policy di tag operativa per l'account:

Policy A+ Policy B = policy di tag operativa per l'account

```
{
    "tags": {
        "Project": {
            "tag_value": [
                "A",
                "B"
            ],
            "tag_key": "Project"
        },
```

```
        "CostCenter": {
            "tag_value": [
                "Production",
                "Test"
            ],
            "tag_key": "CostCenter"
        }
    }
}
```

Per ulteriori informazioni sull'ereditarietà delle policy, inclusi esempi di funzionamento degli operatori di ereditarietà e delle policy di tag operative, consulta Comprendere l'ereditarietà delle policy di gestione.

Esempio 2: impedire l'utilizzo di una chiave di tag

Per impedire l'utilizzo di una chiave di tag, è possibile collegare una policy di tag come la seguente a un'entità dell'organizzazione.

Questa policy di esempio specifica che nessun valore è accettabile per la chiave di tag `Color`. Specifica inoltre che nessun operatore è consentito nelle policy di tag figlio. Pertanto, eventuali tag `Color` sulle risorse negli account interessati sono considerati non conformi. Tuttavia, l'opzione `enforced_for` impedisce effettivamente agli account interessati di aggiungere un tag solo per le tabelle Amazon DynamoDB con il tag `Color`.

```
{
    "tags": {
        "Color": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": "Color"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": []
            },
            "enforced_for": {
                "@@assign": [
```

```
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

Regioni supportate

Le caratteristiche delle policy di tag sono disponibili nelle seguenti regioni:

Nome Regione	Parametro della regione
Regione Stati Uniti orientali (Virginia settentrionale)[1]	**us-east-1**
Stati Uniti orientali (Ohio)	us-east-2
Regione Stati Uniti occidentali (California settentrionale)	us-west-1
Stati Uniti occidentali (Oregon)	us-west-2
Regione Africa (Città del Capo)[2]	af-south-1
Regione Asia Pacifico (Hong Kong)[2]	ap-east-1
Regione Asia Pacifico (Mumbai)	ap-south-1
Asia Pacifico (Hyderabad) [2]	ap-south-2
Regione Asia Pacifico (Tokyo)	ap-northeast-1
Regione Asia Pacifico (Seoul)	ap-northeast-2
Regione Asia Pacifico (Osaka-Locale)	ap-northeast-3
Regione Asia Pacifico (Singapore)	ap-southeast-1
Regione Asia Pacifico (Sydney)	ap-southeast-2
Regione Asia Pacifico (Giacarta) [2]	ap-southeast-3
Asia Pacifico (Melbourne) [2]	ap-southeast-4

Nome Regione	Parametro della regione
Canada occidentale (Calgary) [2]	`ca-west-1`
Regione Canada (Centrale)	`ca-central-1`
Regione Europa (Francoforte)	`eu-central-1`
Regione Europa (Zurigo) [2]	`eu-central-2`
Regione Europa (Milano)[2]	`eu-south-1`
Europa (Spagna) [2]	`eu-south-2`
Regione Europa (Irlanda)	`eu-west-1`
Regione Europa (Londra)	`eu-west-2`
Regione Europa (Parigi)	`eu-west-3`
Regione Europa (Stoccolma)	`eu-north-1`
Regione del Medio Oriente (EAU) [2]	`me-central-1`
Regione Medio Oriente (Bahrein)[2]	`me-south-1`
Regione Sud America (San Paolo)	`sa-east-1`
Israele (Tel Aviv) [2]	`il-central-1`

[1]È necessario specificare la Regione **`us-east-1`** quando si chiamano le operazioni Organizations seguenti:

- DeletePolicy
- DisablePolicyType
- EnablePolicyType
- Qualsiasi altra operazione sulla radice di un'organizzazione, ad esempio ListRoots.

È inoltre necessario specificare la regione **`us-east-1`** quando si chiamano le seguenti operazioni API per l'applicazione di tag a gruppi di risorse che fanno parte della caratteristica delle policy di tag:

- DescribeReportCreation
- GetComplianceSummary
- GetResources
- StartReportCreation

> **Note**
>
> Per valutare la conformità a livello di organizzazione con le policy di tag, è necessario anche avere accesso a un bucket Amazon S3 nella Regione Stati Uniti orientali (Virginia settentrionale) per l'archiviazione dei report. Per ulteriori informazioni, consulta la policy sui bucket di Amazon S3 per l'archiviazione dei report nella Tagging AWS Resources User Guide.

[2]Queste Regioni devono essere abilitate manualmente. Per ulteriori informazioni sull'attivazione e la disabilitazione Regioni AWS, consulta Specificare quali dispositivi può utilizzare Regioni AWS il tuo account nella Guida di riferimento alla gestione degli AWS account. La console Resource Groups non è disponibile in queste Regioni.

Policy di controllo dei servizi (Service Control Policies, SCP)

Le policy di controllo dei servizi (SCP) sono un tipo di policy dell'organizzazione che puoi utilizzare per gestire le autorizzazioni nell'organizzazione. Gli SCP offrono il controllo centralizzato sulle autorizzazioni massime disponibili per gli utenti IAM e i ruoli IAM nell'organizzazione. Le SCP ti aiutano a garantire che i tuoi account rimangano all'interno delle linee guida per il controllo degli accessi della tua organizzazione. Le SCP sono disponibili solo nelle organizzazioni in cui sono abilitate tutte le caratteristiche. Le SCP non sono disponibili se la tua organizzazione ha abilitato solo le caratteristiche di fatturazione consolidata. Per istruzioni su come abilitare le SCP, consulta Abilitazione e disabilitazione di tipi di policy.

Gli SCP non concedono autorizzazioni agli utenti IAM e ai ruoli IAM dell'organizzazione. Nessuna autorizzazione viene concessa da una SCP. Un SCP definisce una barriera di autorizzazioni, o impone dei limiti, alle azioni che gli utenti IAM e i ruoli IAM dell'organizzazione possono eseguire.

Per concedere le autorizzazioni, l'amministratore deve allegare politiche per il controllo dell'accesso, ad esempio politiche basate sull'identità associate agli utenti e ai ruoli IAM e politiche basate sulle risorse allegate alle risorse dei tuoi account. Le autorizzazioni effettive sono l'intersezione logica tra ciò che è consentito da SCP e ciò che è consentito dalle politiche basate sull'identità e sulle risorse.

> **Important**
>
> Le SCP non influenzano gli utenti e i ruoli nell'account di gestione. Influiscono solo sugli account membri nell'organizzazione.

Argomenti in questa pagina

Test degli effetti delle SCP

AWS consiglia vivamente di non collegare gli SCP alla radice dell'organizzazione senza aver testato a fondo l'impatto che la politica ha sugli account. Piuttosto, crea una UO in cui puoi spostare uno alla volta i tuoi account o al massimo in piccole quantità, per accertarti di non escludere inavvertitamente degli utenti dai servizi chiave. Uno dei modi per determinare se un servizio è utilizzato da un account è esaminare i dati a cui il servizio ha effettuato l'ultimo accesso in IAM. Un altro modo consiste nell'utilizzare AWS CloudTrail per registrare l'utilizzo del servizio a livello di API.

> **Note**
>
> Non dovresti rimuovere la AWSAccess politica completa a meno che non la modifichi o la sostituisca con una politica separata con azioni consentite, altrimenti tutte le AWS azioni degli account dei membri falliranno.

Dimensione massima delle SCP

Tutti i caratteri nella SCP sono conteggiati rispetto alla dimensione massima. Gli esempi in questa guida mostrano le SCP formattate con spazio vuoto aggiuntivo per migliorarne la leggibilità. Tuttavia, per risparmiare spazio se la dimensione della policy è prossima alla dimensione massima, puoi eliminare qualsiasi spazio vuoto, come i caratteri spazio e le interruzioni di linea che si trovano al di fuori delle virgolette.

> **Tip**
>
> Utilizza l'editor visivo per creare la SCP. Rimuove automaticamente lo spazio vuoto aggiuntivo.

Collegamento delle SCP a diversi livelli dell'organizzazione

Per una descrizione dettagliata di come funzionano le SCP, consulta Valutazione SCP.

Effetti di SCP sulle autorizzazioni

Gli SCP sono simili alle politiche di autorizzazione AWS Identity and Access Management (IAM) e utilizzano quasi la stessa sintassi. ma non concedono mai le autorizzazioni. Gli SCP sono invece policy JSON che specificano le autorizzazioni massime per gli utenti IAM e i ruoli IAM nell'organizzazione. Per ulteriori informazioni, consulta Logica di valutazione delle policy nella Guida per l'utente di IAM.

- Le SCP influiscono solo su utenti e ruoli IAM gestiti dagli account che fanno parte dell'organizzazione. Le SCP non influiscono direttamente sulle policy basate su risorse. Non influenzano gli utenti e i ruoli degli account al di fuori dell'organizzazione. Ad esempio, considera un bucket Amazon S3 che è di proprietà dell'account A in un'organizzazione. La policy del bucket (una policy basata su risorse) concede l'accesso agli utenti dell'account B al di fuori dell'organizzazione.

L'account A dispone di un'SCP collegata. Tale SCP non si applica agli utenti esterni nell'account B, ma solo agli utenti che sono gestiti dall'account A nell'organizzazione.

- Una SCP limita le autorizzazioni per i ruoli e gli utenti IAM e negli account membri, compreso l'utente root dell'account membro. Ogni account dispone solo delle autorizzazioni consentite da ogni padre al di sopra di esso. Se un'autorizzazione è bloccata a un qualsiasi livello al di sopra dell'account, implicitamente (non essendo inclusa in un'istruzione di policy `Allow`) o esplicitamente (essendo inclusa in un'istruzione di policy `Deny`), gli utenti o i ruoli nell'account interessato non potranno utilizzare tale autorizzazione, anche se l'amministratore dell'account collega la policy IAM `AdministratorAccess` con autorizzazioni */* agli utenti.
- Le SCP influiscono solo sugli account membri nell'organizzazione. Non hanno alcun effetto sugli utenti o sui ruoli nell'account di gestione.
- Agli utenti e ai ruoli devono ancora essere concesse le autorizzazioni con policy di autorizzazione IAM appropriate. Un utente che non dispone di policy di autorizzazione IAM, non avrà accesso anche se le SCP applicabili consentono tutti i servizi e tutte le operazioni.
- Se un utente o un ruolo dispone di una policy di autorizzazione IAM che concede l'accesso a un'operazione consentita anche dalle SCP applicabili, l'utente o il ruolo può effettuare quell'operazione.
- Se un utente o un ruolo dispone di una policy di autorizzazione IAM che concede l'accesso a un'operazione non consentita o rifiutata esplicitamente dalle SCP applicabili, l'utente o il ruolo non possono effettuare quell'operazione.
- Le SCP influiscono su tutti gli utenti e i ruoli negli account collegati, incluso l'utente root. Le uniche eccezioni sono quelle descritte in Attività ed entità non limitate dalle SCP.
- Le SCP non influiscono su alcun ruolo collegato ai servizi. I ruoli collegati ai servizi consentono l'integrazione di altri AWS servizi con gli SCP AWS Organizations e non possono essere limitati da essi.
- Quando si disabilita il tipo di policy SCP in una radice, tutti gli SCP vengono automaticamente scollegati da tutte le entità in quella radice. AWS Organizations AWS Organizations le entità includono unità organizzative, organizzazioni e account. Se riabiliti le SCP in una root, questa root viene ripristinata solo alla policy `FullAWSAccess` predefinita automaticamente collegata a tutte le entità nella root. Gli eventuali collegamenti delle SCP alle entità AWS Organizations effettuati prima che le SCP venissero disabilitate vengono persi e non possono essere ripristinati automaticamente; tuttavia puoi effettuare di nuovo il collegamento manualmente.
- Se sono presenti sia un limite delle autorizzazioni (una caratteristica IAM avanzata) sia una SCP, il limite, la SCP e la policy basata su identità devono tutti consentire l'operazione.

Utilizzo dei dati di accesso per migliorare le SCP

Una volta effettuato l'accesso con le credenziali dell'account di gestione, puoi visualizzare i dati dell'ultimo accesso al servizio per un' AWS Organizations entità o una policy nella AWS Organizationssezione della console IAM. Puoi anche utilizzare AWS Command Line Interface (AWS CLI) o l' AWS API in IAM per recuperare i dati dell'ultimo accesso al servizio. Questi dati includono informazioni su quali servizi consentiti a cui gli utenti e i ruoli IAM in un AWS Organizations account hanno tentato l'ultima volta di accedere e quando. È possibile utilizzare queste informazioni per identificare le autorizzazioni non necessarie, in modo da poter perfezionare le SCP per aderire meglio al principio del privilegio minimo.

Ad esempio, potresti avere un SCP con elenco negato che vieta l'accesso a tre servizi. AWS Sono consentiti tutti i servizi non elencati nella dichiarazione `Deny` della SCP. I dati dell'ultimo accesso al servizio in IAM indicano quali AWS servizi sono consentiti da SCP ma non vengono mai utilizzati. Con queste informazioni, è possibile aggiornare la SCP per negare l'accesso ai servizi non necessari.

Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente IAM:

- Visualizzazione degli ultimi dati di accesso al servizio per Organizations
- Utilizzo dei dati per perfezionare le autorizzazioni di un'unità organizzativa

Attività ed entità non limitate dalle SCP

Non puoi utilizzare le SCP per limitare le seguenti attività:

- Qualsiasi operazione eseguita dall'account di gestione
- Qualsiasi operazione eseguita utilizzando le autorizzazioni collegate a un ruolo collegato ai servizi
- Eseguire la registrazione per il piano di supporto Enterprise come utente root
- Cambia il livello di AWS supporto come utente root
- Fornisci funzionalità di firma affidabile per i contenuti CloudFront privati
- Configurare il DNS inverso per un server di posta elettronica Amazon Lightsail e istanza Amazon EC2 come utente root
- Attività relative ad alcuni AWS servizi correlati:
  - Alexa Top Sites
  - Alexa Web Information Service
  - Amazon Mechanical Turk

- Amazon Product Marketing API

Creazione, aggiornamento ed eliminazione delle policy di controllo dei servizi

Quando effettui l'accesso con le autorizzazioni all'account di gestione dell'organizzazione, puoi creare e aggiornare le policy di controllo dei servizi (SCP). È possibile creare le SCP mediante la creazione di istruzioni che negano o consentono l'accesso ai servizi e alle operazioni specificate.

La configurazione di default per l'utilizzo delle SCP consiste nell'utilizzare una strategia di "elenco di operazioni bloccate", in cui tutte le operazioni sono implicitamente consentite ad eccezione delle operazioni che desideri bloccare creando istruzioni che negano l'accesso. Con le istruzioni di rifiuto, puoi specificare le risorse e le condizioni per l'istruzione e utilizzare l'elemento NotAction. Per le istruzioni di concessione, è possibile specificare solo i servizi e le operazioni. Per ulteriori informazioni sulle istruzioni che negano e consentono l'accesso, consulta Valutazione SCP.

> **Tip**
>
> È possibile utilizzare i dati sull'ultimo accesso al servizio in IAM come punto dati per aggiornare le SCP in modo da limitare l'accesso esclusivamente ai servizi AWS necessari. Per ulteriori informazioni, consulta Visualizzazione degli ultimi dati di accesso al servizio per Organizations nella Guida per l'utente di IAM.

In questo argomento:

- Dopo avere abilitato le policy di controllo dei servizi per l'organizzazione, puoi creare una policy.
- Quando i requisiti delle SCP cambiano, puoi aggiornare una policy esistente.
- Quando una policy non è più necessaria, dopo averla scollegata da tutte le unità organizzative (UO) e da tutti gli account la puoi eliminare.

Creazione di una SCP

> **Autorizzazioni minime**
>
> Per creare le policy di controllo dei servizi, è necessaria l'autorizzazione per la seguente operazione:

- `organizations:CreatePolicy`

AWS Management Console

Per creare una policy di controllo dei servizi

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. Nella pagina Service control policies (Policy di controllo dei servizi), scegli Create policy (Crea policy).
3. Nella pagina Create new service control policy (Crea nuova policy di controllo dei servizi), inserisci un Nome policy e una Descrizione policy (facoltativa).
4. (Facoltativo) Per aggiungere uno o più tag, scegli Add tag (Aggiungi tag) e quindi inserisci una chiave e un valore facoltativo. Lasciando vuoto il valore, questo viene impostato su una stringa vuota; non è `null`. Puoi associare fino a 50 tag a una policy. Per ulteriori informazioni, consulta Tagging delle risorse AWS Organizations.

   > **Note**
   >
   > Nella maggior parte dei passaggi che seguono, facciamo riferimento ai controlli sul lato destro dell'editor JSON per costruire la policy, elemento per elemento. In alternativa puoi, in qualsiasi momento, inserire semplicemente il testo nell'editor JSON sul lato sinistro della finestra. Puoi digitare direttamente o utilizzare la funzione copia e incolla.

5. Per creare la policy, le prossime fasi variano a seconda del fatto che desideri aggiungere un'istruzione che nega o consente l'accesso. Per ulteriori informazioni, consulta Valutazione SCP. Con le istruzioni di `Deny`, disponi di maggiore controllo perché puoi limitare l'accesso a risorse specifiche, definire le condizioni di attivazione delle SCP e utilizzare l'elemento NotAction. Per informazioni dettagliate sulla sintassi, consulta Sintassi delle SCP.

   Per aggiungere un'istruzione che nega l'accesso:

   a. Nel riquadro Modifica istruzione a destra dell'editor, in Aggiungi azioni, scegli un servizio AWS.

Man mano che si scelgono le opzioni a destra, l'editor JSON si aggiorna per visualizzare la policy JSON corrispondente sulla sinistra.

b. Dopo avere selezionato un servizio, viene aperto un elenco contenente le operazioni disponibili per tale servizio. È possibile scegliere All actions (Tutte le operazioni) o scegliere una o più singole operazioni che si desidera negare.

   Il JSON a sinistra viene aggiornato per includere le operazioni selezionate.

   > **Note**
   >
   > Se selezioni una singola operazione e poi torni indietro e selezioni anche All actions (Tutte le operazioni), la voce prevista per *`servicename`*`/*` viene aggiunta al JSON, ma le singole operazioni selezionate in precedenza vengono lasciate nel JSON e non vengono rimosse.

c. Se desideri aggiungere operazioni da servizi aggiuntivi, puoi scegliere All services (Tutti i servizi) nella parte alta della casella Statement (Istruzione), quindi ripeti i due passaggi precedenti in base alle esigenze.

d. Specificare le risorse da includere nell'istruzione.

   - Vicino a Aggiungi una risorsa, scegli Aggiungi.
   - Nella finestra di dialogo Add resource (Aggiungi risorsa), seleziona dall'elenco il servizio di cui desideri controllare le risorse. Puoi scegliere solo tra i servizi selezionati nel passaggio precedente.
   - In Resource type (Tipo di risorsa), scegli il tipo di risorsa da controllare.
   - Infine, completa l'Amazon Resource Name (ARN) in Resource ARN (ARN della risorsa) per identificare la risorsa specifica di cui desideri controllare l'accesso. È necessario sostituire tutti i segnaposto circondati da parentesi graffe `{}`. Puoi specificare caratteri jolly (`*`) dove la sintassi ARN di quel tipo di risorsa lo consente. Per informazioni su dove è possibile utilizzare i caratteri jolly, consulta la documentazione relativa a un tipo di risorsa specifico.
   - Salva la tua aggiunta alla policy scegliendo Add resource (Aggiungi risorsa). L'elemento `Resource` nel JSON riflette le tue aggiunte o modifiche. L'elemento Resource (Risorsa) è obbligatorio.

> **Tip**
>
> Se desideri specificare tutte le risorse per il servizio selezionato, scegli l'opzione All resources (Tutte le risorse) nell'elenco o modifica l'istruzione `Resource` direttamente nel JSON per leggere `"Resource":"*"`.

e. (Facoltativo) Per specificare le condizioni che limitano l'applicazione di un'istruzione delle policy, vicino a Aggiungi condizione, scegli Aggiungi.

- Chiave di condizione - Dall'elenco puoi scegliere qualsiasi chiave di condizione disponibile per tutti i servizi AWS (ad esempio `aws:SourceIp`) o una chiave specifica del servizio per uno solo dei servizi selezionati per questa istruzione.
- Qualifier (Qualificatore) - (Facoltativo) Se si inseriscono più valori per una condizione (che dipende dalla chiave di condizione specificata), è possibile specificare un qualificatore per testare le richieste rispetto ai valori.
  - Default - Verifica un singolo valore nella richiesta in base al valore della chiave di condizione nella policy. La condizione restituisce vero se il valore nella richiesta corrisponde al valore nella policy. Se la policy specifica più di un valore, vengono trattati come un test "oppure"" e la condizione restituisce vero se i valori della richiesta corrispondono a uno qualsiasi dei valori della policy.
  - Per qualsiasi valore in una richiesta - Quando la richiesta può avere più valori, questa opzione verifica se almeno uno dei valori della richiesta corrisponde ad almeno uno dei valori della chiave di condizione nella policy. La condizione restituisce true se uno qualsiasi dei valori della chiave nella richiesta corrisponde a uno qualsiasi valore della condizione nella policy. Nel caso di nessuna chiave corrispondente o di un set di dati vuoto, la condizione restituisce il valore false.
  - Per tutti i valori in una richiesta - Quando la richiesta può avere più valori, questa opzione verifica se il valore di ogni richiesta corrisponde a un valore della chiave di condizione nella policy. La condizione restituisce true se ogni valore delle chiavi nella richiesta corrisponde ad almeno un valore nella policy. Restituisce true anche se non ci sono chiavi nella richiesta o se i valori delle chiavi si riducono a un set di dati nullo, ad esempio una stringa vuota.
- Operatore - L'operatore specifica il tipo di confronto da effettuare. Le opzioni presentate dipendono dal tipo di dato della chiave di condizione. Ad esempio, la chiave di condizione globale `aws:CurrentTime` consente di scegliere da uno qualsiasi degli

operatori di confronto data, o `Null`, che è possibile utilizzare per verificare se il valore è presente nella richiesta.

Per qualsiasi operatore di condizione eccetto il test `Null`, è possibile scegliere l'opzione IfExists.

- Valore - (Facoltativo) Specifica uno o più valori per i quali desideri testare la richiesta.

Scegliere Add condition (Aggiungi condizione).

Per ulteriori informazioni sull'uso delle chiavi di condizione, consulta Elementi delle policy JSON IAM: Condition nella Guida per l'utente di IAM.

f. (Facoltativo) Per utilizzare l'elemento `NotAction` per negare l'accesso a tutte le operazioni ad eccezione di quelle specificate, sostituire `Action` nel riquadro sinistro con `NotAction`, subito dopo l'elemento `"Effect": "Deny",`. Per ulteriori informazioni, consulta Elementi delle policy JSON IAM: NotAction nella Guida per l'utente di IAM.

6. Per aggiungere un'istruzione che consente l'accesso:

a. Nell'editor JSON a sinistra, cambia la riga `"Effect": "Deny"` in `"Effect": "Allow"`.

Man mano che si scelgono le opzioni a destra, l'editor JSON si aggiorna per visualizzare la policy JSON corrispondente sulla sinistra.

b. Dopo avere selezionato un servizio, viene aperto un elenco contenente le operazioni disponibili per tale servizio. È possibile scegliere All actions (Tutte le operazioni) o scegliere una o più singole operazioni che si desidera consentire.

Il JSON a sinistra viene aggiornato per includere le operazioni selezionate.

> **Note**
>
> Se selezioni una singola operazione e poi torni indietro e selezioni anche All actions (Tutte le operazioni), la voce prevista per *`servicename`*`/*` viene aggiunta al JSON, ma le singole operazioni selezionate in precedenza vengono lasciate nel JSON e non vengono rimosse.

c. Se desideri aggiungere operazioni da servizi aggiuntivi, puoi scegliere All services (Tutti i servizi) nella parte alta della casella Statement (Istruzione), quindi ripeti i due passaggi precedenti in base alle esigenze.

7. (Facoltativo) Per aggiungere un'altra istruzione alla policy, scegli Add statement (Aggiungi istruzione) e utilizza l'editor visivo per creare l'istruzione successiva.
8. Una volta terminata l'aggiunta di istruzioni, scegliere Create policy (Crea policy) per salvare la SCP completata.

La nuova SCP viene inserita nell'elenco delle policy dell'organizzazione. A questo punto, è possibile collegare le SCP alla root, alle unità organizzative o agli account.

AWS CLI & AWS SDKs

Per creare una policy di controllo dei servizi

Per creare un'SCP, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: create-policy

L'esempio seguente presuppone l'esistenza di un file denominato `Deny-IAM.json` con il testo della policy JSON al suo interno. Utilizza tale file per creare una nuova policy di controllo dei servizi.

```
$ aws organizations create-policy \
    --content file://Deny-IAM.json \
    --description "Deny all IAM actions" \
    --name DenyIAMSCP \
    --type SERVICE_CONTROL_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "DenyIAMSCP",
            "Description": "Deny all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
```

```
    }
}
```

- SDK AWS: CreatePolicy

> **Note**
>
> Le SCP non diventano effettive per l'account di gestione e in alcune altre situazioni. Per ulteriori informazioni, consulta Attività ed entità non limitate dalle SCP.

Aggiornamento di una SCP

Quando effettui l'accesso all'account di gestione della tua organizzazione, puoi rinominare o modificare i contenuti di una policy. La modifica dei contenuti di una SCP ha effetto immediato su qualsiasi utente, gruppo e ruolo in tutti gli account collegati.

> **Autorizzazioni minime**
>
> Per aggiornare una policy di controllo dei servizi, è necessaria l'autorizzazione per le seguenti operazioni:
>
> - `organizations:UpdatePolicy` con un elemento `Resource` nella stessa istruzione di policy che includa l'ARN della policy specificata (oppure "*")
> - `organizations:DescribePolicy` con un elemento `Resource` nella stessa istruzione di policy che includa l'ARN della policy specificata (oppure "*")

AWS Management Console

Per aggiornare una policy

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. Nella pagina Policy di controllo dei servizi, scegli il nome della policy che desideri aggiornare.
3. Nella pagina dei dettagli della policy, seleziona Edit policy (Modifica policy).
4. Effettua una o tutte le seguenti modifiche:

- È possibile rinominare la policy inserendo un nuovo nome in Policy name (Nome policy).
- È possibile modificare la descrizione inserendo un nuovo testo in Policy description (Descrizione policy).
- È possibile modificare il testo della policy modificando la policy in formato JSON nel riquadro sinistro. In alternativa, puoi scegliere un'istruzione nell'editor a destra e modificarne gli elementi utilizzando i controlli. Per ulteriori dettagli su ciascun controllo, consulta Creazione di una procedura SCP più in alto in questo argomento.

5. Al termine, scegliere Save changes (Salva le modifiche).

AWS CLI & AWS SDKs

Per aggiornare una policy

Per aggiornare una policy, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: update-policy

Nell'esempio seguente viene rinominata una policy.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "MyRenamedPolicy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "Blocks all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

Nell'esempio seguente viene aggiunta o modificata la descrizione di una policy di controllo dei servizi.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

Nell'esempio seguente viene modificato il documento della policy SCP specificando un file contenente il nuovo testo della policy JSON.

```
$ aws organizations update-policy \
    --policy-id p-zlfw1r64
    --content file://MyNewPolicyText.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
```

```
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AModifiedPolicy\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*
\"]}]}"
    }
}
```

- SDK AWS: UpdatePolicy

Ulteriori informazioni

Per ulteriori informazioni sulla creazione di SCP, consulta i seguenti argomenti:

- Esempi di policy di controllo dei servizi
- Sintassi delle SCP

Modifica dei tag collegati a una SCP

Quando effettui l'accesso all'account di gestione dell'organizzazione, puoi aggiungere o rimuovere i tag collegati a una SCP. Per ulteriori informazioni sul tagging, consultare Tagging delle risorse AWS Organizations.

Autorizzazioni minime

Per modificare i tag associati a una SCP nella tua organizzazione AWS, è necessario disporre delle seguenti autorizzazioni:

- `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations
- `organizations:DescribePolicy` - Obbligatorio solo quando si utilizza la console Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Per modificare i tag collegati a una SCP

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. Nella pagina Service control policies (Policy di controllo dei servizi), scegli il nome della policy con i tag che vuoi modificare.
3. Nella pagina dei dettagli della policy, scegli la scheda Tags, quindi scegli Manage tags (Gestisci tag).
4. Effettua una o tutte le seguenti modifiche:
   - Modifica il valore di un tag inserendo un nuovo valore rispetto a quello precedente. Non puoi modificare direttamente la chiave di tag. Per cambiare una chiave, devi eliminare il tag con la vecchia chiave e aggiungere un tag con la nuova chiave.
   - Rimuovi eventuali tag esistenti scegliendo Remove (Rimuovi).
   - Aggiungi una nuova coppia chiave e valore di tag. Scegli Add tag (Aggiungi tag), quindi inserisci il nuovo nome della chiave e il valore facoltativo nelle caselle fornite. Se lasci vuota la casella Value (Valore), il valore è una stringa vuota; non è `null`.
5. Al termine, scegliere Save changes (Salva le modifiche).

AWS CLI & AWS SDKs

Per modificare i tag collegati a una SCP

Per modificare i tag associati a una SCP puoi utilizzare uno dei seguenti comandi:

- AWS CLI: tag-resource e untag-resource
- SDK AWS: TagResource e UntagResource

Eliminazione di una SCP

Quando effettui l'accesso all'account di gestione della tua organizzazione, puoi eliminare una policy di cui non hai più bisogno nella tua organizzazione.

Note

- Prima di poter eliminare una policy, devi distaccarla da tutte le entità collegate.
- Non puoi eliminare nessuna policy di controllo dei sevizi gestita da AWS, come la SCP denominata `FullAWSAccess`.

Autorizzazioni minime

Per eliminare una policy di controllo dei sevizi, è necessaria l'autorizzazione per eseguire la seguente operazione:

- `organizations:DeletePolicy`

AWS Management Console

Per eliminare una SCP

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. Nella pagina Service control policies (Policy di controllo dei servizi), scegli il nome della SCP che vuoi eliminare.
3. È necessario che la policy da scollegare venga prima eliminata da tutti i root, le UO e gli account. Seleziona la scheda Targets (Destinazioni), scegli il pulsante di opzione accanto a ciascun root, UO o account visualizzato nell'elenco Targets e scegli Detach (Scollega). Nella finestra di dialogo di conferma, scegli Detach (Scollega). Ripeti finché non hai rimosso tutti i target.
4. Nella parte superiore della pagina, seleziona Delete (Elimina).
5. Nella finestra di dialogo di conferma, inserisci il nome della policy, quindi scegli Delete (Elimina).

AWS CLI & AWS SDKs

Per eliminare una SCP

Per eliminare una policy, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: delete-policy

  Nell'esempio seguente viene eliminata la SCP specificata.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Questo comando non produce alcun output se ha esito positivo.

- SDK AWS: DeletePolicy

Collegamento e scollegamento delle policy di controllo dei servizi

Quando effettui l'accesso all'account di gestione dell'organizzazione, puoi collegare una policy di controllo dei servizi (SCP) creata in precedenza. È possibile collegare una policy di controllo dei servizi al root dell'organizzazione, a un'unità organizzativa o direttamente a un account. Per creare una policy di controllo dei servizi, completa le fasi seguenti.

> **Autorizzazioni minime**
>
> Per collegare una policy di controllo dei servizi a una root, un'unità organizzativa o un account, è necessaria l'autorizzazione per la seguente operazione:
>
> - `organizations:AttachPolicy` con un elemento `Resource` nella stessa istruzione di policy che includa "*" o l'Amazon Resource Name (ARN) della policy specificata e l'ARN del root, della UO o dell'account ai quali vuoi collegare la policy

AWS Management Console

Puoi collegare una policy di controllo dei servizi accedendo alla policy oppure al root, all'unità organizzativa o all'account a cui vuoi collegare la policy.

Per collegare una policy di controllo dei servizi passando dal root, un'unità organizzativa o un 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. Nella pagina Account AWS, individua e scegli la casella di controllo accanto al root, all'unità organizzativa o all'account a cui desideri collegare una SCP. Potrebbe essere necessario espandere le UO (scegli l'opzione ▶) per individuare l'UO o l'account desiderato.
3. Nella scheda Policies (Policy), alla voce Service control policies (Policy di controllo dei servizi), scegli Attach (Collega).
4. Individua la policy desiderata e scegli Attach policy (Collega policy).

   L'elenco delle SCP collegate nella scheda Policies (Policy) viene aggiornato per includere la nuova aggiunta. La modifica della policy ha effetto immediato, influenzando le autorizzazioni dei ruoli e degli utenti IAM nell'account collegato o in tutti gli account nel root o nell'UO collegati.

Per collegare una SCP passando dalla policy

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. Nella pagina Service control policies (Policy di controllo dei servizi), scegli il nome della policy che desideri collegare.
3. Nella scheda Targets (Destinazioni), scegli Attach (Collega).
4. Scegli il pulsante di opzione accanto al root, all'unità organizzativa o all'account a cui vuoi collegare la policy. Potrebbe essere necessario espandere le UO (scegli l'opzione ▶) per individuare l'UO o l'account desiderato.
5. Scegli Collega policy.

   L'elenco delle SCP collegate nella scheda Targets (Destinazioni) viene aggiornato per includere la nuova aggiunta. La modifica della policy ha effetto immediato, influenzando le

autorizzazioni dei ruoli e degli utenti IAM nell'account collegato o in tutti gli account nel root o nell'UO collegati.

AWS CLI & AWS SDKs

Per collegare una policy di controllo dei servizi passando dal root, un'unità organizzativa o un account

Per collegare una policy di controllo dei servizi, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: attach-policy

  Nell'esempio seguente una SCP viene collegata a un'UO.

```
$ aws organizations attach-policy \
    --policy-id p-i9j8k7l6m5 \
    --target-id ou-a1b2-f6g7h222
```

  Questo comando non produce alcun output se ha esito positivo.

- AWS SDK: AttachPolicy

La modifica della policy ha effetto immediato, influenzando le autorizzazioni dei ruoli e degli utenti IAM nell'account collegato o in tutti gli account nel root o nell'UO collegati.

Scollegamento di una policy di controllo dei servizi dalla root dell'organizzazione, dalle unità organizzative o dagli account

Quando effettui l'accesso all'account di gestione della tua organizzazione, puoi scollegare una SCP dal root, dall'unità organizzativa o dall'account a cui è collegata. Dopo aver scollegato un SCP da un'entità, tale SCP non si applica più agli utenti e ai ruoli IAM interessati dall'entità ora distaccata. Per scollegare una policy di controllo dei servizi, completa le fasi seguenti.

> **Note**
>
> Non è possibile scollegare l'ultima SCP dal root, da un'unità organizzativa o da un account. Ogni root, UO e account deve avere sempre almeno una SCP collegata.

Autorizzazioni minime

Per scollegare una policy di controllo dei servizi dal root, da un'unità organizzativa o da un account, è necessaria l'autorizzazione per eseguire la seguente operazione:

- `organizations:DetachPolicy`

AWS Management Console

Puoi scollegare una policy di controllo dei servizi accedendo alla policy oppure al root, all'unità organizzativa o all'account da cui vuoi scollegare la policy.

Per scollegare una policy di controllo dei servizi passando dal root, dall'unità organizzativa o da un account a cui è collegata

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. Nella pagina Account AWS individua il root, l'unità organizzativa o l'account da cui desideri scollegare una policy. Potrebbe essere necessario espandere le UO (scegli l'opzione ) per individuare l'UO o l'account desiderato. Scegli il nome del root, dell'unità organizzativa o dell'account.
3. Nella scheda Policies (Policy), scegli il pulsante di opzione accanto alla SCP che desideri scollegare, quindi scegli Detach (Scollega).
4. Nella finestra di dialogo di conferma, scegli Detach policy (Scollega policy).

   L'elenco delle policy di controllo dei servizi collegate viene aggiornato. La modifica della policy causata dal suo scollegamento ha effetto immediato. Ad esempio, lo scollegamento di una policy di controllo dei servizi ha effetto immediato sulle autorizzazioni dei ruoli e degli utenti IAM nell'account precedentemente collegato o negli account nel root o nell'unità organizzativa precedentemente collegati.

Per scollegare una SCP passando dalla policy

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. Nella pagina Service control policies (Policy di controllo dei servizi), scegli il nome della policy che vuoi scollegare da un root, un'UO o un account.
3. Nella scheda Targets (Destinazioni), scegli il pulsante di opzione accanto al root, all'unità organizzativa o all'account da cui vuoi scollegare la policy. Potrebbe essere necessario espandere le UO (scegli l'opzione ) per individuare l'UO o l'account desiderato.
4. Seleziona Scollega.
5. Nella finestra di dialogo di conferma, scegli Detach (Scollega).

   L'elenco delle policy di controllo dei servizi collegate viene aggiornato. La modifica della policy causata dal suo scollegamento ha effetto immediato. Ad esempio, lo scollegamento di una policy di controllo dei servizi ha effetto immediato sulle autorizzazioni dei ruoli e degli utenti IAM nell'account precedentemente collegato o negli account nel root o nell'unità organizzativa precedentemente collegati.

AWS CLI & AWS SDKs

Per scollegare una policy di controllo dei servizi da un root, un'unità organizzativa o un account

Per scollegare una policy di controllo dei servizi, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: detach-policy

  Nell'esempio seguente la SCP specificata viene scollegata dall'unità organizzativa specificata.

```
$ aws organizations detach-policy \
    --policy-id p-i9j8k7l6m5 \
    --target-id ou-a1b2-f6g7h222
```

- AWS SDK: DetachPolicy

La modifica della policy ha effetto immediato, influenzando le autorizzazioni dei ruoli e degli utenti IAM nell'account collegato o in tutti gli account nel root o nell'UO collegati

Valutazione SCP

> **Note**
>
> Le informazioni contenute in questa sezione non si applicano ai tipi di policy di gestione, incluse le policy di rifiuto dei servizi di IA, le policy di backup o le policy di tag. Per ulteriori informazioni, consulta Comprendere l'ereditarietà delle policy di gestione.

Poiché è possibile collegare più policy di controllo dei servizi (SCP) a diversi livelli in AWS Organizations, comprendere come vengono valutate le SCP può aiutarti a scrivere SCP che producano il risultato giusto.

Argomenti

- Come funzionano le SCP con l'istruzione allow
- Come funzionano le SCP con l'istruzione deny
- Strategie per l'utilizzo delle SCP

Come funzionano le SCP con l'istruzione allow

Affinché sia concessa un'autorizzazione per un account specifico, deve esserci una istruzione **`Allow`** esplicita a ogni livello, dalla radice a ciascuna unità organizzativa nel percorso diretto verso l'account (incluso l'account di destinazione stesso). Ecco perché quando vengono abilitate le SCP, AWS Organizations collega una policy SCP gestita da AWS denominata FullAWSAccess che consente tutti i servizi e le operazioni. Se questa policy viene rimossa e non sostituita a nessun livello dell'organizzazione, tutte le unità organizzative e gli account al di sotto di quel livello verrebbero bloccati dall'intraprendere qualsiasi azione.

Ad esempio, esaminiamo lo scenario illustrato nelle figure 1 e 2. Per consentire un'autorizzazione o un servizio sull'account B, una SCP che consente l'autorizzazione o il servizio deve essere collegata alla radice, all'unità organizzativa di produzione e all'account B stesso.

La valutazione SCP segue un modello deny-by-default, il che significa che tutte le autorizzazioni non esplicitamente consentite nelle SCP vengono negate. Se un'istruzione allow non è presente nelle

SCP a nessuno dei livelli come radice, unità organizzativa di produzione o account B, l'accesso viene negato.

> **Note**
>
> - Una istruzione `Allow` in un SCP consente all'elemento `Resource`di avere una sola voce `"*"`.
> - Un'istruzione `Allow` in una SCP non può contenere alcun elemento `Condition`.

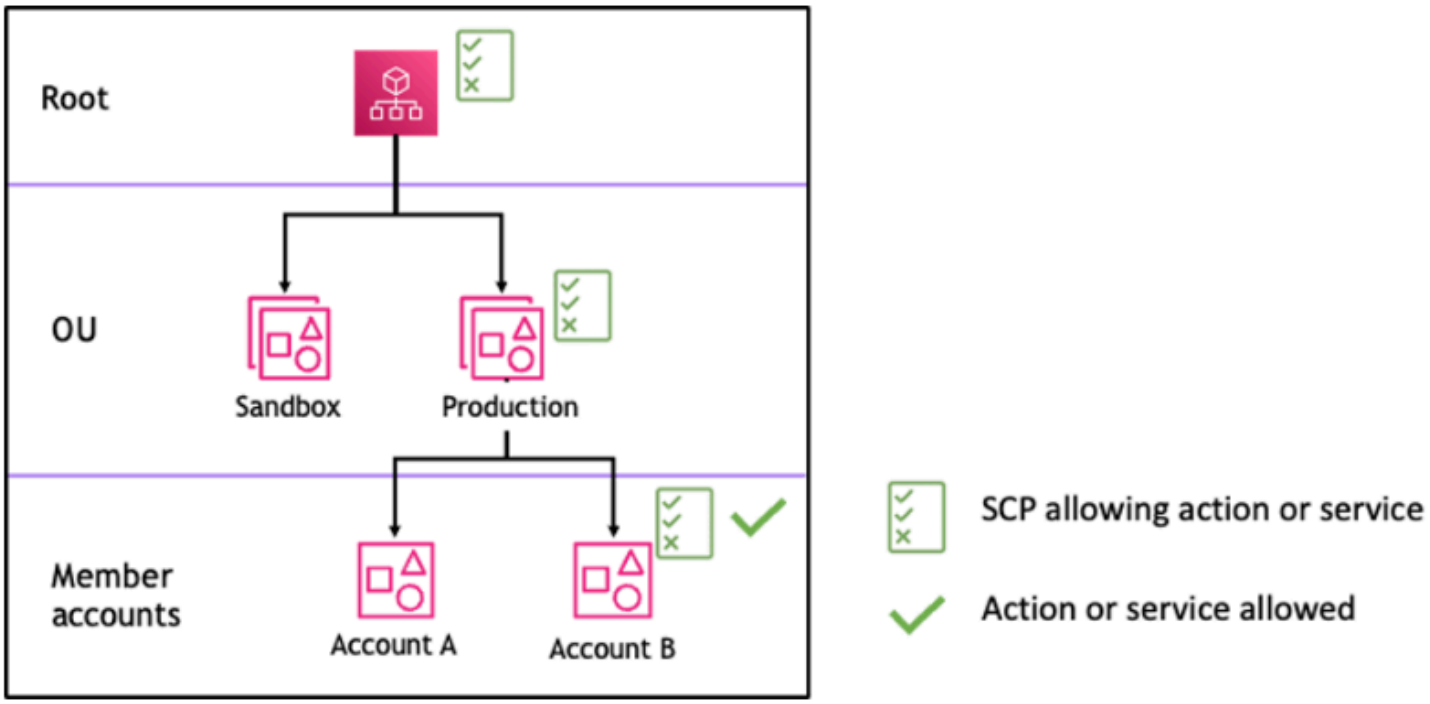


Figura 1: Esempio di struttura organizzativa con una istruzione *`Allow`* collegata alla radice, all'unità organizzativa di produzione e all'account B

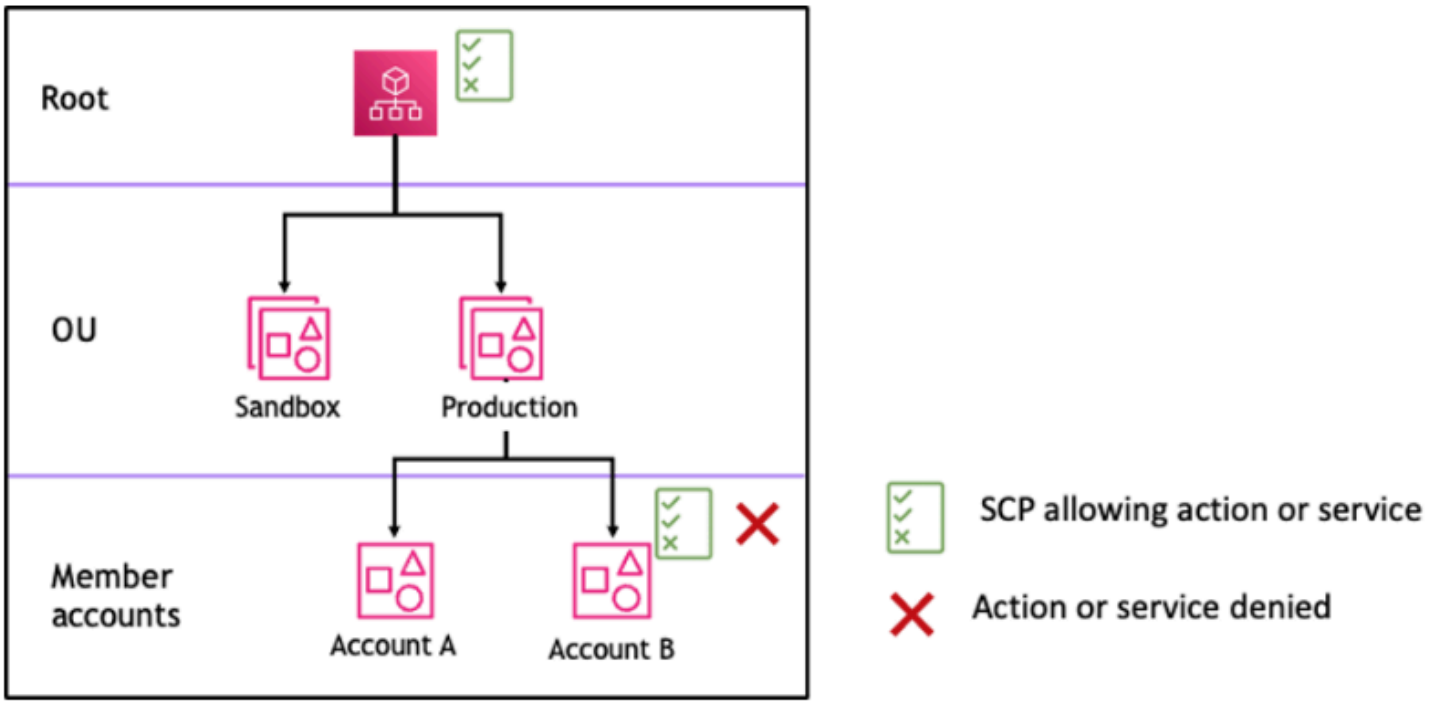


Figura 2: Esempio di struttura organizzativa con una istruzione *`Allow`* mancante sull'unità organizzativa di produzione e relativo impatto sull'account B

Come funzionano le SCP con l'istruzione deny

Affinché un'autorizzazione venga negata per un account specifico, qualsiasi SCP dalla radice a ciascuna unità organizzativa nel percorso diretto verso l'account (incluso l'account di destinazione stesso) può negare tale autorizzazione.

Ad esempio, supponiamo che all'unità organizzativa di produzione sia associata una SCP con un'istruzione `Deny` esplicita specificata per un determinato servizio. È inoltre presente un'altra SCP collegata alla radice e all'account B che consente esplicitamente l'accesso a quello stesso servizio, come mostrato nella Figura 3. Di conseguenza, sia all'account A che all'account B verrà negato l'accesso al servizio, in quanto una policy di negazione applicata a qualsiasi livello dell'organizzazione viene valutata per tutte le unità organizzative e gli account dei membri sottostanti.

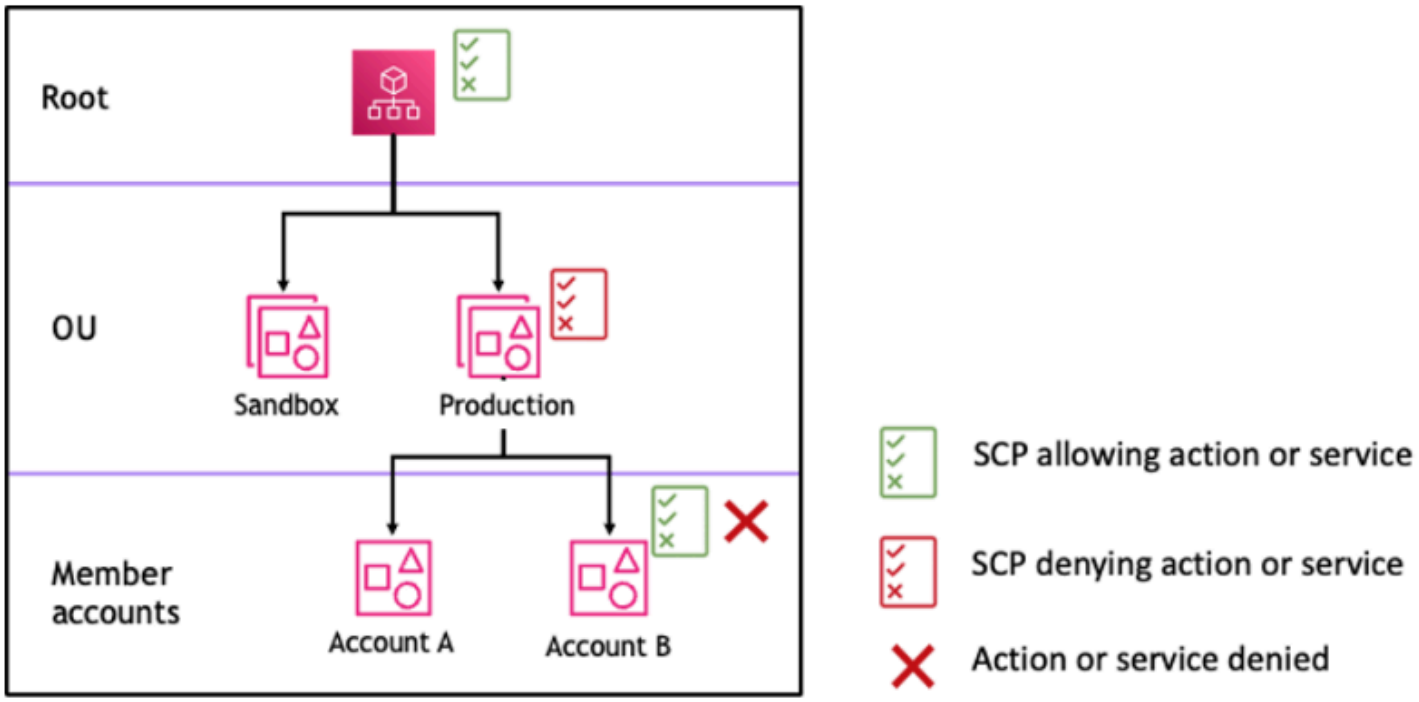


Figura 3: Esempio di struttura organizzativa con una istruzione *Deny* collegata all'unità organizzativa di produzione e relativo impatto sull'account B

Strategie per l'utilizzo delle SCP

Durante la scrittura delle SCP, è possibile utilizzare una combinazione di istruzioni `Allow` e `Deny` per consentire le operazioni e i servizi previsti all'interno dell'organizzazione. Le istruzioni `Deny` sono uno strumento efficace per implementare restrizioni che dovrebbero valere per una parte più ampia dell'organizzazione o delle unità organizzative, poiché quando vengono applicate alla radice o a livello di unità organizzativa influiscono su tutti gli account che ne fanno parte.

Ad esempio, è possibile implementare una policy utilizzando L'account di gestione può anche impedire agli account membri di lasciare l'organizzazione. a livello di radice, che sarà efficace per tutti gli account dell'organizzazione. Le istruzioni deny supportano anche l'elemento condition che può essere utile per creare eccezioni.

> **Tip**
>
> È possibile utilizzare i dati sull'ultimo accesso al servizio in IAM per aggiornare le SCP in modo da limitare l'accesso esclusivamente ai servizi AWS necessari. Per ulteriori informazioni, consulta Visualizzazione degli ultimi dati di accesso al servizio per Organizations nella Guida per l'utente di IAM.

AWS Organizations collega una SCP gestita da AWS denominata FullAWSAccess a ogni radice, unità organizzativa e account al momento della creazione. Questa policy consente tutte le operazioni e i servizi. È possibile sostituire FullAWSAccess con una policy che consenta solo un insieme di servizi in modo che i nuovi servizi AWS non siano consentiti a meno che non siano esplicitamente consentiti aggiornando le SCP. Ad esempio, se l'organizzazione desidera consentire nel proprio ambiente solo l'uso di un sottoinsieme di servizi, è possibile utilizzare un'istruzione `Allow` in modo da consentire solo i servizi specifici.

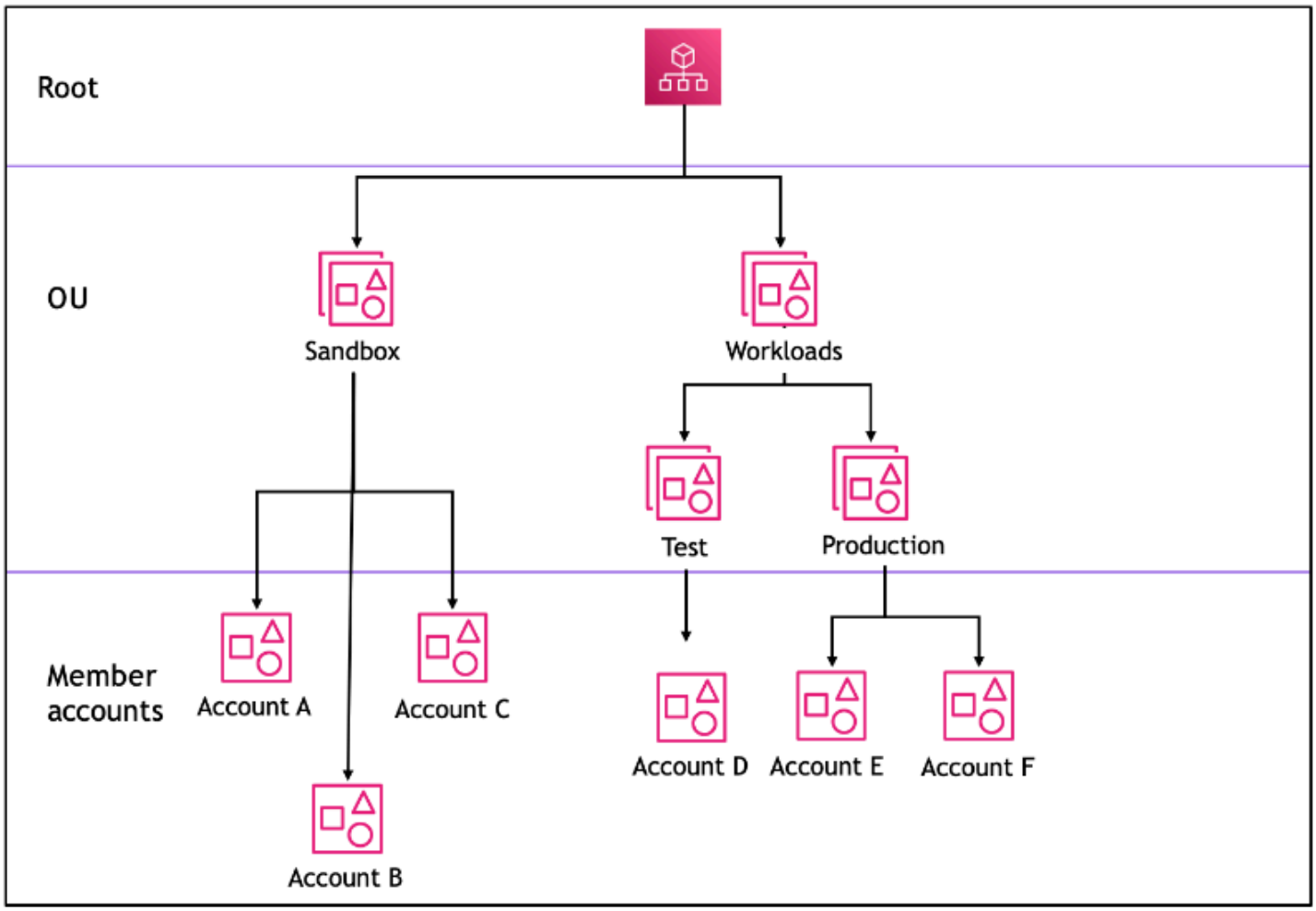
```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Questa policy, che combina le due istruzioni potrebbe essere simile al seguente esempio, impedisce agli account membri di lasciare l'organizzazione e consente l'uso dei servizi AWS desiderati. L'amministratore dell'organizzazione può scollegare la policy FullAWSAccess e collegare questa al suo posto.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        },
        {
```

```
            "Effect": "Deny",
            "Action":"organizations:LeaveOrganization",
            "Resource": "*"
        }
    ]
}
```

Si consideri ora la seguente struttura organizzativa di esempio per capire come applicare più SCP a diversi livelli in un'organizzazione.



La seguente tabella mostra le policy efficaci nell'unità organizzativa dell'ambiente di sperimentazione (sandbox).

Scenario	SCP a livello di radice	SCP a livello di unità organizzativa dell'ambiente di speriment azione (sandbox)	SCP a livello di account A	Policy risultante sull'account A	Policy risultante sull'account B e sull'account C
1	Accesso completo ad AWS	Accesso AWS completo + nega l'accesso a S3	Accesso AWS completo + nega l'accesso a EC2	Nessun accesso S3, nessun accesso EC2	Nessun accesso a S3
2	Accesso completo ad AWS	Consentir e l'accesso ad Amazon Elastic Compute Cloud (Amazon EC2)	Consenti l'accesso a EC2	Consente solo l'accesso a EC2	Consente solo l'accesso a EC2
3	Nega l'accesso a S3	Consenti l'accesso a S3	Accesso completo ad AWS	Nessun accesso al servizio	Nessun accesso al servizio

La seguente tabella mostra le policy efficaci nell'unità organizzativa dei carichi di lavoro.

Scenario	SCP a livello di radice	SCP a livello di unità organizzativa dei carichi di lavoro	SCP a livello di unità organizzativa di test	Policy risultante sull'account D	Policy risultanti a livello di unità organizzativa di produzione, account E e account F
1	Accesso completo ad AWS	Accesso completo ad AWS	Accesso AWS completo + nega l'accesso a EC2	Nessun accesso a EC2	Accesso completo ad AWS
2	Accesso completo ad AWS	Accesso completo ad AWS	Consenti l'accesso a EC2	Consenti l'accesso a EC2	Accesso completo ad AWS
3	Nega l'accesso a S3	Accesso completo ad AWS	Consenti l'accesso a S3	Nessun accesso al servizio	Nessun accesso al servizio

Sintassi delle SCP

Le policy di controllo dei servizi (SCP) utilizzano una sintassi simile a quella utilizzata dalle policy di autorizzazione AWS Identity and Access Management (IAM) e dalle policy basate sulle risorse (come le bucket policy di Amazon S3). Per ulteriori informazioni sulle policy IAM consulta Panoramica sulle policy IAM nella Guida per l'utente di IAM.

Una SCP è un file di testo normale strutturato in base alle regole di JSON. Utilizza gli elementi descritti in questo argomento.

> **Note**
>
> Tutti i caratteri nella SCP sono conteggiati rispetto alla dimensione massima. Gli esempi in questa guida mostrano le SCP formattate con spazio vuoto aggiuntivo per migliorarne

la leggibilità. Tuttavia, per risparmiare spazio se la dimensione della policy è prossima alla dimensione massima, puoi eliminare qualsiasi spazio vuoto, come i caratteri spazio e le interruzioni di linea che si trovano al di fuori delle virgolette.

Per informazioni generali sulle SCP, consulta Policy di controllo dei servizi (Service Control Policies, SCP).

Riepilogo degli elementi

La tabella seguente riepiloga gli elementi di policy che è possibile utilizzare nelle SCP. Alcuni elementi di policy sono disponibili solo nelle SCP che negano le operazioni. La colonna Supported Effects (Effetti supportati) elenca il tipo di effetto che può essere utilizzato con ciascun elemento di policy nelle SCP.

Elemento	Scopo	Effetti supportati
Versione	Specifica le regole di sintassi del linguaggio da utilizzare per elaborare la policy.	`Allow`, `Deny`
Statement	Serve da container per gli elementi di policy. È possibile avere più istruzion	`Allow`, `Deny`

Elemento	Scopo	Effetti supportati
	i nelle SCP.	
Statement ID (Sid)	(Facoltativo) Fornisce un nome semplice per l'istruzione.	`Allow`, `Deny`
Effetto	Definisce se l'istruzione SCP consente o nega l'accesso agli utenti e ai ruoli IAM in un account.	`Allow`, `Deny`
Action	Specifica il AWS servizio e le azioni consentite o negate da SCP.	`Allow`, `Deny`

Elemento	Scopo	Effetti supportati
NotAction	Specifica il AWS servizio e le azioni che sono esenti dall'SCP. Utilizzato invece dell'elemento `Action`.	`Deny`
Resource (Risorsa)	Speciifica le AWS risorse a cui si applica l'SCP.	`Deny`
Condition	Specifica le condizioni che stabiliscono quando l'istruzione è attiva.	`Deny`

Le seguenti sezioni forniscono ulteriori informazioni ed esempi sull'utilizzo degli elementi di policy nelle SCP.

Elemento **`Version`**

Ogni SCP deve includere un elemento `Version` con il valore `"2012-10-17"`. Questo è lo stesso valore di versione della versione più recente delle policy di autorizzazione IAM:

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

Per ulteriori informazioni, consulta Elementi delle policy JSON IAM: Version nella Guida per l'utente di IAM.

Elemento **`Statement`**

Un SCP consiste di uno o più elementi `Statement`. È possibile avere una sola parola chiave `Statement` in una policy, ma il valore può essere una matrice JSON di istruzioni (circondata da caratteri [ ]).

Nell'esempio seguente viene illustrata una singola istruzione composta di elementi `Effect`, `Action` e `Resource`.

```
    "Statement": {
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
```

L'esempio seguente include due istruzioni come un elenco matrice all'interno di un elemento `Statement`. La prima istruzione consente tutte le operazioni, mentre la seconda nega qualsiasi operazione di EC2. Il risultato è che un amministratore nell'account può delegare qualsiasi autorizzazione eccetto quelle da Amazon Elastic Compute Cloud (Amazon EC2).

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*"
```

```
        }
    ]
```

Per ulteriori informazioni, consulta Elementi delle policy JSON IAM: Statement nella Guida per l'utente di IAM.

Elemento Statement ID (**`Sid`**)

`Sid` è un identificatore opzionale fornito per l'istruzione della policy. Puoi assegnare un valore `Sid` a ogni istruzione in una matrice di istruzioni. La seguente SCP mostra un esempio di istruzione `Sid`.

```
{
    "Statement": {
        "Sid": "AllowsAllActions",
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
}
```

Per ulteriori informazioni, consulta Elementi delle policy JSON IAM: Id nella Guida per l'utente di IAM.

Elemento **`Effect`**

Ogni istruzione deve contenere un elemento `Effect`. Il valore può essere `Allow` o `Deny`. Influenza tutte le operazioni elencate nella stessa istruzione.

Per ulteriori informazioni, consulta Elementi delle policy JSON IAM: Effect nella Guida per l'utente di IAM.

`"Effect": "Allow"`

Nell'esempio seguente viene illustrata una SCP con un'istruzione che contiene un elemento `Effect` con un valore `Allow` che consente agli utenti di eseguire operazioni per il servizio Amazon S3. Questo esempio è utile se un'organizzazione utilizza la strategia dell'elenco consentiti (ove le policy `FullAWSAccess` predefinite sono tutte scollegate, in modo che le autorizzazioni vengano negate in modo implicito per impostazione predefinita). Il risultato è che l'istruzione concede le autorizzazioni Amazon S3 per qualsiasi account collegato:

```
{
```

```
    "Statement": {
        "Effect": "Allow",
        "Action": "s3:*",
        "Resource": "*"
    }
}
```

Sebbene utilizzi la stessa parola chiave di valore `Allow` di una policy di autorizzazione IAM, in una SCP non vengono effettivamente concesse a un utente le autorizzazioni per eseguire qualsiasi operazione. Gli SCP agiscono invece come filtri che specificano le autorizzazioni massime per gli utenti IAM e i ruoli IAM in un'organizzazione. Nell'esempio precedente, anche se un utente nell'account aveva la policy gestita `AdministratorAccess` collegata, la SCP limita le operazioni di tutti gli utenti nell'account alle sole operazioni Amazon S3.

`"Effect": "Deny"`

In un'istruzione in cui l'elemento `Effect` ha un valore `Deny`, è anche possibile limitare l'accesso a risorse specifiche o definire condizioni di attivazione delle SCP.

Quanto segue mostra un esempio di come utilizzare una condizione di chiave in un'istruzione di rifiuto.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "ec2:RunInstances",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:InstanceType": "t2.micro"
            }
        }
    }
}
```

Questa istruzione in una SCP imposta un guardrail per evitare che gli account interessati (per cui la SCP è collegata all'account stesso o al root dell'organizzazione o UO che contiene l'account) avviino istanze Amazon EC2 se l'istanza Amazon EC2 non è impostata su `t2.micro`. Anche se una policy IAM che consente questa operazione è collegata all'account, il guardrail creato dalla SCP la impedisce.

Elementi **`Action`** e **`NotAction`**

Ogni istruzione deve contenere uno dei seguenti:

- Nelle istruzioni di concessione o rifiuto, un elemento `Action`.
- Solo nelle istruzioni di rifiuto (in cui il valore dell'elemento `Effect` è `Deny`), un elemento `Action` o `NotAction`.

Il valore dell'`NotAction`elemento `Action` or è un elenco (un array JSON) di stringhe che identificano i AWS servizi e le azioni consentiti o negati dall'istruzione.

Ogni stringa è composta dall'abbreviazione per il servizio (come "s3", "ec2", "iam" o "organizzazioni"), in lettere minuscole, seguita da due punti e quindi da un'operazione da quel servizio. Le operazioni e le notazioni rispettano la distinzione tra maiuscole e minuscole e devono essere digitate come illustrato nella documentazione relativa a ciascun servizio. Di solito, queste vengono digitate con ogni parola che inizia con una lettera maiuscola e il resto in minuscolo. Ad esempio: `"s3:ListAllMyBuckets"`.

È inoltre possibile utilizzare caratteri jolly come asterisco (*) o punto interrogativo (?) in una SCP:

- Utilizzare un asterisco (*) come carattere jolly per abbinare più operazioni che condividono parte di un nome. Il valore `"s3:*"` indica tutte le operazioni del servizio Amazon S3. Il valore `"ec2:Describe*"` corrisponde solo alle operazioni EC2 che iniziano con "Describe".
- Utilizzare il punto interrogativo (?) come carattere jolly per abbinare un singolo carattere.

> **Note**
>
> In una SCP, i caratteri jolly (*) e (?) in un elemento `Action` o `NotAction` possono essere utilizzati unicamente da soli o al termine della stringa. Non può trovarsi all'inizio o al centro della stringa. Pertanto, `"servicename:action*"` è valida, ma `"servicename:*action"` e `"servicename:some*action"` non sono entrambe valide nelle SCP.

Per un elenco di tutti i servizi e le azioni che supportano sia negli AWS Organizations SCP che nelle politiche di autorizzazione IAM, consulta Actions, Resources and Condition Keys for AWS Services nella IAM User Guide.

Per ulteriori informazioni, consulta IAM JSON Policy Elements: Action e IAM JSON Policy Elements: NotAction nella IAM User Guide.

Esempio di elemento **`Action`**

L'esempio seguente mostra una SCP con un'istruzione che consente agli amministratori degli account di delegare le autorizzazioni describe, start, stop e terminate per le istanze EC2 nell'account. Questo è un esempio di elenco di consentiti ed è utile quando le policy `Allow *` di default non sono collegate in modo che, per impostazione predefinita, le autorizzazioni vengono negate in modo implicito. Se la policy `Allow *` di default è ancora collegata al root, all'UO o all'account a cui è collegata la seguente policy, la policy non ha effetto:

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
          "ec2:DescribeInstances", "ec2:DescribeImages", "ec2:DescribeKeyPairs",
          "ec2:DescribeSecurityGroups", "ec2:DescribeAvailabilityZones",
 "ec2:RunInstances",
          "ec2:TerminateInstances", "ec2:StopInstances", "ec2:StartInstances"
        ],
        "Resource": "*"
    }
}
```

L'esempio seguente mostra come è possibile negare l'accesso ai servizi che non desideri utilizzare negli account collegati. Presuppone che gli SCP `"Allow *"` predefiniti siano ancora collegati a tutte le UO e tutte le radici. Questa policy di esempio impedisce agli amministratori degli account collegati di delegare qualsiasi autorizzazione per i servizi IAM, Amazon EC2 e Amazon RDS. Qualsiasi operazione da altri servizi può essere delegata a condizione che non vi sia un'altra policy collegata che li neghi.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": [ "iam:*", "ec2:*", "rds:*" ],
        "Resource": "*"
    }
}
```

Esempio di elemento **NotAction**

L'esempio seguente mostra come utilizzare un `NotAction` elemento per escludere AWS i servizi dall'effetto della policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LimitActionsInRegion",
      "Effect": "Deny",
      "NotAction": "iam:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-west-1"
        }
       }
     }
   ]
}
```

Con questa dichiarazione, gli account interessati si limitano a intraprendere azioni nei limiti specificati Regione AWS, tranne quando utilizzano azioni IAM.

Elemento **Resource**

In istruzioni in cui l'elemento `Effect` ha un valore `Allow`, è possibile specificare solo "*" nell'elemento `Resource` di una SCP. Non è possibile specificare l'ARN (Amazon Resource Name) di singole risorse.

È inoltre possibile utilizzare caratteri jolly come asterisco (*) o punto interrogativo (?) nell'elemento risorsa:

- Utilizzare un asterisco (*) come carattere jolly per abbinare più operazioni che condividono parte di un nome.
- Utilizzare il punto interrogativo (?) come carattere jolly per abbinare un singolo carattere.

In istruzioni in cui l'elemento `Effect` ha un valore `Deny`, è possibile specificare singoli ARN, come mostrato nel seguente esempio.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToAdminRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/role-to-deny"
      ]
    }
  ]
}
```

Questa SCP impedisce agli utenti e ai ruoli IAM negli account interessati di apportare modifiche a un ruolo IAM di amministrazione comune creato in tutti gli account nella tua organizzazione.

Per ulteriori informazioni, consulta Elementi delle policy JSON IAM: Resource nella Guida per l'utente di IAM.

Elemento **`Condition`**

È possibile specificare un elemento `Condition` nelle istruzioni di rifiuto in una SCP.

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

```
                "cloudfront:*",
                "iam:*",
                "route53:*",
                "support:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

Questa SCP nega l'accesso a tutte le operazioni al di fuori delle regioni `eu-central-1` e `eu-west-1`, tranne per le operazioni nei servizi elencati.

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

Elementi non supportati

I seguenti elementi non sono supportati nelle SCP:

- `Principal`
- `NotPrincipal`
- `NotResource`

Esempi di policy di controllo dei servizi

Le policy di controllo dei servizi (SCP) di esempio riportate in questo argomento sono solo a scopo informativo.

> **Prima di utilizzare questi esempi**
>
> Prima di utilizzare queste SCP di esempio nella tua organizzazione, esegui le operazioni descritte di seguito:

- Esamina attentamente e personalizza le SCP per i tuoi requisiti specifici.
- Testa accuratamente le SCP nel tuo ambiente con i servizi AWS che utilizzi.

  Le policy di esempio riportate in questa sezione illustrano l'implementazione e l'utilizzo delle SCP. Non devono essere interpretate come suggerimenti o best practice AWS ufficiali da implementare esattamente come mostrato. È tua responsabilità testare accuratamente l'idoneità di qualsiasi policy basata su rifiuto a risolvere i requisiti aziendali del tuo ambiente. Le policy di controllo dei servizi basate sul diniego possono limitare o bloccare involontariamente l'utilizzo dei servizi AWS a meno che non si aggiungano le opportune eccezioni alla policy. Per un esempio di tale eccezione, consulta il primo esempio che esenta i servizi globali dalle regole che bloccano l'accesso a Regioni AWS indesiderate.
- Ricorda che una SCP influisce su ogni utente e ruolo, incluso l'utente root, in ogni account a cui è collegata.

Tip

È possibile utilizzare i dati sull'ultimo accesso al servizio in IAM per aggiornare le SCP in modo da limitare l'accesso esclusivamente ai servizi AWS necessari. Per ulteriori informazioni, consulta Visualizzazione degli ultimi dati di accesso al servizio per Organizations nella Guida per l'utente di IAM.

Ciascuna delle seguenti policy è l'esempio di una strategia di policy di elenco di rifiuto. Le policy di elenco di rifiuto devono essere collegate assieme ad altre policy che consentono le operazioni approvate negli account interessati. Ad esempio, la policy `FullAWSAccess` predefinita permette l'uso di tutti i servizi in un account. Questa policy è collegata per impostazione predefinita alla root, a tutte le unità organizzative (UO) e a tutti gli account. In realtà non concede alcuna autorizzazione (nessuna SCP lo fa). Piuttosto, consente agli amministratori nell'account di delegare l'accesso alle operazioni collegando le policy delle autorizzazioni AWS Identity and Access Management (IAM) standard a utenti, ruoli o gruppi nell'account. Ognuna di queste policy di elenco di rifiuto sovrascrive qualsiasi policy bloccando l'accesso ai servizi o alle operazioni specificati.

Examples (Esempi)

- Esempi generali
  - Rifiuta l'accesso a AWS in base alla Regione AWS richiesta.

- Impedire a qualsiasi VPC che non dispone già dell'accesso a Internet di ottenerlo

Esempi generali

Rifiuta l'accesso a AWS in base alla Regione AWS richiesta.

Questa SCP nega l'accesso a qualsiasi operazione al di fuori delle Regioni specificate. Sostituisci `eu-central-1` e `eu-west-1` con le Regioni AWS che desideri utilizzare. Fornisce esenzioni per le operazioni nei servizi globali approvati. In questo esempio viene inoltre illustrato come esentare le richieste effettuate da uno dei due ruoli di amministratore specificati.

> **Note**
>
> Per utilizzare l'SCP Region deny (Regione negata) con l'AWS Control Tower, consulta Rifiuta l'accesso a AWS in base alla Regione AWS richiesta..

Questa policy utilizza l'effetto `Deny` per rifiutare l'accesso a tutte le richieste di operazioni non presenti una delle due regioni approvate (`eu-central-1` e `eu-west-1`). L'elemento NotAction consente di elencare i servizi le cui operazioni (o singole operazioni) sono esentate da questa restrizione. Poiché i servizi globali dispongono di endpoint ospitati fisicamente dalla `us-east-1`, devono essere esentati in questo modo. Con un SCP strutturato in questo modo, le richieste fatte ai servizi globali nella regione `us-east-1` sono consentite se il servizio richiesto è incluso nell'elemento `NotAction`. Eventuali altre richieste ai servizi nella regione `us-east-1` sono negate da questa policy di esempio.

> **Note**
>
> Questo esempio potrebbe non includere tutti i servizi o le operazioni AWS globali più recenti. Sostituisci l'elenco di servizi e operazioni con i servizi globali utilizzati dagli account nella tua organizzazione.
>
> > **Suggerimento**
> >
> > È possibile visualizzare i dati sull'ultimo accesso al servizio nella console IAM per determinare i servizi globalmente utilizzati dall'organizzazione. Nella scheda Access Advisor (Consulente accessi) nella pagina dei dettagli di un utente, un gruppo o un

ruolo IAM vengono visualizzati i servizi AWS utilizzati da tale entità, ordinati in base all'accesso più recente.

Considerazioni

- AWS KMS e AWS Certificate Manager supportano gli endpoint regionali. Tuttavia, se desideri utilizzarli con un servizio globale come Amazon CloudFront, è necessario includerli nell'elenco di esclusione dei servizi globali, come nell'esempio di SCP riportato di seguito. Un servizio globale come Amazon CloudFront richiede in genere l'accesso a AWS KMS e ACM nella stessa Regione, che per un servizio globale è la Regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`).
- Per impostazione predefinita, AWS STS è un servizio globale e deve essere incluso nell'elenco di esclusione dei servizi globali. Tuttavia, è possibile abilitare AWS STS per utilizzare gli endpoint regionali al posto di un singolo endpoint globale. In questo caso, puoi rimuovere STS dall'elenco di esclusione dei servizi globali nell'esempio di SCP riportato di seguito. Per ulteriori informazioni, consulta Gestione di AWS STS in una Regione AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "chime:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
```

```
            "ec2:DescribeRegions",
            "ec2:DescribeTransitGateways",
            "ec2:DescribeVpnGateways",
            "fms:*",
            "globalaccelerator:*",
            "health:*",
            "iam:*",
            "importexport:*",
            "kms:*",
            "mobileanalytics:*",
            "networkmanager:*",
            "organizations:*",
            "pricing:*",
            "route53:*",
            "route53domains:*",
            "route53-recovery-cluster:*",
            "route53-recovery-control-config:*",
            "route53-recovery-readiness:*",
            "s3:GetAccountPublic*",
            "s3:ListAllMyBuckets",
            "s3:ListMultiRegionAccessPoints",
            "s3:PutAccountPublic*",
            "shield:*",
            "sts:*",
            "support:*",
            "trustedadvisor:*",
            "waf-regional:*",
            "waf:*",
            "wafv2:*",
            "wellarchitected:*"
        ],
        "Resource": "*",
        "Condition": {
            "StringNotEquals": {
                "aws:RequestedRegion": [
                    "eu-central-1",
                    "eu-west-1"
                ]
            },
            "ArnNotLike": {
                "aws:PrincipalARN": [
                    "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                    "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                ]
```

```
                }
            }
        }
    ]
}
```

Impedire agli utenti e ai ruoli IAM di apportare alcune modifiche

Questa SCP impedisce agli utenti e ai ruoli IAM di apportare modifiche al ruolo IAM specificato creato in tutti gli account nell'organizzazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToASpecificRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ]
    }
  ]
}
```

Impedire agli utenti e ai ruoli IAM di apportare modifiche specifiche, con un'eccezione per un ruolo di amministratore specificato

Questa SCP si basa sull'esempio precedente per fare un'eccezione per gli amministratori. Impedisce agli utenti e ai ruoli IAM negli account interessati di apportare modifiche a un ruolo IAM

di amministrazione comune creato in tutti gli account nella tua organizzazione ad eccezione degli amministratori che usano un ruolo specifico.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessWithException",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN":"arn:aws:iam::*:role/name-of-admin-role-to-allow"
        }
      }
    }
  ]
}
```

Richiedere la MFA per eseguire un'operazione API

Utilizza una SCP simile alla seguente per richiedere che l'autenticazione a più fattori (MFA) sia abilitata prima che un utente o un ruolo IAM possa eseguire un'operazione. In questo esempio, l'operazione consiste nell'interrompere un'istanza Amazon EC2.

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

```
    {
      "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
      "Effect": "Deny",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": false}}
    }
  ]
}
```

Bloccare l'accesso al servizio per l'utente root

La policy seguente impedisce tutti gli accessi alle operazioni specificate per l'utente root in un account. Se desideri impedire agli account di usare le credenziali root in modi specifici, aggiungi le tue operazioni a questa policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictEC2ForRoot",
      "Effect": "Deny",
      "Action": [
        "ec2:*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:root"
          ]
        }
      }
    }
  ]
}
```

L'account di gestione può anche impedire agli account membri di lasciare l'organizzazione.

La policy seguente blocca l'utilizzo dell'operazione API `LeaveOrganization` in modo che gli amministratori degli account membri non possano rimuovere i propri account dall'organizzazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "organizations:LeaveOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

SCP di esempio per Amazon CloudWatch

Esempi in questa categoria

- Impedire agli utenti di disabilitare CloudWatch o di alterarne la configurazione

Impedire agli utenti di disabilitare CloudWatch o di alterarne la configurazione

Un operatore CloudWatch di livello inferiore deve monitorare pannelli di controllo e allarmi. Tuttavia, l'operatore non deve essere in grado di eliminare o modificare alcun pannello di controllo o allarme attuati da personale senior. Questa SCP impedisce agli utenti o ai ruoli in qualsiasi account interessato di eseguire qualsiasi comando CloudWatch che potrebbe eliminare o modificare i pannelli di controllo o gli allarmi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DeleteDashboards",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:PutDashboard",
```

```
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:SetAlarmState"
      ],
      "Resource": "*"
    }
  ]
}
```

SCP di esempio per AWS Config

Esempi in questa categoria

- Impedire agli utenti di disabilitare AWS Config o di modificarne le regole

Impedire agli utenti di disabilitare AWS Config o di modificarne le regole

Questa SCP impedisce agli utenti o ai ruoli in qualsiasi account interessato di eseguire operazioni AWS Config che potrebbero disabilitare AWS Config o alterarne le regole o i trigger.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "config:DeleteConfigRule",
        "config:DeleteConfigurationRecorder",
        "config:DeleteDeliveryChannel",
        "config:StopConfigurationRecorder"
      ],
      "Resource": "*"
    }
  ]
}
```

SCP di esempio per Amazon Elastic Compute Cloud (Amazon EC2)

Esempi in questa categoria

- Richiedere che le istanze Amazon EC2 utilizzino un tipo specifico
- Impedire l'avvio di istanze EC2 senza IMDSv2
- Impedire la disabilitazione della crittografia Amazon EBS predefinita

Richiedere che le istanze Amazon EC2 utilizzino un tipo specifico

Con questa SCP, qualsiasi avvio di istanza che non utilizza il tipo di istanza `t2.micro` viene negato.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireMicroInstanceType",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ec2:InstanceType": "t2.micro"
        }
      }
    }
  ]
}
```

Impedire l'avvio di istanze EC2 senza IMDSv2

La seguente policy impedisce a tutti gli utenti di avviare istanze EC2 senza IMDSv2.

```
[
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "StringNotEquals":{
            "ec2:MetadataHttpTokens":"required"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
```

```
         "NumericGreaterThan":{
            "ec2:MetadataHttpPutResponseHopLimit":"3"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"*",
      "Resource":"*",
      "Condition":{
         "NumericLessThan":{
            "ec2:RoleDelivery":"2.0"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:ModifyInstanceMetadataOptions",
      "Resource":"*"
   }
]
```

La seguente policy impedisce a tutti gli utenti di avviare istanze EC2 senza IMDSv2, ma consente a identità IAM specifiche di modificare le opzioni dei metadati delle istanze.

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "NumericGreaterThan": {
        "ec2:MetadataHttpPutResponseHopLimit": "3"
```

```
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*",
    "Condition": {
      "StringNotLike": {
        "aws:PrincipalARN": [
          "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
        ]
      }
    }
  }
]
```

Impedire la disabilitazione della crittografia Amazon EBS predefinita

La seguente policy impedisce a tutti gli utenti di disabilitare la crittografia Amazon EBS predefinita.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

SCP di esempio per Amazon GuardDuty

Esempi in questa categoria

- Impedire agli utenti di disabilitare GuardDuty o di alterarne la configurazione

Impedire agli utenti di disabilitare GuardDuty o di alterarne la configurazione

Questa SCP impedisce agli utenti o ai ruoli in qualsiasi account interessato di disabilitare GuardDuty o di alterarne la configurazione, direttamente come comando oppure tramite la console. Consente in modo efficace l'accesso in sola lettura alle informazioni e alle risorse GuardDuty.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "guardduty:AcceptInvitation",
                "guardduty:ArchiveFindings",
                "guardduty:CreateDetector",
                "guardduty:CreateFilter",
                "guardduty:CreateIPSet",
                "guardduty:CreateMembers",
                "guardduty:CreatePublishingDestination",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteDetector",
                "guardduty:DeleteFilter",
                "guardduty:DeleteInvitations",
                "guardduty:DeleteIPSet",
                "guardduty:DeleteMembers",
                "guardduty:DeletePublishingDestination",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:DisassociateMembers",
                "guardduty:InviteMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:TagResource",
                "guardduty:UnarchiveFindings",
                "guardduty:UntagResource",
                "guardduty:UpdateDetector",
                "guardduty:UpdateFilter",
                "guardduty:UpdateFindingsFeedback",
                "guardduty:UpdateIPSet",
                "guardduty:UpdatePublishingDestination",
                "guardduty:UpdateThreatIntelSet"
```

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

SCP di esempio per AWS Resource Access Manager

Esempi in questa categoria

- Impedire la condivisione esterna
- Consentire ad account specifici di condividere solo tipi di risorse specificati
- Impedire la condivisione con organizzazioni o unità organizzative (UO)
- Consentire la condivisione solo con utenti e ruoli IAM specificati

Impedire la condivisione esterna

La seguente SCP di esempio impedisce agli utenti di creare condivisioni di risorse che consentono la condivisione con utenti e ruoli IAM che non fanno parte dell'organizzazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:UpdateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "ram:RequestedAllowsExternalPrincipals": "true"
                }
            }
        }
    ]
}
```

Consentire ad account specifici di condividere solo tipi di risorse specificati

La seguente SCP consente agli account 111111111111 e 222222222222 di creare condivisioni di risorse che condividono elenchi di prefissi e associare elenchi di prefissi a condivisioni di risorse esistenti.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OnlyNamedAccountsCanSharePrefixLists",
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalAccount": [
                        "111111111111",
                        "222222222222"
                    ]
                },
                "StringEquals": {
                    "ram:RequestedResourceType": "ec2:PrefixList"
                }
            }
        }
    ]
}
```

Impedire la condivisione con organizzazioni o unità organizzative (UO)

La seguente SCP impedisce agli utenti di creare condivisioni di risorse che condividono le risorse con una AWS Organization o UO.

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

```
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "ram:Principal": [
                        "arn:aws:organizations::*:organization/*",
                        "arn:aws:organizations::*:ou/*"
                    ]
                }
            }
        }
    ]
}
```

Consentire la condivisione solo con utenti e ruoli IAM specificati

La seguente SCP di esempio consente agli utenti di condividere le risorse solo con l'organizzazione `o-12345abcdef`, l'unità organizzativa `ou-98765fedcba` e l'account `111111111111`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "ram:Principal": [
                        "arn:aws:organizations::123456789012:organization/
o-12345abcdef",
                        "arn:aws:organizations::123456789012:ou/o-12345abcdef/
ou-98765fedcba",
                        "111111111111"
                    ]
                }
            }
        }
```

```
    ]
}
```

Esempi di SCP per il Sistema di controllo Amazon Route 53 per il ripristino di applicazioni (Route53 ARC)

Esempi in questa categoria

- Impedisci agli utenti di aggiornare gli stati di controllo di routing di Route 53 ARC

Impedisci agli utenti di aggiornare gli stati di controllo di routing di Route 53 ARC

Un operatore Route 53 ARC di livello inferiore deve monitorare i pannelli di controllo e visualizzare le informazioni di Route 53 ARC. Tuttavia, l'operatore non deve essere in grado di aggiornare i controlli di routing per eseguire il failover dell'applicazione da una Regione AWS all'altra, come potrebbe essere consentito a un operatore senior. Questa SCP impedisce agli utenti o ai ruoli in qualsiasi account interessato di eseguire operazioni Route 53 ARC che aggiornano i controlli di routing di Route 53 ARC.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAll",
            "Effect": "Deny",
            "Action": [
                "route53-recovery-cluster:UpdateRoutingControlState",
                "route53-recovery-cluster:UpdateRoutingControlStates"
            ],
            "Resource": "*",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

Esempi di SCP per Amazon S3

Esempi in questa categoria

- Impedire il caricamento di oggetti non crittografati su Amazon S3

Impedire il caricamento di oggetti non crittografati su Amazon S3

La seguente policy impedisce a tutti gli utenti di caricare oggetti non crittografati nei bucket S3.

```
{
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption": "true"
    }
  }
}
```

La seguente policy impedisce a tutti gli utenti di caricare oggetti non crittografati nei bucket S3 e applica anche un tipo di crittografia specificato (AES256 o aws:kms) per il caricamento di oggetti nei propri bucket.

```
[
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption": "true"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "StringNotEquals": {
```

```
        "s3:x-amz-server-side-encryption": "AES256"
      }
    }
  }
]
```

SCP di esempio per l'assegnazione di tag alle risorse

Esempi in questa categoria

- Richiedere un tag sulle risorse create specificate
- Impedire la modifica dei tag se non da parte dei principali autorizzati

Richiedere un tag sulle risorse create specificate

La seguente SCP impedisce agli utenti e ai ruoli IAM negli account interessati di creare determinati tipi di risorse se la richiesta non include i tag specificati.

> **Important**
>
> Ricorda di testare le policy basate su rifiuto con i servizi che utilizzi nel tuo ambiente. L'esempio seguente è un semplice blocco per la creazione di segreti senza tag o l'esecuzione di istanze Amazon EC2 senza tag e non include eccezioni.
> Il seguente esempio di policy non è compatibile con AWS CloudFormation come scritto, perché quel servizio crea un segreto e quindi lo contrassegna come due passaggi separati. Questa policy di esempio impedisce efficacemente a AWS CloudFormation di creare un segreto come parte di uno stack, perché tale operazione risulterebbe, anche se per breve tempo, nell'esistenza di un segreto che non è contrassegnato come richiesto.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreateSecretWithNoProjectTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
```

```
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoProjectTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyCreateSecretWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    }
  ]
```

```
}
```

Per un elenco di tutti i servizi e tutte le operazioni che supportano sia nelle SCP AWS Organizations sia nelle policy di autorizzazione IAM, consulta Operazioni, risorse e chiavi di condizione per i servizi AWS nella Guida per l'utente di IAM.

Impedire la modifica dei tag se non da parte dei principali autorizzati

La seguente SCP mostra come una policy può consentire solo ai principali autorizzati di modificare i tag associati alle risorse. Questa è una parte importante dell'utilizzo del controllo degli accessi basato su attributi (ABAC) come parte della tua strategia di sicurezza di AWS Cloud. La policy consente a un chiamante di modificare i tag solo su quelle risorse in cui il tag di autorizzazione (in questo esempio `access-project`) corrisponde esattamente allo stesso tag di autorizzazione associato all'utente o al ruolo da cui proviene la richiesta. Inoltre, la policy impedisce all'utente autorizzato di modificare il valore del tag utilizzato per l'autorizzazione. Il principale chiamante deve avere il tag di autorizzazione per apportare qualsiasi modifica.

Questa policy impedisce solo agli utenti non autorizzati di modificare i tag. Un utente autorizzato che non è bloccato da questa policy deve comunque disporre di una policy IAM separata che concede esplicitamente l'autorizzazione `Allow` sulle API di assegnazione di tag pertinenti. Ad esempio, se l'utente dispone di una policy di amministratore con `Allow */*` (consentire tutti i servizi e tutte le operazioni), la combinazione determina l'autorizzazione all'utente amministratore di modificare solo i tag che hanno un valore del tag di autorizzazione corrispondente al valore del tag di autorizzazione associato al principale dell'utente. Questo perché il `Deny` esplicito in questa policy sovrascrive il `Allow` esplicito nella policy di amministratore.

> **Important**
>
> Questa non è una soluzione di policy completa e non deve essere utilizzata come illustrato di seguito. Questo esempio ha lo scopo di illustrare solo una parte di una strategia ABAC e deve essere personalizzato e testato in base agli ambienti di produzione.
> Per la policy completa con un'analisi dettagliata del suo funzionamento, consulta Protezione dei tag delle risorse utilizzati per l'autorizzazione utilizzando una policy di controllo dei servizi in AWS Organizations
> Ricorda di testare le policy basate su rifiuto con i servizi che utilizzi nel tuo ambiente.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "ec2:ResourceTag/access-project": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "access-project"
```

```
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "aws:PrincipalTag/access-project": true
                }
            }
        }
    ]
}
```

SCP di esempio per Amazon Virtual Private Cloud (Amazon VPC)

Esempi in questa categoria

- Impedire agli utenti di eliminare i registri di flusso Amazon VPC
- Impedire a qualsiasi VPC che non dispone già dell'accesso a Internet di ottenerlo

Impedire agli utenti di eliminare i registri di flusso Amazon VPC

Questa SCP impedisce agli utenti o ai ruoli in qualsiasi account interessato di eliminare i registri di flusso Amazon Elastic Compute Cloud (Amazon EC2) o i gruppi di registri o i flussi di registri CloudWatch.

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

```
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteFlowLogs",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": "*"
    }
  ]
 }
```

Impedire a qualsiasi VPC che non dispone già dell'accesso a Internet di ottenerlo

Questa SCP impedisce agli utenti o ai ruoli in qualsiasi account interessato di modificare la configurazione dei Virtual Private Cloud (VPC) Amazon EC2 per concedere loro l'accesso diretto a Internet. Questa SCP non blocca l'accesso diretto esistente né alcun accesso che permette di accedere all'ambiente di rete locale.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:AttachInternetGateway",
        "ec2:CreateInternetGateway",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateVpcPeeringConnection",
        "ec2:AcceptVpcPeeringConnection",
        "globalaccelerator:Create*",
        "globalaccelerator:Update*"
      ],
      "Resource": "*"
    }
  ]
}
```

Gestione delle unità organizzative (UO)

Puoi utilizzare le unità organizzative (UO) per raggruppare gli account e amministrarli come singola unità. Questo semplifica notevolmente la gestione degli account. Ad esempio, collegando un controllo basato su policy a una UO, tutti gli account nella UO erediteranno automaticamente la policy. Puoi creare più UO in una singola organizzazione e UO all'interno di altre UO. Ogni UO può contenere più account, che puoi trasferire da una UO all'altra. Tuttavia, i nomi delle UO devono essere univoci all'interno di una UO padre o root.

> **Note**
>
> C'è un'unica radice nell'organizzazione, che AWS Organizations viene creata automaticamente quando si configura l'organizzazione per la prima volta.

Argomenti

Puoi anche esaminare tutte le unità organizzative della tua organizzazione. Per ulteriori informazioni, consulta Visualizzazione dei dettagli di una unità organizzativa.

Esplorazione della root e della gerarchia delle UO

Per passare a diverse UO o al root durante il trasferimento degli account o il collegamento delle policy, puoi utilizzare la visualizzazione di default ad albero.

AWS Management Console

Per navigare nell'organizzazione come "albero"

1. Accedi alla consoleAWS 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. Nella pagina Account AWS, nella parte superiore della sezione Organization (Organizzazione), seleziona Hierarchy (Gerarchia) (invece che List (Elenco).
3. Inizialmente la struttura mostra il root, visualizzando solo il primo livello di UO e account figli. Per espandere la struttura e visualizzare ulteriori livelli, scegli l'icona Espandi ( ) accanto a un'entità padre. Per ridurre la quantità di elementi visualizzati e comprimere un ramo dell'albero, scegli l'icona comprimi ( ) accanto a un'entità padre espansa.
4. Scegli il nome di un'unità organizzativa o root per visualizzarne i dettagli ed eseguire determinate operazioni. In alternativa, puoi scegliere il pulsante di opzione accanto al nome ed eseguire determinate operazioni su tale entità nel menu Actions (Operazioni).

È inoltre possibile visualizzare l'elenco dei soli account dell'organizzazione in forma tabulare, senza dover passare da un'unità organizzativa per trovarli. In questa visualizzazione non è possibile visualizzare le unità organizzative o modificare le policy ad esse associate.

AWS Management Console

Per visualizzare l'organizzazione come un elenco semplice di account senza gerarchia

1. Accedi alla consoleAWS 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. Nella Account AWSpagina, nella parte superiore della sezione Organizzazione, scegli l'icona dell'interruttore Visualizza Account AWS solo per attivarla.  .
3. L'elenco degli account viene visualizzato senza alcuna gerarchia.

Creazione di una UO

Quando effettui l'accesso all'account di gestione della tua organizzazione, puoi creare un'UO nel root dell'organizzazione. Le UO possono essere nidificate fino a cinque livelli di profondità. Per creare una UO, completa le fasi seguenti.

Important

Se questa organizzazione è gestita con AWS Control Tower, crea le tue unità organizzative con la AWS Control Tower console o le API. Se si crea l'unità organizzativa in Organizations, l'unità organizzativa non è registrata presso AWS Control Tower. Per ulteriori informazioni, consulta Riferimento alle risorse esterne a AWS Control Tower nella Guida per l'utente diAWS Control Tower .

Autorizzazioni minime

Per creare una UO che si trova in una root nella tua organizzazione, devi disporre delle seguenti autorizzazioni:

- `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations
- `organizations:CreateOrganizationalUnit`

AWS Management Console

Per creare un'unità organizzativa

1. Accedi alla consoleAWS 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. Accedi alla pagina Account AWS.

   La console mostra i contenuti del root dell'UO e i rispettivi contenuti. La prima volta che si visita un root, la console visualizza tutti gli Account AWS in quella visualizzazione di livello superiore. Se precedentemente si sono create delle UO in cui sono stati trasferiti degli

account, la console mostra solo le UO di livello superiore e gli account che non sono ancora stati trasferiti in una UO.

3. (Facoltativo) Se desideri creare una UO all'interno di una UO esistente, individua la UO figlia scegliendo il relativo nome (non la casella di controllo) oppure scegliendo la 
accanto alle UO nella visualizzazione ad albero fino a individuare quella desiderata, poi selezionane il nome.
4. Dopo avere selezionato l'unità organizzativa padre corretta nella gerarchia, nel menu Actions (Operazioni), in Organizational Unit (Unità organizzativa), scegli Create new (Crea nuova)
5. Nella finestra di dialogo Create organizational unit (Crea unità organizzativa), digita il nome della UO che desideri creare.
6. (Facoltativo) Per aggiungere uno o più tag, scegli Add tag (Aggiungi tag) e quindi inserisci una chiave e un valore facoltativo. Lasciando vuoto il valore, questo viene impostato su una stringa vuota; non è `null`. Puoi associare fino a 50 tag a un'UO.
7. Infine, scegli Create organizational unit (Crea unità organizzativa).

La nuova UO viene visualizzata all'interno del padre. A questo punto, è possibile trasferire gli account in questa unità organizzativa oppure collegarvi le policy.

AWS CLI & AWS SDKs

Per creare un'unità organizzativa

Per creare una UO, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: create-organizational-unit

  Per creare un'unità organizzativa, è innanzitutto necessario individuare l'identità del root o dell'unità organizzativa che desideri configurare come padre della nuova unità organizzativa.

  Per trovare l'identità del root, utilizza il comando list-roots. Per trovare l'identità di un'unità organizzativa, utilizza il comando list-children per passare all'unità organizzativa desiderata.

  Nell'esempio seguente viene illustrato come trovare l'identità del root e quindi individuare l'identità di un'unità organizzativa sotto il root. L'ultimo comando mostra come creare una nuova unità organizzativa nell'UO trovata.

  ```
  $ aws organizations list-roots
  ```

```
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
        }
    ]
}
$ aws organizations list-children \
    --parent-id r-a1b2 \
    --child-type ORGANIZATIONAL_UNIT
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
$ aws organizations create-organizational-unit \
    --parent-id ou-a1b2-f6g7h111 \
    --name New-Child-OU
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "New-Child-OU"
    }
}
```

- AWS SDK: CreateOrganizationalUnit

Ridenominazione di una UO

Quando effettui l'accesso all'account di gestione della tua organizzazione, puoi rinominare un'UO. Per farlo, completa le seguenti fasi.

Autorizzazioni minime

Per rinominare un'unità organizzativa all'interno di una cartella principale AWS dell'organizzazione, è necessario disporre delle seguenti autorizzazioni:

- `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations
- `organizations:UpdateOrganizationalUnit`

AWS Management Console

Per rinominare un'unità organizzativa

1. Accedi alla consoleAWS 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. Nella pagina Account AWS, vai all'unità organizzativa da rinominare e quindi esegui una delle operazioni seguenti:
   - Scegli il pulsante di opzione

     accanto all'UO da rinominare. Quindi, nel menu Actions (Operazioni), in Organizational unit (Unità organizzativa) scegli Rename (Rinomina).
   - Scegli il nome dell'unità organizzativa per accedere alla pagina dei dettagli dell'unità organizzativa. Nella parte superiore della pagina, scegli Rename (Rinomina).
3. Nella finestra di dialogo Rename organizational unit (Rinomina unità organizzativa), inserisci un nuovo nome, quindi scegli Save changes (Salva modifiche).

AWS CLI & AWS SDKs

Per rinominare un'unità organizzativa

Per rinominare una UO, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: update-organizational-unit

L'esempio seguente mostra come rinominare un'UO.

```
$ aws organizations update-organizational-unit \
    --organizational-unit-id ou-a1b2-f6g7h222 \
    --name "Renamed-OU"
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "Renamed-OU"
    }
}
```

- AWS SDK: UpdateOrganizationalUnit

Modifica dei tag collegati a un'unità organizzativa

Quando effettui l'accesso all'account di gestione dell'organizzazione, puoi aggiungere o rimuovere i tag collegati a una UO. Per farlo, completa le seguenti fasi.

Autorizzazioni minime

Per modificare i tag allegati a un'unità organizzativa all'interno di una cartella principale AWS dell'organizzazione, è necessario disporre delle seguenti autorizzazioni:

- `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations
- `organizations:DescribeOrganizationalUnit` - Obbligatorio solo quando si utilizza la console Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Per modificare i tag collegati a un'unità organizzativa

1. Accedi alla consoleAWS 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. Nella pagina Account AWS, vai al nome dell'unità organizzativa di cui desideri modificare i tag e selezionalo.
3. Nella pagina dei dettagli dell'UO, scegli la scheda Tags, quindi scegli Manage tags (Gestisci tag).
4. In questa scheda puoi eseguire le seguenti operazioni:
   - Modifica il valore di un tag inserendo un nuovo valore rispetto a quello precedente. Non puoi modificare la chiave di tag. Per cambiare una chiave, devi eliminare il tag con la vecchia chiave e aggiungere un tag con la nuova chiave.
   - Rimuovi un tag esistente scegliendo Remove (Rimuovi) accanto al tag da rimuovere.
   - Aggiungi una nuova coppia chiave e valore di tag. Scegli Add tag (Aggiungi tag), quindi inserisci il nuovo nome della chiave e il valore facoltativo nelle caselle fornite. Se lasci vuota la casella Value (Valore), il valore è una stringa vuota; non è `null`.
5. Scegli Save changes (Salva le modifiche) dopo avere apportato tutte le aggiunte, le rimozioni e le modifiche opportune.

AWS CLI & AWS SDKs

Per modificare i tag collegati a un'unità organizzativa

Per modificare i tag collegati a un'UO, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: tag-resource e untag-resource

  L'esempio seguente collega il tag `"Department"="12345"` a un'UO. Nota che `Key` e `Value` fanno distinzione tra lettere maiuscole e minuscole.

```
$ aws organizations tag-resource \
    --resource-id ou-a1b2-f6g7h222 \
    --tags Key=Department,Value=12345
```

Questo comando non produce alcun output se ha esito positivo.

L'esempio seguente rimuove il tag `Department` da un'UO.

```
$ aws organizations untag-resource \
    --resource-id ou-a1b2-f6g7h222 \
    --tag-keys Department
```

Questo comando non produce alcun output se ha esito positivo.

- AWS SDK: e TagResourceUntagResource

Trasferimento di un account a un'UO o tra root e UO

Quando effettui l'accesso all'account di gestione della tua organizzazione, puoi trasferire gli account nell'organizzazione dal root a un'UO, da un'UO a un'altra o di nuovo al root da un'UO. Collocandolo all'interno di un'UO, un account sarà soggetto alle eventuali policy collegate all'UO padre e a qualsiasi altra UO nel padre fino al root. Se non si trova in un'UO, un account sarà soggetto solo alle policy collegate direttamente al root e a quelle eventualmente collegate direttamente all'account. Per trasferire degli account, completa i seguenti passaggi.

> **Autorizzazioni minime**
>
> Per trasferire gli account in una nuova posizione nella gerarchia delle UO, devi disporre delle seguenti autorizzazioni:
>
> - `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations
> - `organizations:MoveAccount`

AWS Management Console

Per trasferire gli account in una UO

1. Accedi alla consoleAWS 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. Nella pagina Account AWS, individua l'account o gli account che desideri spostare. È possibile spostarsi nella gerarchia delle unità organizzative o abilitare View Account AWS only (Visualizza solo gli Account AWS) per visualizzare un elenco dei soli account senza la struttura dell'unità organizzativa. Se hai molti account, potresti dover scegliere Load more accounts (Carica più account) in 'nome-UO' nella parte inferiore dell'elenco per trovare tutti gli oggetti da spostare.
3. Seleziona la casella di controllo
   
   accanto al nome di ciascun account da spostare.
4. Nel menu Actions (Operazioni), in Account AWS scegli Move (Sposta).
5. Nella finestra di dialogo Move (Trasferisci) Account AWS, scegli l'UO o il root in cui desideri trasferire gli account, quindi scegli Move (Trasferisci) Account AWS.

AWS CLI & AWS SDKs

Per trasferire un account in un'UO

Per trasferire un account, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: move-account

  L'esempio seguente sposta an Account AWS dalla radice a un'unità organizzativa. Nota: è necessario specificare gli ID dei container sia di origine sia di destinazione.

  ```
  $ aws organizations move-account \
      --account-id 111122223333 \
      --source-parent-id r-a1b2 \
      --destination-parent-id ou-a1b2-f6g7h111
  ```

  Questo comando non produce alcun output se ha esito positivo.
- AWS SDK: MoveAccount

Eliminazione di UO

Quando effettui l'accesso all'account di gestione della tua organizzazione, puoi eliminare le UO di cui non hai più bisogno.

Dovrai prima trasferire tutti gli account fuori dalla UO e da qualsiasi UO figlia, quindi potrai procedere con l'eliminazione delle UO figlie.

> **Autorizzazioni minime**
>
> Per eliminare una UO, devi disporre delle seguenti autorizzazioni:
>
> - `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations
> - `organizations:DeleteOrganizationalUnit`

AWS Management Console

Per eliminare un'UO

1. Accedi alla consoleAWS 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. Nella pagina Account AWS, individua le UO che desideri eliminare e seleziona la casella di controllo
   ☑
   accanto al nome di ciascuna unità organizzativa.
3. Scegli Actions (Operazioni) e quindi in Organizational unit (Unità organizzativa) scegli Delete (Elimina).
4. Per confermare che desideri eliminare le unità organizzative, inserisci il nome dell'unità organizzativa (se hai scelto di eliminarne solo una) o la parola "delete" (elimina) (se hai scelto di eliminarne diverse), quindi seleziona Delete (Elimina).

   AWS Organizations elimina le unità organizzative e le rimuove dall'elenco.

AWS CLI & AWS SDKs

Per eliminare un'UO

Per eliminare una UO, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: delete-organizational-unit

L'esempio seguente mostra come eliminare un'UO.

```
$ aws organizations delete-organizational-unit \
    --organizational-unit-id ou-a1b2-f6g7h222
```

Questo comando non produce alcun output se ha esito positivo.

- AWS SDK: DeleteOrganizationalUnit

Tagging delle risorse AWS Organizations

Un tag è un'etichetta di attributi personalizzata aggiunta a una risorsa AWS per semplificare l'identificazione, l'organizzazione e la ricerca delle risorse. Ogni tag è costituito da due parti:

- Una chiave del tag (ad esempio, `CostCenter`, `Environment` o `Project`). Le chiavi dei tag fanno distinzione tra maiuscole e minuscole e possono contenere fino a 128 caratteri.
- Un valore di tag (ad esempio, `111122223333` oppure `Production`). I valori dei tag fanno distinzione tra maiuscole e minuscole e possono contenere fino a 256 caratteri. È possibile impostare il valore di un tag su una stringa vuota, ma non su null. Non specificare il valore del tag equivale a utilizzare una stringa vuota.

Per ulteriori informazioni sui caratteri consentiti in una chiave o in un valore di tag, consulta il Parametro dei tag dell'API di tag nella Documentazione di riferimento delle API - Assegnazione di tag in Resource Groups.

È possibile utilizzare i tag per suddividere le risorse in categorie in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Per ulteriori informazioni, consulta Best practice per l'etichettatura AWS delle risorse.

> **Tip**
>
> Puoi utilizzare le policy di tag per standardizzare i tag tra le risorse degli account dell'organizzazione.

Al momento, AWS Organizations supporta le seguenti operazioni di assegnazione di tag quando si esegue l'accesso con l'account di gestione:

- Puoi aggiungere tag ai seguenti tipi di risorse dell'organizzazione:
  - Account AWS
  - Unità organizzative
  - Il root dell'organizzazione
  - Policy

È possibile aggiungere tag nelle seguenti occasioni:

- Quando si crea la risorsa - Specifica i tag nella console Organizations oppure utilizza il parametro `Tags` con una delle operazioni API `Create`. Questo non è applicabile al root dell'organizzazione.
- Dopo avere creato la risorsa - Utilizza la console Organizations o richiama l'operazione `TagResource`.

Puoi visualizzare i tag su una delle risorse taggabili in AWS Organizations utilizzando la console o richiamando l'operazione `ListTagsForResource`.

Puoi rimuovere i tag da una risorsa specificando le chiavi da rimuovere mediante la console o richiamando l'operazione `UntagResource`.

Utilizzo dei tag

I tag aiutano a organizzare le risorse consentendo di raggrupparle in base alle categorie più utili. Ad esempio, è possibile assegnare un tag "Reparto" che tiene traccia del reparto proprietario. Puoi assegnare un tag "Ambiente" per monitorare se una determinata risorsa fa parte degli ambienti x, y o z o di produzione.

Puoi usare i tag anche per:

- Applica gli standard di tagging alle tue risorse.
- Controlla chi può accedere alle risorse.

Aggiunta, aggiornamento e rimozione di tag

Quando hai effettuato l'accesso all'account di gestione della tua organizzazione, puoi aggiungere tag alle risorse all'interno dell'organizzazione.

Aggiunta dei tag durante la creazione di una risorsa

> **Autorizzazioni minime**
>
> Per aggiungere tag a una risorsa quando viene creata, è necessario disporre delle seguenti autorizzazioni:
>
> - Autorizzazione a creare una risorsa del tipo specificato

- `organizations:TagResource`
- `organizations:ListTagsForResource` - Obbligatorio solo quando si utilizza la console Organizations

Durante la creazione, puoi includere le chiavi e i valori dei tag associati alle seguenti risorse.

- Account AWS
  - Account creato
  - Account invitato
- Unità organizzativa (UO)
- Policy
  - Policy di rifiuto dei servizi di IA
  - Policy di backup
  - Policy di controllo dei servizi
  - Policy di tag

Il root dell'organizzazione viene creato nel momento della creazione iniziale dell'organizzazione, quindi è possibile aggiungervi tag solo come risorsa esistente.

Aggiunta o aggiornamento di tag per una risorsa esistente

Puoi inoltre aggiungere nuovi tag o aggiornare i valori dei tag associati alle risorse esistenti.

Autorizzazioni minime

Per aggiungere o aggiornare i tag alle risorse nell'organizzazione, è necessario disporre delle seguenti autorizzazioni:

- `organizations:TagResource`
- `organizations:ListTagsForResource` - Obbligatorio solo quando si utilizza la console Organizations

Per rimuovere i tag dalle risorse nell'organizzazione, è necessario disporre delle seguenti autorizzazioni:

- `organizations:UntagResource`

AWS Management Console

Per aggiungere, aggiornare o rimuovere i tag di una risorsa esistente

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. Vai all'account, al root, all'unità organizzativa o alla policy, scegli quello di tuo interesse e fai clic sul relativo nome per aprire la pagina dei dettagli.
3. Nella scheda Tag scegliere Gestisci tag.
4. È possibile aggiungere nuovi tag, modificare i valori dei tag esistenti o rimuovere i tag.

   Per aggiungere un tag, seleziona Add tag (Aggiungi tag), quindi inserisci una Chiave e, se desideri, specifica un valore per il tag.

   Per rimuovere un tag, scegli Remove (Rimuovi).

   I valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole. Usa la distinzione tra maiuscole e minuscole che si desidera standardizzare. È inoltre necessario rispettare i requisiti di tutte le policy di tag applicabili.
5. Ripeti il passaggio precedente per il numero di volte necessarie.
6. Seleziona Salvataggio delle modifiche.

AWS CLI & AWS SDKs

Per aggiungere o aggiornare i tag di una risorsa esistente

È possibile utilizzare uno dei seguenti comandi per aggiungere i tag alle risorse taggabili nell'organizzazione:

- AWS CLI: tag-resource
- AWSSDK: TagResource

Per eliminare tag da una risorsa nell'organizzazione

Per eliminare i tag, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: untag-resource
- AWSSDK: UntagResource

Uso di AWS Organizations con altri servizi AWS

Puoi utilizzare l'accesso attendibile per abilitare un servizio AWS supportato, denominato servizio attendibile, per eseguire attività all'interno della tua organizzazione e dei relativi account per tuo conto. Ciò comporta la concessione di autorizzazioni al servizio attendibile, ma non influisce in altro modo sulle autorizzazioni degli utenti o dei ruoli. Quando abiliti l'accesso, il servizio attendibile può creare un ruolo IAM denominato ruolo collegato ai servizi in ogni account dell'organizzazione, ogni qualvolta il ruolo sia necessario. Questo ruolo possiede una policy di autorizzazioni che consente il servizio sicuro per eseguire le attività descritte nella documentazione del servizio. Ciò consente di specificare le impostazioni e i dettagli di configurazione che desideri vengano mantenute negli account dell'organizzazione per tuo conto dal servizio sicuro. Il servizio attendibile crea ruoli collegati al servizio solo quando è necessario eseguire operazioni di gestione sugli account e non necessariamente in tutti gli account dell'organizzazione.

Important

Consigliamo vivamente di abilitare e disabilitare l'accesso attendibile, quando l'opzione è disponibile, utilizzando solo la console del servizio attendibile oppure le operazioni dell'AWS CLI o dell'API equivalenti. Ciò consente al servizio attendibile di eseguire qualsiasi inizializzazione richiesta quando si abilita l'accesso attendibile, ad esempio la creazione di tutte le risorse richieste e la pulizia delle risorse necessarie quando si disabilita l'accesso attendibile.
Per informazioni su come abilitare o disabilitare l'accesso al servizio attendibile all'organizzazione tramite il servizio attendibile, consulta il link Ulteriori informazioni nella colonna Supporta l'accesso attendibile alla pagina AWS servizi che puoi utilizzare con AWS Organizations.
Se disabiliti l'accesso utilizzando la console Organizations, i comandi della CLI o le operazioni API, si verificano le seguenti operazioni:

- Il servizio non può più creare un ruolo collegato ai servizi negli account dell'organizzazione. Ciò significa che il servizio non può eseguire operazioni per tuo conto su nuovi account nell'organizzazione. Il servizio può ancora eseguire operazioni in account meno recenti fino a quando non completa la pulizia da AWS Organizations.
- Il servizio non può più eseguire attività negli account membro dell'organizzazione, a meno che tali operazioni non siano esplicitamente consentite dalle policy IAM associate ai ruoli.

Ciò include qualsiasi aggregazione di dati dagli account membro all'account di gestione o a un account di amministratore delegato, se applicabile.

- Alcuni servizi rilevano questa modifica e ripuliscono tutti i dati o le risorse rimanenti relativi all'integrazione, mentre altri servizi smettono di accedere all'organizzazione ma lasciano in atto tutti i dati e la configurazione storici per supportare una possibile riabilitazione dell'integrazione.

L'utilizzo della console o dei comandi dell'altro servizio per disabilitare l'integrazione garantisce invece che l'altro servizio possa ripulire tutte le risorse richieste esclusivamente per l'integrazione. Il modo in cui il servizio ripulisce le proprie risorse negli account dell'organizzazione dipende da tale servizio. Per ulteriori informazioni, consulta la documentazione dell'altro servizio AWS.

Autorizzazioni necessarie per abilitare l'accesso sicuro

L'accesso sicuro richiede le autorizzazioni per due servizi: AWS Organizations e il servizio sicuro. Per abilitare l'accesso sicuro, scegli uno dei seguenti scenari:

- Se disponi delle credenziali con le autorizzazioni sia in AWS Organizations e nel servizio attendibile, abilita l'accesso utilizzando gli strumenti (la console o AWS CLI) disponibili nel servizio attendibile. Ciò consente al servizio di abilitare l'accesso attendibile a AWS Organizations per tuo conto e di creare tutte le risorse necessarie affinché il servizio funzioni nella tua organizzazione.

  Le autorizzazioni minime per queste credenziali sono le seguenti:

  - `organizations:EnableAWSServiceAccess`. Puoi anche utilizzare la condizione chiave `organizations:ServicePrincipal` con questa operazione per limitare le richieste che tali operazioni effettuano a un elenco dei principali nomi di servizio approvati. Per ulteriori informazioni, consulta Chiavi di condizione.
  - `organizations:ListAWSServiceAccessForOrganization` - Obbligatoria se si utilizza la console di AWS Organizations.
  - Le autorizzazioni minime necessarie per il servizio sicuro dipende dal servizio. Per ulteriori informazioni, consulta la documentazione del servizio sicuro.
- Se una persona dispone delle credenziali con le autorizzazioni in AWS Organizations, ma un'altra persona dispone delle credenziali con le autorizzazioni nel servizio sicuro, esegui questi passaggi nel seguente ordine:

1. La persona che dispone delle credenziali con le autorizzazioni in AWS Organizations deve utilizzare la console di AWS Organizations, la AWS CLI o un SDK AWS per abilitare l'accesso sicuro per il servizio sicuro. Ciò autorizza l'altro servizio a eseguire la configurazione richiesta nell'organizzazione quando viene eseguito il seguente passaggio (passaggio 2).

   Le autorizzazioni minime per AWS Organizations sono le seguenti:

   - `organizations:EnableAWSServiceAccess`
   - `organizations:ListAWSServiceAccessForOrganization` - Obbligatoria solo se si utilizza la console di AWS Organizations

   Per i passaggi per abilitare l'accesso sicuro in AWS Organizations, consulta Come abilitare o disabilitare l'accesso sicuro.

2. La persona che dispone delle credenziali con le autorizzazioni nel servizio sicuro consente a quel servizio di funzionare con AWS Organizations. Ciò indica al servizio di eseguire qualsiasi inizializzazione richiesta, ad esempio la creazione di tutte le risorse necessarie per il funzionamento del servizio sicuro nell'organizzazione. Per ulteriori informazioni, consulta le istruzioni specifiche del servizio alla pagina AWS servizi che puoi utilizzare con AWS Organizations.

Autorizzazioni necessarie per disabilitare l'accesso sicuro

Quando non desideri più consentire al servizio sicuro di operare nella tua autorizzazione o nel relativo account, scegli uno dei seguenti scenari.

> **Important**
>
> Disabilitare l'accesso al servizio sicuro non impedisce agli utenti e ai ruoli con le autorizzazioni appropriate di utilizzare quel servizio. Per bloccare completamente gli utenti e i ruoli dall'accesso a un servizio AWS, puoi rimuovere le autorizzazioni IAM che concedono tale accesso, oppure puoi utilizzare le policy di controllo dei servizi (SCP) in AWS Organizations.
> Puoi applicare le SCP solo agli account membri. Le SCP non sono applicabili all'account di gestione. Ti consigliamo di non eseguire servizi nell'account di gestione. Consigliamo invece di eseguirli negli account membri in cui puoi controllare la sicurezza tramite le SCP.

- Se disponi delle credenziali con le autorizzazioni in entrambi AWS Organizations e servizio sicuro, disabilita l'accesso utilizzando gli strumenti (console o AWS CLI) disponibili nel servizio sicuro. Il servizio quindi pulisce rimuovendo le risorse che non sono più necessarie e disabilitando l'accesso sicuro per il servizio in AWS Organizations per tuo conto.

  Le autorizzazioni minime per queste credenziali sono le seguenti:

  - `organizations:DisableAWSServiceAccess`. Puoi anche utilizzare la condizione chiave `organizations:ServicePrincipal` con questa operazione per limitare le richieste che tali operazioni effettuano a un elenco dei principali nomi di servizio approvati. Per ulteriori informazioni, consulta Chiavi di condizione.
  - `organizations:ListAWSServiceAccessForOrganization` - Obbligatoria se si utilizza la console di AWS Organizations.
  - Le autorizzazioni minime necessarie per il servizio sicuro dipendono dal servizio. Per ulteriori informazioni, consulta la documentazione del servizio sicuro.
- Se le credenziali con le autorizzazioni in AWS Organizations non sono le credenziali con le autorizzazioni nel servizio sicuro, esegui questi passaggi nel seguente ordine:

  1. La persona con le autorizzazioni nel servizio sicuro disabilita innanzitutto l'accesso tramite il servizio. Questo indica al servizio trusted di pulire rimuovendo le risorse necessarie per il servizio sicuro. Per ulteriori informazioni, consulta le istruzioni specifiche del servizio alla pagina AWS servizi che puoi utilizzare con AWS Organizations.
  2. La persona con le autorizzazioni in AWS Organizations può quindi utilizzare la console AWS Organizations o AWS CLI o un SDK AWS per disabilitare l'accesso per il servizio sicuro. Ciò rimuove le autorizzazioni per il servizio sicuro dall'organizzazione e dal relativo account.

     Le autorizzazioni minime per AWS Organizations sono le seguenti:

     - `organizations:DisableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization` - Obbligatoria solo se si utilizza la console di AWS Organizations

     Per i passaggi per disabilitare l'accesso sicuro in AWS Organizations, consulta Come abilitare o disabilitare l'accesso sicuro.

Come abilitare o disabilitare l'accesso sicuro

Se disponi delle autorizzazioni solo per AWS Organizations e desideri abilitare o disabilitare l'accesso sicuro alla tua organizzazione per conto dell'amministratore dell'altro servizio AWS, utilizza la seguente procedura.

Important

Consigliamo vivamente di abilitare e disabilitare l'accesso attendibile, quando l'opzione è disponibile, utilizzando solo la console del servizio attendibile oppure le operazioni dell'AWS CLI o dell'API equivalenti. Ciò consente al servizio attendibile di eseguire qualsiasi inizializzazione richiesta quando si abilita l'accesso attendibile, ad esempio la creazione di tutte le risorse richieste e la pulizia delle risorse necessarie quando si disabilita l'accesso attendibile.
Per informazioni su come abilitare o disabilitare l'accesso al servizio attendibile all'organizzazione tramite il servizio attendibile, consulta il link Ulteriori informazioni nella colonna Supporta l'accesso attendibile alla pagina AWS servizi che puoi utilizzare con AWS Organizations.
Se disabiliti l'accesso utilizzando la console Organizations, i comandi della CLI o le operazioni API, si verificano le seguenti operazioni:

- Il servizio non può più creare un ruolo collegato ai servizi negli account dell'organizzazione. Ciò significa che il servizio non può eseguire operazioni per tuo conto su nuovi account nell'organizzazione. Il servizio può ancora eseguire operazioni in account meno recenti fino a quando non completa la pulizia da AWS Organizations.
- Il servizio non può più eseguire attività negli account membro dell'organizzazione, a meno che tali operazioni non siano esplicitamente consentite dalle policy IAM associate ai ruoli. Ciò include qualsiasi aggregazione di dati dagli account membro all'account di gestione o a un account di amministratore delegato, se applicabile.
- Alcuni servizi rilevano questa modifica e ripuliscono tutti i dati o le risorse rimanenti relativi all'integrazione, mentre altri servizi smettono di accedere all'organizzazione ma lasciano in atto tutti i dati e la configurazione storici per supportare una possibile riabilitazione dell'integrazione.

L'utilizzo della console o dei comandi dell'altro servizio per disabilitare l'integrazione garantisce invece che l'altro servizio possa ripulire tutte le risorse richieste esclusivamente per l'integrazione. Il modo in cui il servizio ripulisce le proprie risorse negli account

dell'organizzazione dipende da tale servizio. Per ulteriori informazioni, consulta la documentazione dell'altro servizio AWS.

AWS Management Console

Per abilitare l'accesso al servizio attendibile

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. Nella pagina Services (Servizi), trova la riga per il servizio che desideri abilitare e scegline il nome.
3. Scegliere Enable trusted access (Abilita accesso sicuro).
4. Nella finestra di dialogo di conferma, seleziona la casella Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
5. Se stai abilitando l'accesso, informa l'amministratore dell'altro servizio AWS che ora è possibile abilitare l'altro servizio il funzionamento con le AWS Organizations.

Per disabilitare l'accesso al servizio attendibile

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. Nella pagina Services (Servizi), trova la riga per il servizio che desideri disabilitare e scegline il nome.
3. Attendi fino a quando l'amministratore non ti informa che il servizio è disabilitato e che le relative risorse sono state pulite.
4. Nella finestra di dialogo di conferma, inserisci **`disable`** nella casella, quindi scegli Disable trusted access (Disabilita accesso attendibile).

AWS CLI, AWS API

Per abilitare o disabilitare l'accesso al servizio attendibile

Puoi utilizzare i seguenti comandi AWS CLI oppure le operazioni API per abilitare o disabilitare l'accesso al servizio sicuro:

- AWS CLI: AWS organizations enable-aws-service-access
- AWS CLI: AWS organizations disable-aws-service-access
- API AWS: EnableAWSServiceAccess
- API AWS: DisableAWSServiceAccess

AWS Organizations e ruoli collegati ai servizi

AWS Organizations utilizza ruoli collegati ai servizi IAM per abilitare i servizi attendibili a eseguire attività per tuo conto negli account membri dell'organizzazione. Quando configuri un servizio sicuro e lo autorizzi a integrarsi con la tua organizzazione, tale servizio può richiedere che AWS Organizations crei un ruolo collegato ai servizi nel proprio account membro. Il servizio sicuro crea i ruoli in modo asincrono in base alle esigenze e non necessariamente in tutti gli account dell'organizzazione allo stesso tempo. Il ruolo collegato ai servizi possiede le autorizzazioni IAM predefinite che permettono al servizio attendibile di eseguire soltanto attività specifiche all'interno di tale account. In generale, AWS gestisce tutti i ruoli collegati ai servizi, il che significa che in genere non puoi modificare i ruoli o le policy collegate.

Per rendere possibile tutto ciò, quando crei un account in un'organizzazione o accetti un invito a unire l'account esistente a un'organizzazione, AWS Organizations dota l'account membro di un ruolo collegato ai servizi, denominato `AWSServiceRoleForOrganizations`. Solo il servizio AWS Organizations può assumere questo ruolo. Il ruolo dispone delle autorizzazioni che permettono a AWS Organizations di creare ruoli collegati ai servizi per altri servizi AWS. Questo ruolo collegato ai servizi è presente in tutte le organizzazioni.

Anche se non è consigliabile, se la tua organizzazione ha solo le caratteristiche di fatturazione consolidata abilitate, il ruolo collegato ai servizi denominato `AWSServiceRoleForOrganizations` non viene mai utilizzato e puoi eliminarlo. Se in seguito desideri abilitare tutte le caratteristiche della tua organizzazione, il ruolo è obbligatorio ed è necessario ripristinarlo. I seguenti controlli si verificano all'inizio della procedura per abilitare tutte le caratteristiche:

- Per ogni account membro che è stato invitato a unirsi all'organizzazione - L'amministratore dell'account riceve una richiesta per accettare di abilitare tutte le caratteristiche. Per accettare con successo la richiesta, l'amministratore deve disporre di entrambe le autorizzazioni `organizations:AcceptHandshake` `eiam:CreateServiceLinkedRole` se il ruolo

collegato al servizio (`AWSServiceRoleForOrganizations`) non esiste già. Se il `AWSServiceRoleForOrganizations` ruolo esiste già, l'amministratore necessita solo dell'autorizzazione `organizations:AcceptHandshake` per accettare la richiesta. Quando l'amministratore accetta la richiesta, AWS Organizations crea il ruolo collegato ai servizi, se non esiste già.

- Per ogni account membro che è stato creato nell'organizzazione - L'amministratore dell'account riceve una richiesta per creare nuovamente il ruolo collegato ai servizi. (L'amministratore dell'account membro non riceve una richiesta per abilitare tutte le caratteristiche in quanto l'amministratore dell'account di gestione (in precedenza noto come "account principale") è considerato il proprietario dell'account membro creato). AWS Organizations crea il ruolo collegato ai servizi quando l'amministratore dell'account membro accetta la richiesta. L'amministratore deve disporre di entrambe le autorizzazioni `organizations:AcceptHandshake` e `iam:CreateServiceLinkedRole` per accettare con successo l'handshake.

Dopo aver abilitato tutte le caratteristiche nella tua organizzazione, non puoi più eliminare il ruolo collegato ai servizi `AWSServiceRoleForOrganizations` da qualsiasi account.

> **Important**
>
> Gli SCP AWS Organizations non influiscono mai sui ruoli collegati ai servizi. Questi ruoli sono esenti da qualsiasi restrizione SCP.

AWS servizi che puoi utilizzare con AWS Organizations

Con AWS Organizations puoi svolgere attività di gestione degli account su larga scala consolidandone più di una Account AWS in un'unica organizzazione. Il consolidamento degli account semplifica l'utilizzo di altri servizi. AWS È possibile sfruttare i servizi di gestione multiaccount disponibili in AWS Organizations determinati AWS servizi per eseguire attività su tutti gli account membri dell'organizzazione.

La tabella seguente elenca AWS i servizi che è possibile utilizzare e AWS Organizations i vantaggi derivanti dall'utilizzo di ciascun servizio a livello di organizzazione.

Accesso affidabile: è possibile abilitare un AWS servizio compatibile per eseguire operazioni in tutta l'organizzazione Account AWS . Per ulteriori informazioni, consulta Uso di AWS Organizations con altri servizi AWS.

Amministratore delegato per AWS i servizi: un AWS servizio compatibile può registrare un account AWS membro nell'organizzazione come amministratore degli account dell'organizzazione in quel servizio. Per ulteriori informazioni, consulta Amministratore delegato per i servizi AWS che funzionano con Organizations.

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
AWS Account Management Gestisci tutti i dettagli e i metadati della Account AWS tua organizzazione.	Puoi creare, aggiornare ed eliminare le informazioni di contatto alternative per tutti gli account nell'organizzazione.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	
AWS Servizio di migrazione delle applicazioni (MGN) AWS Application Migration Service	Puoi gestire migrazioni su larga scala su più account.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
consente lift-and-shift alle aziende di AWS accedere a un gran numero di server fisici, virtuali o cloud senza problemi di compatibilità, interruzioni delle prestazioni o lunghi intervalli di tempo.				
AWS Artifact Scarica i report AWS sulla conformità alla sicurezza come i report ISO e PCI.	È possibile accettare accordi per conto di tutti gli account all'interno dell'organizzazione.	 Sì Ulteriori informazioni	 Sì Per informazioni, consulta AWS Artifact.	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
AWS Audit Manager Automatizza la raccolta continua di prove per aiutarti a verificare l'utilizzo dei servizi cloud.	Verifica continuamente il tuo AWS utilizzo su più account della tua organizzazione per semplificare la valutazione del rischio e della conformità.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
AWS Backup Gestisce e monitora i backup di tutti gli account nell'organizzazione.	È possibile configurare e gestire piani di backup per l'intera organizzazione o per gruppi di account nelle unità organizzative. È possibile monitorare centralmente i backup di tutti gli account.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
StackSets AWS CloudFormation Creazione, aggiornamento o eliminazione di stack in più account e regioni con un'unica operazione.	Un utente nell'account di gestione o un account di amministratore delegato può creare un set di stack con autorizzazioni gestite dal servizio che implementa istanze di stack negli account dell'organizzazione.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato
AWS CloudTrail Abilita la funzionalità di audit a livello di governance, conformità, rischi e operatività per l'account.	Un utente in un account di gestione o un account amministratore delegato può creare un trail dell'organizzazione o un archivio dati degli eventi che registra tutti gli eventi per tutti gli account nell'organizzazione.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
AWS Compute Optimizer Ottieni consigli per l'ottimizzazione dell' AWS elaborazione.	È possibile analizzare tutte le risorse presenti negli account dell'organizzazione per ottenere consigli per l'ottimizzazione. Per ulteriori informazioni, consulta Account supportati da Compute Optimizer nella Guida per l'utente	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	di AWS Compute Optimizer.			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
AWS Config Valuta, controlla e verifica le configurazioni delle risorse AWS .	È possibile ottenere una visione dello stato di conformità a livello di organizzazione. Puoi anche utilizzare le operazioni AWS Config API per gestire AWS Config regole e pacchetti di conformità Account AWS	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni: Regole di configurazione Pacchetti di conformità Aggregazione di dati da più account e regioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	in tutta l'organizzazione. Puoi utilizzare un account di amministratore delegato per aggregare i dati di configurazione e conformità delle risorse provenienti da tutti gli account membri dell'organizzazione in AWS Organizations. Per ulteriori			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	informazioni, consulta Registrazione di un amministratore delegato nella Guida per sviluppatori di AWS Config .			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
AWS Control Tower Configura e gestisci un ambiente AWS con più account sicuro e conforme.	Puoi configurare una landing zone, un ambiente multi-account per tutte le tue AWS risorse. Questo ambiente include un'organizzazione e le entità dell'organizzazione. Puoi utilizzare questo ambiente per applicare le normative di conformit	 Sì Ulteriori informazioni	 No	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	à a tutti i tuoi. Account AWS Per ulteriori informazioni, consulta Come AWS Control Tower e Gestisci gli account tramite AWS Organizations nella AWS Control Tower Guida utente.			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
Centrale ottimizzazione costi AWS Raccogli consigli sui costi per tutti i prodotti di AWS ottimizzazione.	Puoi identificare, filtrare e aggregare facilmente i consigli per l'ottimizzazione dei AWS costi nei tuoi account AWS Organizations membri e AWS nelle aree geografiche. Per ulteriori informazioni, consulta Cost Optimizat	 Sì Ulteriori informazioni	 No	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	ion Hub nella guida per l'utente di Cost Optimization Hub.			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
Amazon Detective Genera visualizzazioni dai dati di log per analizzare, indagare e identificare rapidamente la causa principale dei risultati sulla sicurezza o delle attività sospette.	Puoi integrare Amazon Detective con AWS Organizations per assicurarti che il grafico del comportamento di Amazon Detective fornisca visibilità sull'attività di tutti gli account della tua organizzazione.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
Amazon DevOps Guru Analizzare i dati operativi e i parametri e gli eventi delle applicazioni per identificare i comportamenti che si discostano dai normali modelli operativi. Gli utenti vengono avvisati quando DevOps Guru rileva un problema o un rischio operativo.	Puoi integrarlo con AWS Organizations per gestire le informazioni da tutti gli account dell'intera organizzazione. È possibile delegare un amministratore per visualizzare, ordinare e filtrare le informazioni da tutti gli account per ottenere lo stato di	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	integrità dell'organizzazione di tutte le applicazioni monitorate.			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato
AWS Directory Service Configura ed esegui le directory nel AWS Cloud o connetti AWS le tue risorse con un Microsoft Active Directory locale esistente.	È possibile eseguire l'integrazione AWS Directory Service con AWS Organizations per una condivisione di directory senza interruzioni tra più account e qualsiasi VPC in una regione.	 Sì Ulteriori informazioni	 No

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
Amazon EventBridge Monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale.	Puoi abilitare la condivisione di tutti gli EventBridge eventi Amazon, precedentemente Amazon CloudWatch Events, su tutti gli account della tua organizzazione. Per ulteriori informazioni, consulta Invio e ricezione di EventBridge eventi Amazon	 No	 No	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	tra due Account AWS nella Amazon EventBridge User Guide.			
AWS Firewall Manager Configura e gestisci centralmente le regole del firewall per le applicazioni Web su tutti gli account e le applicazioni.	Puoi configurare e gestire centralmente AWS WAF le regole per tutti gli account della tua organizzazione.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
Amazon GuardDuty GuardDuty è un servizio di monitoraggio continuo della sicurezza che analizza ed elabora le informazioni provenienti da una varietà di fonti di dati. Utilizza feed di intelligence di minacce e il machine learning per identificare attività inattese e potenzialmente non autorizzate e dannose nell'ambiente AWS .	Puoi designare un account membro per visualizzare e gestire GuardDuty tutti gli account della tua organizzazione. L'aggiunta di account membri abilita GuardDuty automaticamente tali account tra quelli selezionati Regione AWS.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	Puoi anche automatizzare GuardDuty l'attivazione di nuovi account aggiunti alla tua organizzazione. Per ulteriori informazioni, consulta GuardDuty la sezione Organizations in the Amazon GuardDuty User Guide.			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
AWS Health Ottieni visibilità sugli eventi che potrebbero influire sulle prestazioni delle risorse o sui problemi di disponibilità dei AWS servizi.	Puoi aggregare AWS Health gli eventi tra gli account della tua organizzazione.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
AWS Identity and Access Management Controlla in modo sicuro l'accesso alle risorse. AWS	È possibile utilizzare i dati a cui il servizio ha effettuato l'ultimo accesso in IAM per aiutarti a comprendere meglio le attività AWS all'interno dell'azienda. È possibile utilizzare questi dati per creare e aggiornare le policy di controllo dei servizi (SCP)	 No	 No	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	che limitano l'accesso esclusivamente ai servizi AWS utilizzati dagli account dell'organizzazione. Per un esempio, consulta Utilizzo dei dati per perfezionare le autorizzazioni di un'unità organizzativa nella Guida per l'utente di IAM.			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
IAM Access Analyzer Analizza le politiche basate sulle risorse del tuo AWS ambiente per identificare le politiche che concedono l'accesso a un soggetto che non rientra nella tua zona di fiducia.	Puoi designare un account membro come amministratore per IAM Access Analyzer. Per ulteriori informazioni, consulta Abilitazione di Access Analyzer nella Guida per l'utente di IAM.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
Amazon Inspector Scansiona automaticamente i AWS carichi di lavoro alla ricerca di vulnerabilità per scoprire le istanze di Amazon EC2 e le immagini dei container che risiedono in Amazon ECR per individuare vulnerabilità del software ed esposizione involontaria della rete.	Delegare un amministratore per abilitare o disabilitare le scansioni degli account membri, visualizzare i dati di ricerca aggregati dell'intera organizzazione, creare e gestire regole di soppressione. Per ulteriori informazioni, consultare	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	Gestione di più account con AWS Organizations nella Guida per l'utente di Amazon Inspector.			
AWS License Manager Semplifica il processo di trasferimento nel cloud delle licenze software.	È possibile abilitare il rilevamento tra più account delle risorse di elaborazione in tutta l'azienda.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
Amazon Macie Individua e classifica i contenuti business-critical utilizzando il Machine Learning per soddisfare i requisiti di sicurezza e di privacy dei dati. Valuta continuamente i contenuti archiviati in Amazon S3 e invia notifiche relative a potenziali problemi.	Puoi configurare Amazon Macie per tutti gli account dell'organizzazione e per ottenere una vista consolidata di tutti i dati in Amazon S3, su tutti gli account da un account di amministratore designato di Macie. È possibile configurare Macie	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	per proteggere automaticamente le risorse nei nuovi account man mano che l'organizzazione cresce. Si ricevono avvisi per correggere le configurazioni errate delle policy nei bucket S3 nell'organizzazione.			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
Marketplace AWS Un catalogo di risorse digitali selezionate che puoi utilizzare per individuare, acquistare, implementare e gestire in modo semplice i servizi e i software di terze parti necessari per creare soluzioni e gestire la tua attività.	Puoi condividere le licenze per i tuoi Marketplace AWS abbonamenti e acquisti tra gli account della tua organizzazione.	 Sì Ulteriori informazioni	 No	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
Marketplace AWS Marketplace privato Fornisce un ampio catalogo di prodotti disponibili in Marketplace AWS, oltre a un controllo approfondito di tali prodotti.	Consente di creare più esperienze di marketplace private associate all'intera organizzazione, a una o più unità organizzative o a uno o più account dell'organizzazione, ciascuno con il proprio set di prodotti approvati. AWS Gli amministratori	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	possono anche applicare il marchio aziendale a ogni esperienza di marketplace privato con il logo, i messaggi e lo schema di colori dell'azienda o del team.			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
AWS Network Manager Consente di gestire centralmente la rete principale AWS Cloud WAN e la rete AWS Transit Gateway tra AWS account, regioni e sedi locali.	Puoi gestire e monitorare centralmente le tue reti globali con gateway di transito e le relative risorse collegate in più AWS account all'interno della tua organizzazione.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
AWS Resource Access Manager Condividi AWS risorse specifiche di tua proprietà con altri account.	È possibile condividere risorse all'interno della propria organizzazione senza scambiare inviti aggiuntivi. Le risorse che puoi condividere includono le regole Route 53 Resolver, le prenotazioni della capacità on demand e altro ancora.	 Sì Ulteriori informazioni	 No	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	Per informazioni sulla condivisione delle prenotazioni di capacità, consulta la Guida per l'utente di Amazon EC2 per le istanze Linux o la Guida per l'utente di Amazon EC2 per Windows. Per un elenco delle risorse condivisibili, consulta Risorse			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	condivisibili nella Guida per l'utente di AWS RAM .			
Esploratore di risorse AWS Esplora le tue risorse utilizzando un'esperienza simile a quella dei motori di ricerca su Internet.	Abilita la ricerca multi-account.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
AWS Security Hub Visualizza il tuo stato di sicurezza AWS e verifica il tuo ambiente rispetto agli standard e alle best practice del settore della sicurezza.	Puoi abilitare automaticamente Security Hub per tutti gli account dell'organizzazione, inclusi i nuovi account man mano che vengono aggiunti. Ciò aumenta la copertura per i controlli e i risultati di Security Hub, che fornisce un quadro	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	più accurato della posizione di sicurezza generale.			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
Amazon S3 Storage Lens Ottieni visibilità sui parametri di utilizzo e attività dell'architettura Amazon S3 con suggerimenti utili per ottimizzare l'archiviazione.	Configura Amazon S3 Storage Lens per ottenere visibilità sulle tendenze di attività e utilizzo dell'architettura Amazon S3 e per ricevere suggerimenti per tutti gli account membri della tua organizzazione.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
Amazon Security Lake Amazon Security Lake centralizza i dati di sicurezza provenienti da origini cloud, on-premise e personalizzate in un data lake archiviato nel tuo account.	Crea un data lake che raccoglie log ed eventi nei tuoi account.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
AWS Service Catalog Crea e gestisci i cataloghi di servizi IT approvati per l'uso in AWS.	È possibile condividere portafogli e copiare i prodotti nei diversi account in modo più semplice, senza condividere gli ID dei portafogli.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
Service Quotas Visualizza e gestisci le quote di servizio, note anche come limiti da una posizione centrale.	È possibile creare un modello di richiesta quota per richiedere automaticamente un aumento della quota quando vengono creati gli account nell'organizzazione.	 Sì Ulteriori informazioni	 No	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
AWS IAM Identity Center Fornisci l'accesso Single Sign-On per tutte le applicazioni cloud e tutti gli account.	Gli utenti possono accedere al portale di AWS accesso con le proprie credenziali aziendali e accedere alle risorse nell'account di gestione assegnato o negli account membro.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
AWS Systems Manager Abilita la visibilità e il controllo delle tue AWS risorse.	È possibile sincronizzare i dati operativi Account AWS in tutta l'organizzazione utilizzando Systems Manager Explorer. Ora puoi gestire modelli di modifica, approvazioni e report per tutti gli account membri dell'organizzazione e da un account di	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	amministratore delegato utilizzando Systems Manager Change Manager.			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
Policy di tag Utilizza tag standardizzati in tutte le risorse negli account dell'organizzazione.	Puoi creare policy di tag per definire regole di assegnazione di tag per risorse specifiche e collegarle alle unità organizzative e agli account per fare applicare tali regole.	 Sì Ulteriori informazioni	 No	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
AWS Trusted Advisor Trusted Advisor ispeziona l'AWS ambiente e fornisce raccomandazioni quando esistono opportunità per risparmiare denaro, migliorare la disponibilità e le prestazioni del sistema o contribuire a colmare le lacune di sicurezza.	Esegui Trusted Advisor controlli per tutti i componenti dell'Account AWS organizzazione.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato
AWS Well-Architected Tool Ti AWS Well-Architected Tool aiuta a documentare lo stato dei tuoi carichi di lavoro e a confrontarli con le migliori pratiche AWS architettoniche più recenti.	Consente AWS WA Tool sia ai clienti di Organizations che a quelli di Organizations di semplificare il processo di condivisione AWS WA Tool delle risorse con gli altri membri della propria organizzazione.	 Sì Ulteriori informazioni	 No

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
IP Address Manager (IPAM) di Amazon VPC IPAM è una funzionalità VPC che semplifica la pianificazione, il monitoraggio e il monitoraggio degli indirizzi IP per AWS i carichi di lavoro.	Monitora l'utilizzo degli indirizzi IP in tutta l'organizzazione e condividi i pool di indirizzi IP tra gli account membri.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
Sistema di analisi della reperibilità Amazon VPC Reachability Analyzer è uno strumento di analisi della configurazione che consente di eseguire test di connettività tra una risorsa di origine e una risorsa di destinazione nei cloud privati virtuali (VPC).	Tieni traccia dei percorsi tra gli account delle tue organizzazioni.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS Account Management e AWS Organizations

AWS Account Management aiuta a gestire le informazioni sull'account e i metadati per tutte gli Account AWSnella tua organizzazione. È possibile impostare, modificare o eliminare le informazioni di contatto alternative per ciascun account membro dell'organizzazione. Per ulteriori informazioni, consulta Utilizzo di AWS Account Management nell'organizzazione nella AWS Account ManagementGuida per l'utente.

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS Account Management con AWS Organizations.

Abilitare l'accesso attendibile tramite Gestione dell'account

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Gestione dell'account richiede l'accesso attendibile a AWS Organizations prima di designare un account membro come amministratore delegato per questo servizio per l'organizzazione.

Puoi abilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

È possibile abilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI o chiamando un'operazione API in un SDK AWS.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

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. Nella pagina Services (Servizi), trova la riga per AWS Account Management, scegli il nome del servizio, quindi scegli Enable trusted access (Abilita accesso attendibile).
3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS Account Management che ora può abilitare quel servizio utilizzando la console per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Puoi eseguire il comando seguente per abilitare AWS Account Management come servizio attendibile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.

- API AWS: EnableAWSServiceAccess

Disabilitare l'accesso attendibile tramite Gestione dell'account

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Solo un amministratore nell'account di gestione di AWS Organizations può disabilitare l'accesso attendibile con AWS Account Management.

Puoi disabilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

È possibile disabilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI Organizations oppure chiamando un'operazione API Organizations in un SDK AWS.

AWS Management Console

Per disabilitare l'accesso al servizio attendibile utilizzando la console Organizations

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. Nella pagina Services (Servizi), individuare la riga per AWS Account Management e scegliere il nome del servizio.
3. Scegli Disable trusted access (Disabilita accesso attendibile).
4. Nella finestra di dialogo di conferma, inserisci **`disable`** nella casella, quindi scegli Disable trusted access (Disabilita accesso attendibile).

5. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS Account Management che ora può disabilitare quel servizio utilizzando la console o gli strumenti per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare AWS Account Management come servizio attendibile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.

- API AWS: DisableAWSServiceAccess

Abilitazione di un account di amministratore delegato per Gestione dell'account

Quando si designa un account membro come amministratore delegato per l'organizzazione, gli utenti e i ruoli dell'account designato possono gestire i metadati dell'Account AWS per altri account membri dell'organizzazione. Se non si abilita un account amministratore delegato, queste attività possono essere eseguite solo dall'account di gestione dell'organizzazione. Ciò consente di separare la gestione dell'organizzazione dalla gestione dei dettagli dell'account.

> **Autorizzazioni minime**
>
> Solo un utente o un ruolo nell'account di gestione di Organizations può configurare un account membro come amministratore delegato per la Gestione dell'account nell'organizzazione

Per le istruzioni generali su come configurare una policy di delega, consulta Creazione o aggiornamento di una policy di delega basata sulle risorse.

AWS CLI, AWS API

Se desideri configurare un account di amministratore delegato utilizzando AWS CLI o uno degli SDK AWS, puoi utilizzare anche i seguenti comandi:

- AWS CLI:

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

- SDK AWS: richiama l'operazione `RegisterDelegatedAdministrator` di Organizations e il numero ID dell'account membro e identifica il principale del servizio dell'account `account.amazonaws.com` come parametri.

Servizio AWS di migrazione delle applicazioni (AWS MGN) e AWS Organizations

Servizio AWS di migrazione delle applicazioni semplifica, velocizza e riduce i costi della migrazione delle applicazioni verso AWS. Grazie all'integrazione con Organizations, puoi utilizzare la funzionalità di visualizzazione globale per gestire migrazioni su larga scala e su più account. Per ulteriori informazioni, consulta Setting up your AWS Organizations nella Guida per l'utente di MGN.

Utilizza le seguenti informazioni per facilitare l'integrazione di Servizio AWS di migrazione delle applicazioni con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a MGN di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra MGN e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForApplicationMigrationService`

Principali del servizio utilizzati da MGN

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da MGN concedono l'accesso ai seguenti principali del servizio:

- `mgn.amazonaws.com`

Abilitazione dell'accesso attendibile con MGN

Quando abiliti l'accesso attendibile con MGN, puoi utilizzare la funzionalità di visualizzazione globale, che consente di gestire migrazioni su larga scala e su più account. La visualizzazione globale offre visibilità e la possibilità di eseguire operazioni specifiche su server di origine, app e onde in diversi account AWS. Per ulteriori informazioni, consulta Setting up your AWS Organizations nella Guida per l'utente di Servizio AWS di migrazione delle applicazioni.

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Puoi abilitare l'accesso attendibile utilizzando la console Servizio AWS di migrazione delle applicazioni o AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti Servizio AWS di migrazione delle applicazioni per abilitare l'integrazione con Organizations. Ciò consente a Servizio AWS di migrazione delle applicazioni di eseguire qualsiasi configurazione richiesta, ad esempio la creazione di risorse necessarie al servizio. Procedi con questi passaggi solo se non è possibile abilitare l'integrazione utilizzando gli strumenti forniti da Servizio AWS di migrazione delle applicazioni. Per ulteriori informazioni, consulta questa nota.
>
> Se abiliti l'accesso attendibile utilizzando la console o gli strumenti di Servizio AWS di migrazione delle applicazioni, non è necessario completare questi passaggi.

È possibile abilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI o chiamando un'operazione API in un SDK AWS.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

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. Nella pagina Servizi, trova la riga per Servizio AWS di migrazione delle applicazioni, scegli il nome del servizio, quindi scegli Abilita accesso attendibile.
3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di Servizio AWS di migrazione delle applicazioni che ora può abilitare quel servizio utilizzando la console per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Puoi eseguire il comando seguente per abilitare Servizio AWS di migrazione delle applicazioni come servizio attendibile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: EnableAWSServiceAccess

Disabilitazione dell'accesso attendibile con MGN

Solo un amministratore nell'account di gestione di Organizations può disabilitare l'accesso attendibile con MGN.

Puoi disabilitare l'accesso attendibile utilizzando Servizio AWS di migrazione delle applicazioni o gli strumenti AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti Servizio AWS di migrazione delle applicazioni per disabilitare l'integrazione con Organizations. Ciò consente a Servizio AWS di migrazione delle applicazioni di eseguire qualsiasi operazione di pulizia necessaria, ad esempio l'eliminazione di risorse o di ruoli di accesso che non sono più necessari dal servizio. Procedi con questi passaggi solo se non è possibile disabilitare l'integrazione utilizzando gli strumenti forniti da Servizio AWS di migrazione delle applicazioni. Se disabiliti l'accesso attendibile utilizzando la console o gli strumenti di Servizio AWS di migrazione delle applicazioni, non è necessario completare questi passaggi.

È possibile disabilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI Organizations oppure chiamando un'operazione API Organizations in un SDK AWS.

AWS Management Console

Per disabilitare l'accesso al servizio attendibile utilizzando la console Organizations

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. Nella pagina Servizi, individua la riga per Servizio AWS di migrazione delle applicazioni, quindi scegli il nome del servizio.
3. Scegli Disable trusted access (Disabilita accesso attendibile).
4. Nella finestra di dialogo di conferma, inserisci **`disable`** nella casella, quindi scegli Disable trusted access (Disabilita accesso attendibile).
5. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di Servizio AWS di migrazione delle applicazioni che ora può disabilitare quel servizio utilizzando la console o gli strumenti per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare Servizio AWS di migrazione delle applicazioni come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal mgn.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: DisableAWSServiceAccess

Abilitazione di un account amministratore delegato per MGN

Quando designi un account membro come amministratore delegato per l'organizzazione, gli utenti e i ruoli di tale account possono eseguire operazioni amministrative per MGN che altrimenti potrebbero essere eseguite solo da utenti o ruoli nell'account di gestione dell'organizzazione. Ciò consente di separare la gestione dell'organizzazione dalla gestione di MGN. Per ulteriori informazioni, consulta Setting up your AWS Organizations nella Guida per l'utente di MGN.

> **Autorizzazioni minime**
>
> Solo un utente o un ruolo nell'account di gestione di Organizations può configurare un account membro come amministratore delegato per MGN nell'organizzazione

AWS CLI, AWS API

Se desideri configurare un account di amministratore delegato utilizzando AWS CLI o uno degli SDK AWS, puoi utilizzare anche i seguenti comandi:

- AWS CLI:

  ```
  $ aws organizations register-delegated-administrator \
  ```

```
    --account-id 123456789012 \
    --service-principal mgn.amazonaws.com
```

- AWS SDK: richiama l'operazione di `RegisterDelegatedAdministrator` di Organizations, il numero identificativo dell'account membro e identificativo del servizio dell'account `mgn.amazonaws.com`come parametri.

Disabilitazione di un amministratore delegato per MGN

Solo un amministratore nell'account di gestione di Organizations può rimuovere un amministratore delegato per MGN. Puoi rimuovere l'amministratore delegato utilizzando la CLI o l'operazione SDK `DeregisterDelegatedAdministrator` di Organizations.

AWS Artifact e AWS Organizations

AWS Artifact è un servizio che consente di scaricare i rapporti di conformità alla sicurezza di AWS, ad esempio i rapporti ISO e PCI. Utilizzando AWS Artifact, un utente in un account di gestione dell'organizzazione può accettare automaticamente accordi per conto di tutti gli account membri in un'organizzazione, anche quando vengono aggiunti nuovi rapporti e account. Glu utenti degli account membri possono visualizzare e scaricare gli accordi. Per ulteriori informazioni, consulta Gestione di un contratto per più account inAWS Artifact nella Guida per l'utente di AWS Artifact.

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS Artifact con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a AWS Artifact di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra AWS Artifact e Organizations o se rimuovi l'account membro dall'organizzazione.

Sebbene sia possibile eliminare o modificare questo ruolo se si rimuove l'account membro dall'organizzazione, non è consigliabile farlo.

La modifica del ruolo non è consigliata perché può portare a problemi di sicurezza come il "confused deputy" tra servizi. Per ulteriori informazioni sulla protezione dal "confused deputy", consulta Prevenzione del confused deputy tra servizi nella AWS Artifact Guida per l'utente.

- `AWSServiceRoleForArtifact`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da AWS Artifact concedono l'accesso ai seguenti principali del servizio:

- `artifact.amazonaws.com`

Abilitazione dell'accesso attendibile con AWS Artifact

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Puoi abilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

È possibile abilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI o chiamando un'operazione API in un SDK AWS.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

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. Nella pagina Services (Servizi), trova la riga per AWS Artifact, scegli il nome del servizio, quindi scegli Enable trusted access (Abilita accesso attendibile).
3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS Artifact che ora può abilitare quel servizio utilizzando la console per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Puoi eseguire il comando seguente per abilitare AWS Artifact come servizio attendibile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.

- API AWS: EnableAWSServiceAccess

Disabilitazione dell'accesso attendibile con AWS Artifact

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Solo un amministratore nell'account di gestione di AWS Organizations può disabilitare l'accesso attendibile con AWS Artifact.

Puoi disabilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

AWS Artifact richiede l'accesso attendibile con AWS Organizations per funzionare con gli accordi dell'organizzazione. Se disabiliti l'accesso utilizzando AWS Organizations durante l'utilizzo di AWS Artifact per gli accordi dell'organizzazione, smette di funzionare in quanto non può accedere all'organizzazione. Qualsiasi accordo dell'organizzazione che accetti in AWS Artifact rimane, ma AWS Artifact non può accedervi. Il ruolo AWS Artifact che crea AWS Artifact rimane. Se quindi riabiliti l'accesso sicuro, AWS Artifact continua a funzionare come prima, senza la necessità di riconfigurare il servizio.

Un account autonomo rimosso da un'organizzazione non ha più accesso a qualsiasi accordo dell'organizzazione.

È possibile disabilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI Organizations oppure chiamando un'operazione API Organizations in un SDK AWS.

AWS Management Console

Per disabilitare l'accesso al servizio attendibile utilizzando la console Organizations

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. Nella pagina Services (Servizi), individuare la riga per AWS Artifact e scegliere il nome del servizio.
3. Scegli Disable trusted access (Disabilita accesso attendibile).
4. Nella finestra di dialogo di conferma, inserisci **`disable`** nella casella, quindi scegli Disable trusted access (Disabilita accesso attendibile).
5. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS Artifact che ora può disabilitare quel servizio utilizzando la console o gli strumenti per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare AWS Artifact come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal artifact.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- API AWS: DisableAWSServiceAccess

Abilitazione di un account amministratore delegato per AWS Artifact

Per ulteriori informazioni sull'abilitazione di un amministratore delegato per AWS Artifact, consulta AWS Artifact.

AWS Audit Manager e AWS Organizations

AWS Audit Manager ti aiuta a verificare continuamente il tuo utilizzo di AWS per semplificare la gestione dei rischi e della conformità alle normative e agli standard di settore. Audit Manager automatizza la raccolta delle prove per semplificare la valutazione dell'efficacia delle policy, delle procedure e delle attività. Quando è il momento di una verifica, Audit Manager ti aiuta a gestire le revisioni dei tuoi controlli a cura delle parti interessate e ti aiuta a creare report pronti per la verifica con sforzi manuali assai ridotti.

Quando integri Audit Manager con AWS Organizations, puoi raccogliere prove da una fonte più ampia includendo più Account AWS all'interno dell'organizzazione nell'ambito delle valutazioni.

Per ulteriori informazioni, consulta Abilitazione di AWS Organizations nella Guida per l'utente di Audit Manager.

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS Audit Manager con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente ad Audit Manager di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra Audit Manager e Organizations o se rimuovi l'account membro dall'organizzazione.

Per ulteriori informazioni su come Audit Manager utilizza questo ruolo, consulta Utilizzo di ruoli collegati ai servizi nella Guida per l'utente di AWS Audit Manager.

- `AWSServiceRoleForAuditManager`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da Audit Manager concedono l'accesso ai seguenti principali del servizio:

- `auditmanager.amazonaws.com`

Per abilitare l'accesso attendibile tramite Audit Manager

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Audit Manager richiede l'accesso attendibile a AWS Organizations prima di designare un account membro come amministratore delegato dell'organizzazione.

È possibile abilitare l'accesso sicuro utilizzando la console AWS Audit Manager o la console AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti AWS Audit Manager per abilitare l'integrazione con Organizations. Ciò consente a AWS Audit Manager di eseguire qualsiasi configurazione richiesta, ad esempio la creazione di risorse necessarie al servizio. Procedi con questi passaggi solo se non è possibile abilitare l'integrazione utilizzando gli strumenti forniti da AWS Audit Manager. Per ulteriori informazioni, consulta questa nota.
> Se abiliti l'accesso attendibile utilizzando la console o gli strumenti di AWS Audit Manager, non è necessario completare questi passaggi.

Per abilitare l'accesso attendibile tramite la console Audit Manager

Per istruzioni su come abilitare l'accesso attendibile, consulta Configurazione nella Guida per l'utente di AWS Audit Manager.

> **Note**
>
> Se si configura un amministratore delegato utilizzando la console AWS Audit Manager, AWS Audit Manager abilita automaticamente l'accesso attendibile per tuo conto.

Puoi abilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Puoi eseguire il comando seguente per abilitare AWS Audit Manager come servizio attendibile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: EnableAWSServiceAccess

Per disabilitare l'accesso attendibile tramite Audit Manager

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Solo un amministratore nell'account di gestione di AWS Organizations può disabilitare l'accesso attendibile con AWS Audit Manager.

Puoi disabilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

Puoi disabilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare AWS Audit Manager come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal auditmanager.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: DisableAWSServiceAccess

Abilitazione di un account di amministratore delegato per Audit Manager

Quando si designa un account membro come amministratore delegato per l'organizzazione, gli utenti e i ruoli di tale account possono eseguire operazioni amministrative per Audit Manager che altrimenti possono essere eseguiti solo da utenti o ruoli nell'account di gestione dell'organizzazione. Ciò consente di separare la gestione dell'organizzazione dalla gestione di Audit Manager.

> **Autorizzazioni minime**
>
> Solo un utente o un ruolo nell'account di gestione di Organizations con la seguente autorizzazione può configurare un account membro come amministratore delegato per la Gestione audit nell'organizzazione: `audit-manager:RegisterAccount`

Per istruzioni sull'abilitazione di un account di amministratore delegato per Audit Manager, consulta Configurazione nella Guida per l'utente di AWS Audit Manager.

Se si configura un amministratore delegato utilizzando la console AWS Audit Manager, Audit Manager abilita automaticamente l'accesso attendibile per tuo conto.

AWS CLI, AWS API

Se desideri configurare un account di amministratore delegato utilizzando AWS CLI o uno degli SDK AWS, puoi utilizzare anche i seguenti comandi:

- AWS CLI:

```
$  aws audit-manager register-account \
    --delegated-admin-account 123456789012
```

- SDK AWS: chiama l'operazione `RegisterAccount` e fornisci `delegatedAdminAccount` come parametro per delegare l'account amministratore.

AWS Backup e AWS Organizations

AWS Backup è un servizio che consente di gestire e monitorare i processi AWS Backup nell'organizzazione. Utilizzando AWS Backup, se si accede come utente nell'account di gestione dell'organizzazione, è possibile abilitare la protezione e il monitoraggio dei backup a livello di organizzazione. Consente di ottenere la conformità utilizzando policy di backup per applicare piani AWS Backup a livello centrale alle risorse in tutti gli account dell'organizzazione. Quando si utilizzano AWS Backup e AWS Organizations insieme, è possibile ottenere i seguenti vantaggi:

Protezione

È possibile abilitare il tipo di policy di backup nell'organizzazione e quindi creare policy di backup da collegare alla root, alle unità organizzative o agli account dell'organizzazione. Una policy di backup combina un piano AWS Backup con gli altri dettagli necessari per applicare automaticamente il piano agli account. Le policy collegate direttamente a un account vengono unite con le policy ereditate dal root dell'organizzazione e dalle unità organizzative padre per creare una policy effettiva che si applica all'account. La policy include l'ID di un ruolo IAM che dispone delle autorizzazioni per eseguire AWS Backup sulle risorse negli account. AWS Backup utilizza il ruolo IAM per eseguire il backup per tuo conto come specificato dal piano di backup nella policy effettiva.

Monitoraggio

Quando si abilita l'accesso sicuroAWS Backup nell'organizzazione, è possibile utilizzare la console AWS Backup per visualizzare i dettagli sui processi di backup, ripristino e copia in uno qualsiasi degli account dell'organizzazione. Per ulteriori informazioni, consulta Monitoraggio dei lavori di backup nella Guida per sviluppatori di AWS Backup.

Per ulteriori informazioni su AWS Backup, consulta la Guida per sviluppatori di AWS Backup.

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS Backup con AWS Organizations.

Abilitazione dell'accesso attendibile con AWS Backup

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

È possibile abilitare l'accesso sicuro utilizzando la console AWS Backup o la console AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti AWS Backup per abilitare l'integrazione con Organizations. Ciò consente a AWS Backup di eseguire qualsiasi configurazione richiesta, ad esempio la creazione di risorse necessarie al servizio. Procedi con questi passaggi solo se non è possibile abilitare l'integrazione utilizzando gli strumenti forniti da AWS Backup. Per ulteriori informazioni, consulta questa nota.
> Se abiliti l'accesso attendibile utilizzando la console o gli strumenti di AWS Backup, non è necessario completare questi passaggi.

Per abilitare l'accesso attendibile utilizzando AWS Backup, consulta Attivazione del backup in più Account AWS nella Guida per gli sviluppatori di AWS Backup.

Disabilitazione dell'accesso attendibile con AWS Backup

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

AWS Backup richiede l'accesso attendibile con AWS Organizations per abilitare il monitoraggio dei processi di backup, ripristino e copia negli account dell'organizzazione. Se si disattiva l'accesso sicuro AWS Backup, si perde la possibilità di visualizzare i processi al di fuori dell'account corrente. Il ruolo AWS Backup che crea AWS Backup rimane. Se si riabilita l'accesso sicuro, AWS Backup continua a funzionare come prima, senza la necessità di riconfigurare il servizio.

Puoi disabilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

Puoi disabilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare AWS Backup come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal backup.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: DisableAWSServiceAccess

Abilitazione di un account amministratore delegato per AWS Backup

Vedi la sezione Amministratore delegato nella Guida per gli sviluppatori di AWS Backup.

AWS CloudFormation StackSets e AWS Organizations

AWS CloudFormation StackSets consente di creare, aggiornare o eliminare gli stack in più Account AWS e Regioni AWS con un'unica operazione. L'integrazione di StackSets con AWS Organizations consente di creare set di stack con autorizzazioni gestite dal servizio, utilizzando un ruolo collegato ai servizi che dispone dell'autorizzazione pertinente in ogni account membro. Ciò consente di implementare istanze dello stack a tutti gli account membri dell'organizzazione. Non devi creare i ruoli AWS Identity and Access Management necessari; StackSets crea il ruolo IAM in ogni account membro per tuo conto.

Puoi anche abilitare le implementazioni automatiche agli account che verranno aggiunti all'organizzazione in futuro. Con l'implementazione automatica abilitata, i ruoli e l'implementazione delle istanze associate dei set di stack vengono aggiunti automaticamente a tutti gli account inseriti successivamente in tale UO.

Quando si abilita l'accesso attendibile tra StackSets e Organizations, l'account di gestione dispone delle autorizzazioni per creare e gestire set di stack per l'organizzazione. L'account di gestione può registrare fino a cinque account membri come amministratori delegati. Con l'accesso attendibile abilitato, gli amministratori delegati dispongono anche delle autorizzazioni per creare e gestire stack set per l'organizzazione. I set di stack con le autorizzazioni gestite dai servizi vengono creati nell'account di gestione, inclusi i set di stack creati dagli amministratori delegati.

> **Important**
>
> Gli amministratori delegati dispongono delle autorizzazioni complete per la distribuzione negli account dell'organizzazione. L'account di gestione non può limitare le autorizzazioni di amministratore delegato per la distribuzione in unità organizzative specifiche o per eseguire operazioni specifiche del set di stack.

Per ulteriori informazioni sull'integrazione di StackSets con Organizations, consulta Utilizzo di AWS CloudFormation StackSets nella Guida per l'utente di AWS CloudFormation.

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS CloudFormation StackSets con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a AWS CloudFormation Stacksets di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra AWS CloudFormation Stacksets e Organizations o se rimuovi l'account membro dall'organizzazione.

- Account di gestione: `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`

Per creare il ruolo collegato ai servizi `AWSServiceRoleForCloudFormationStackSetsOrgMember` per gli account membri nell'organizzazione, sarà necessario innanzitutto creare un set di stack nell'account di gestione. In questo modo viene creata un'istanza del set di stack, che quindi crea il ruolo negli account membri.

- Account membri: `AWSServiceRoleForCloudFormationStackSetsOrgMember`

Per ulteriori dettagli sulla creazione di set di stack, consulta Utilizzo di AWS CloudFormation StackSets nella Guida per l'utente di AWS CloudFormation.

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da AWS CloudFormation Stacksets concedono l'accesso ai seguenti principali del servizio:

- Account di gestione: `stacksets.cloudformation.amazonaws.com`

  Puoi modificare o eliminare questo ruolo solo se è disabilitato l'accesso attendibile tra StackSets e Organizations.
- Account membri: `member.org.stacksets.cloudformation.amazonaws.com`

  Puoi modificare o eliminare questo ruolo da un account solo se prima disabiliti l'accesso attendibile tra StackSets e Organizations o se prima rimuovi l'account dall'organizzazione o dall'unità organizzativa (UO) di destinazione.

Abilitazione dell'accesso attendibile con AWS CloudFormation Stacksets

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Solo un amministratore nell'account di gestione dell'organizzazione dispone delle autorizzazioni per abilitare l'accesso attendibile con un altro servizio AWS. Puoi abilitare l'accesso attendibile utilizzando la console AWS CloudFormation o la console Organizations.

Puoi abilitare l'accesso attendibile utilizzando solo AWS CloudFormation StackSets.

Per abilitare l'accesso attendibile tramite la console AWS CloudFormation Stacksets, consulta Abilitazione dell'accesso attendibile con AWS Organizations nella Guida per l'utente di AWS CloudFormation.

Disabilitazione dell'accesso attendibile con AWS CloudFormation Stacksets

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Solo un amministratore nell'account di gestione dell'organizzazione dispone delle autorizzazioni per disabilitare l'accesso attendibile con un altro servizio AWS. Puoi disabilitare l'accesso attendibile

utilizzando solo la console Organizations. Se disabiliti l'accesso attendibile con Organizations mentre utilizzi StackSets, tutte le istanze dello stack create in precedenza vengono mantenute. Tuttavia, i set di stack implementati utilizzando le autorizzazioni del ruolo collegato ai servizi non possono più eseguire implementazioni negli account gestiti da Organizations.

Puoi disabilitare l'accesso attendibile utilizzando la console AWS CloudFormation o la console Organizations.

> **Important**
>
> Se disabiliti l'accesso attendibile a livello di programmazione (ad esempio tramite AWS CLI o un'API), tieni presente che questo rimuoverà l'autorizzazione. È meglio disabilitare l'accesso attendibile tramite la console AWS CloudFormation.

È possibile disabilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI Organizations oppure chiamando un'operazione API Organizations in un SDK AWS.

AWS Management Console

Per disabilitare l'accesso al servizio attendibile utilizzando la console Organizations

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. Nella pagina Services (Servizi), individuare la riga per AWS CloudFormation StackSets, quindi scegli il nome del servizio.
3. Scegli Disable trusted access (Disabilita accesso attendibile).
4. Nella finestra di dialogo di conferma, inserisci **`disable`** nella casella, quindi scegli Disable trusted access (Disabilita accesso attendibile).
5. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS CloudFormation StackSets che ora può disabilitare quel servizio utilizzando la console o gli strumenti per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare AWS CloudFormation StackSets come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal stacksets.cloudformation.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: DisableAWSServiceAccess

Abilitazione di un account di amministratore delegato per AWS CloudFormation Stacksets

Quando si designa un account membro come amministratore delegato per l'organizzazione, gli utenti e i ruoli di tale account possono eseguire operazioni amministrative per i set di stack AWS CloudFormation che altrimenti possono essere eseguiti solo da utenti o ruoli nell'account di gestione dell'organizzazione. Ciò consente di separare la gestione dell'organizzazione dalla gestione di AWS CloudFormation Stacksets.

Per istruzioni su come designare un account membro come amministratore delegato di AWS CloudFormation Stacksets nell'organizzazione, consulta Registrazione di un amministratore delegato nella Guida per l'utente di AWS CloudFormation.

AWS CloudTrail e AWS Organizations

AWS CloudTrail è un AWS servizio che vi aiuta ad abilitare la governance, la conformità e il controllo operativo e dei rischi del vostro Account AWS. Utilizzando AWS CloudTrail, un utente di un account di gestione può creare un percorso organizzativo che registra tutti gli eventi per tutti Account AWS i membri dell'organizzazione. I trail di organizzazione vengono automaticamente applicati a tutti gli account membro dell'organizzazione. Gli account dei membri possono vedere il trail dell'organizzazione, ma non possono modificarlo o eliminarlo. Per impostazione predefinita, gli account membri non hanno accesso ai file di log per il trail dell'organizzazione nel bucket Amazon S3. Questo consente di applicare in modo omogeneo la tua strategia di registrazione di eventi agli account della tua organizzazione.

Per ulteriori informazioni, consulta Creazione di un trail per un'organizzazione nella Guida per l'utente diAWS CloudTrail .

Utilizza le seguenti informazioni per semplificare l'integrazione AWS CloudTrail con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Questo ruolo consente di CloudTrail eseguire operazioni supportate all'interno degli account dell'organizzazione all'interno dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra CloudTrail e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForCloudTrail`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da CloudTrail Concedono l'accesso ai seguenti principali di servizio:

- `cloudtrail.amazonaws.com`

Abilitazione dell'accesso attendibile con CloudTrail

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Se abiliti l'accesso affidabile creando un percorso dalla AWS CloudTrail console, l'accesso affidabile viene configurato automaticamente per te (scelta consigliata). Puoi anche abilitare l'accesso affidabile utilizzando la AWS Organizations console. Devi accedere con il tuo account di AWS Organizations gestione per creare un percorso organizzativo.

Se scegli di creare un percorso organizzativo utilizzando l' AWS CLI o l' AWS API, devi configurare manualmente l'accesso affidabile. Per ulteriori informazioni, consulta Enabling CloudTrail as a trusted service AWS Organizationsnella Guida per l'AWS CloudTrail utente.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS CloudTrail console o gli strumenti per abilitare l'integrazione con Organizations.

Puoi abilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione API Organizations in uno degli AWS SDK.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile ai servizi:

- AWS CLI: enable-aws-service-access

  È possibile eseguire il comando seguente per abilitarlo AWS CloudTrail come servizio affidabile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: Abilita AWSServiceAccess

Disabilitazione dell'accesso attendibile con CloudTrail

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

AWS CloudTrail richiede un accesso affidabile AWS Organizations per utilizzare i percorsi organizzativi e gli archivi dati degli eventi organizzativi. Se disabiliti l'accesso affidabile AWS Organizations durante l'utilizzo AWS CloudTrail, tutti gli itinerari organizzativi per gli account dei membri vengono eliminati perché non CloudTrail possono accedere all'organizzazione. Tutti gli itinerari di organizzazione degli account di gestione e gli archivi dati degli eventi organizzativi vengono convertiti in percorsi a livello di account e archivi dati di eventi. Il

`AWSServiceRoleForCloudTrail` ruolo creato per l'integrazione tra CloudTrail e AWS Organizations rimane all'interno dell'account. Se riattivi l'accesso affidabile, non CloudTrail interverrà sui percorsi e sugli archivi di dati di eventi esistenti. L'account di gestione deve aggiornare tutti gli itinerari e gli archivi di dati degli eventi a livello di account per applicarli all'organizzazione.

Per convertire un percorso o un data store di eventi a livello di account in un percorso organizzativo o in un data store di eventi organizzativi, procedi come segue:

- Dalla CloudTrail console, aggiorna il trail o event data store e scegli l'opzione Abilita per tutti gli account della mia organizzazione.
- Da AWS CLI, procedi come segue:
  - Per aggiornare una traccia, esegui il update-trailcomando e includi il `--is-organization-trail` parametro.
  - Per aggiornare un archivio dati di eventi, esegui il update-event-data-storecomando e includi il `--organization-enabled` parametro.

Solo un amministratore dell'account di AWS Organizations gestione può disabilitare l'accesso affidabile con AWS CloudTrail. Puoi disabilitare l'accesso affidabile solo con gli strumenti Organizations, utilizzando la AWS Organizations console, eseguendo un comando Organizations AWS CLI o chiamando un'operazione dell'API Organizations in uno degli AWS SDK.

Puoi disabilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno degli AWS SDK.

AWS Management Console

Per disabilitare l'accesso al servizio attendibile utilizzando la console Organizations

1. Accedi alla consoleAWS 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. Nella pagina Services (Servizi), individuare la riga per AWS CloudTrail e scegliere il nome del servizio.
3. Scegli Disable trusted access (Disabilita accesso attendibile).
4. Nella finestra di dialogo di conferma, inserisci **`disable`** nella casella, quindi scegli Disable trusted access (Disabilita accesso attendibile).

5. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS CloudTrail che ora può disabilitare quel servizio utilizzando la console o gli strumenti con AWS Organizationscui non può funzionare.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  È possibile eseguire il comando seguente per disabilitarlo AWS CloudTrail come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal cloudtrail.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: disabilita AWSServiceAccess

Abilitazione di un account amministratore delegato per CloudTrail

Quando si utilizza CloudTrail con Organizations, è possibile registrare qualsiasi account all'interno dell'organizzazione per agire come amministratore CloudTrail delegato per gestire i percorsi e gli archivi di dati degli eventi dell'organizzazione per conto dell'organizzazione. Un amministratore delegato è un account membro di un'organizzazione che può eseguire le stesse attività amministrative dell'account di gestione. CloudTrail

> **Autorizzazioni minime**
>
> Solo un amministratore dell'account di gestione Organizations può registrare un amministratore delegato per CloudTrail.

È possibile registrare un account amministratore delegato utilizzando la CloudTrail console o utilizzando l'operazione Organizations `RegisterDelegatedAdministrator` CLI o SDK. Per

registrare un amministratore delegato utilizzando la CloudTrail console, consulta Aggiungere un amministratore delegato. CloudTrail

Disabilitazione di un amministratore delegato per CloudTrail

Solo un amministratore dell'account di gestione Organizations può rimuovere un amministratore delegato per CloudTrail. È possibile rimuovere l'amministratore delegato utilizzando la CloudTrail console o utilizzando l'operazione Organizations `DeregisterDelegatedAdministrator` CLI o SDK. Per informazioni su come rimuovere un amministratore delegato utilizzando la CloudTrail console, consulta Rimuovere un amministratore delegato. CloudTrail

AWS Compute Optimizer e AWS Organizations

AWS Compute Optimizer è un servizio che analizza i parametri di configurazione e di utilizzo delle risorse AWS. Esempi di risorse includono le istanze Amazon Elastic Compute Cloud (Amazon EC2) e i gruppi Auto Scaling. Compute Optimizer segnala se le risorse sono ottimali e genera suggerimenti di ottimizzazione per ridurre i costi e migliorare le prestazioni dei carichi di lavoro. Per ulteriori informazioni su Compute Optimizer, consulta la Guida per l'utente di AWS Compute Optimizer.

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS Compute Optimizer con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a Compute Optimizer di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra Compute Optimizer e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForComputeOptimizer`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da Compute Optimizer concedono l'accesso ai seguenti principali del servizio:

- `compute-optimizer.amazonaws.com`

Abilitazione dell'accesso attendibile con Compute Optimizer

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

È possibile abilitare l'accesso sicuro utilizzando la console AWS Compute Optimizer o la console AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti AWS Compute Optimizer per abilitare l'integrazione con Organizations. Ciò consente a AWS Compute Optimizer di eseguire qualsiasi configurazione richiesta, ad esempio la creazione di risorse necessarie al servizio. Procedi con questi passaggi solo se non è possibile abilitare l'integrazione utilizzando gli strumenti forniti da AWS Compute Optimizer. Per ulteriori informazioni, consulta questa nota.
> Se abiliti l'accesso attendibile utilizzando la console o gli strumenti di AWS Compute Optimizer, non è necessario completare questi passaggi.

Per abilitare l'accesso attendibile tramite la console Compute Optimizer

È necessario accedere alla console Compute Optimizer utilizzando l'account di gestione dell'organizzazione. Accetta per conto della tua organizzazione seguendo le istruzioni di Abilitazione dell'account nella Guida per l'utente di AWS Compute Optimizer.

È possibile abilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI o chiamando un'operazione API in un SDK AWS.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

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. Nella pagina Services (Servizi), trova la riga per AWS Compute Optimizer, scegli il nome del servizio, quindi scegli Enable trusted access (Abilita accesso attendibile).

3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS Compute Optimizer che ora può abilitare quel servizio utilizzando la console per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Puoi eseguire il comando seguente per abilitare AWS Compute Optimizer come servizio attendibile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: EnableAWSServiceAccess

Disabilitazione dell'accesso attendibile con Compute Optimizer

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Solo un amministratore nell'account di gestione di AWS Organizations può disabilitare l'accesso attendibile con AWS Compute Optimizer.

Puoi disabilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare AWS Compute Optimizer come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal compute-optimizer.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: DisableAWSServiceAccess

Abilitazione di un account amministratore delegato per Compute Optimizer

Quando si designa un account membro come amministratore delegato per l'organizzazione, gli utenti e i ruoli dell'account designato possono gestire i metadati dell'Account AWS per altri account membri dell'organizzazione. Se non si abilita un account amministratore delegato, queste attività possono essere eseguite solo dall'account di gestione dell'organizzazione. Ciò consente di separare la gestione dell'organizzazione dalla gestione dei dettagli dell'account.

> **Autorizzazioni minime**
>
> Solo un utente o un ruolo nell'account di gestione di Organizations può configurare un account membro come amministratore delegato per il Sistema di ottimizzazione del calcolo nell'organizzazione

Per istruzioni sull'abilitazione di un account di amministratore delegato per Compute Optimizer, consulta https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html nella Guida per l'utente di AWS Compute Optimizer.

AWS CLI, AWS API

Se desideri configurare un account di amministratore delegato utilizzando AWS CLI o uno degli SDK AWS, puoi utilizzare anche i seguenti comandi:

- AWS CLI:

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

- SDK AWS: richiama l'operazione `RegisterDelegatedAdministrator` di Organizations e il numero ID dell'account membro e identifica il principale del servizio dell'account `account.amazonaws.com` come parametri.

Disattivazione di un amministratore delegato per Compute Optimizer

Solo un amministratore nell'account di gestione dell'organizzazione può configurare un amministratore delegato per Compute Optimizer.

Per disattivare l'account di un amministratore delegato Compute Optimizer utilizzando la console di Compute Optimizer, consulta https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html nella Guida per l'utente di AWS Compute Optimizer.

Per rimuovere un amministratore delegato utilizzando la AWS CLI AWS, consulta deregister-delegated-administrator (annulla registrazione-amministratore-delegato) in AWS AWS CLI Command Reference (Riferimento ai comandi).

AWS Config e AWS Organizations

L'aggregazione di dati di più Regioni e account in AWS Config consente di aggregare i dati di AWS Config provenienti da più account e Regioni AWS in un unico account. L'aggregazione di dati multi-regione e multi-account è utile per gli amministratori del reparto IT per monitorare la conformità dei molteplici Account AWS nell'azienda. Un aggregatore è un tipo di risorsa in AWS Config che raccoglie i dati di AWS Config da più account e regioni di origine. Crea un aggregatore nella regione in cui desideri visualizzare i dati AWS Config aggregati. Durante la creazione di un aggregatore, è possibile scegliere di aggiungere ID di account individuali o la tua organizzazione. Per ulteriori informazioni su AWS Config, consulta la AWS ConfigGuida per sviluppatori di .

Puoi inoltre utilizzare le API AWS Config per gestire le regole AWS Config per tutti gli Account AWS nell'organizzazione. Per ulteriori informazioni, consulta Abilitazione delle regole AWS Config per tutti gli account dell'organizzazione nella Guida per gli sviluppatori di AWS Config.

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS Config con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato negli account dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a AWS Config di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

- `AWSServiceRoleForConfig`

Questo ruolo viene creato quando si abilita AWS Config nell'organizzazione creando un aggregatore multi-account. AWS Config chiede di selezionare o creare un ruolo e di fornire il nome. Il nome non viene generato automaticamente.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra AWS Config e Organizations o se rimuovi l'account membro dall'organizzazione.

Abilitazione dell'accesso attendibile con AWS Config

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

È possibile abilitare l'accesso sicuro utilizzando la console AWS Config o la console AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti AWS Config per abilitare l'integrazione con Organizations. Ciò consente a AWS Config di eseguire qualsiasi configurazione richiesta, ad esempio la creazione di risorse necessarie al servizio. Procedi con questi passaggi solo se non è possibile abilitare l'integrazione utilizzando gli strumenti forniti da AWS Config. Per ulteriori informazioni, consulta questa nota.
> Se abiliti l'accesso attendibile utilizzando la console o gli strumenti di AWS Config, non è necessario completare questi passaggi.

Per abilitare l'accesso attendibile tramite la console AWS Config

Per abilitare l'accesso attendibile a AWS Organizations tramite AWS Config, crea un aggregatore multi-account e aggiungi l'organizzazione. Per ulteriori informazioni su come configurare un

aggregatore multi-account, consulta Impostazione di un aggregatore utilizzando la console nella Guida per gli sviluppatori di AWS Config.

È possibile abilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI o chiamando un'operazione API in un SDK AWS.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

1. Accedere 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. Nella pagina Services (Servizi), trova la riga per AWS Config, scegli il nome del servizio, quindi scegli Enable trusted access (Abilita accesso attendibile).
3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS Config che ora può abilitare quel servizio utilizzando la console per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Puoi eseguire il comando seguente per abilitare AWS Config come servizio attendibile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: EnableAWSServiceAccess

Disabilitazione dell'accesso attendibile con AWS Config

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Puoi disabilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

Puoi disabilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare AWS Config come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal config.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: DisableAWSServiceAccess

Centrale ottimizzazione costi AWS e AWS Organizations

Centrale ottimizzazione costi AWS è una funzionalità di AWS Billing and Cost Management che ti aiuta a consolidare e dare priorità ai consigli di ottimizzazione dei costi nei AWS tuoi account AWS e nelle aree geografiche, in modo da ottenere il massimo dalla tua spesa. AWS Utilizzando Cost Optimization Hub con, AWS Organizations è possibile identificare, filtrare e aggregare facilmente i consigli per l'ottimizzazione dei AWS costi tra gli account membri e le AWS aree geografiche di Organizations.

Per ulteriori informazioni, consulta Cost Optimization Hub nella Guida per l'AWS Cost Management utente.

Utilizza le seguenti informazioni per semplificare l'integrazione Centrale ottimizzazione costi AWS con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Questo ruolo consente a Cost Optimization Hub di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

È possibile eliminare o modificare questo ruolo solo se si disabilita l'accesso affidabile tra Cost Optimization Hub e Organizations o se si rimuove l'account membro dall'organizzazione.

Per ulteriori informazioni, consulta Autorizzazioni dei ruoli collegati ai servizi per Cost Optimization Hub nella Guida per l'AWS Cost Management utente.

- `AWSServiceRoleForCostOptimizationHub`

Principali del servizio utilizzati da Cost Optimization Hub

Cost Optimization Hub utilizza il `cost-optimization-hub.bcm.amazonaws.com` service principal.

Consentire un accesso affidabile con Cost Optimization Hub

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Quando scegli di utilizzare l'account di gestione dell'organizzazione e includi tutti gli account dei membri all'interno dell'organizzazione, l'accesso affidabile per Cost Optimization Hub viene automaticamente abilitato nell'account dell'organizzazione.

Puoi abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in uno degli AWS SDK.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

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. Nella pagina Services (Servizi), trova la riga per Centrale ottimizzazione costi AWS, scegli il nome del servizio, quindi scegli Enable trusted access (Abilita accesso attendibile).
3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore Centrale ottimizzazione costi AWS che ora può abilitare quel servizio utilizzando la sua console con AWS Organizations cui lavorare.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  È possibile eseguire il comando seguente per abilitarlo Centrale ottimizzazione costi AWS come servizio affidabile con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: Abilita AWSServiceAccess

Disabilitazione dell'accesso attendibile

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Puoi disabilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

> **Important**
>
> Se disabiliti l'accesso affidabile di Cost Optimization Hub dopo aver aderito, Cost Optimization Hub nega l'accesso ai consigli per gli account dei membri della tua

organizzazione. Inoltre, gli account membri all'interno dell'organizzazione non sono iscritti a Cost Optimization Hub. Scopri di più in Cost Optimization Hub and Organizations trusted access nella AWS Cost Management User Guide.

Puoi disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno degli AWS SDK.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  È possibile eseguire il comando seguente per disabilitarlo Centrale ottimizzazione costi AWS come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: disabilita AWSServiceAccess

AWS Control Tower e AWS Organizations

AWS Control Tower offre un modo semplice per impostare e governare un AWS ambiente multi-account, seguendo le best practice prescrittive. L'orchestrazione AWS Control Tower estende le capacità di AWS Organizations. AWS Control Tower applica controlli preventivi e investigativi (guardrail) per evitare che le organizzazioni e gli account divergano dalle best practice (deriva).

L'orchestrazione AWS Control Tower estende le capacità di AWS Organizations.

Per ulteriori informazioni, consulta la Guida per l'utente di AWS Control Tower.

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS Control Tower con AWS Organizations.

Ruoli necessari per l'integrazione

Il ruolo `AWSControlTowerExecution` deve essere presente in tutti gli account registrati. Consente a AWS Control Tower di gestire i singoli account e di segnalare le informazioni su di essi agli account di controllo e dell'archivio di log.

Per ulteriori informazioni su ruoli utilizzati da AWS Control Tower, consulta Come AWS Control Tower lavora con i ruoli per creare e gestire account e Utilizzo di policy basate su identità (Policy IAM) per AWS Control Tower.

Principali del servizio usati da AWS Control Tower

AWS Control Tower utilizza il `controltower.amazonaws.com` Principale del servizio.

Abilitazione dell'accesso attendibile con AWS Control Tower

AWS Control Tower utilizza l'accesso attendibile per rilevare le derive per i controlli preventivi e per tenere traccia delle modifiche di account e OU che causano derive.

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Puoi abilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

Per abilitare l'accesso attendibile dalla console Organizations, scegli **`Enable access`** accanto a AWS Control Tower.

Puoi abilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Puoi eseguire il comando seguente per abilitare AWS Control Tower come servizio attendibile con Organizations.

```
$ aws organizations enable-aws-service-access \
```

```
    --service-principal controltower.amazonaws.com
```

Questo comando non produce alcun output se ha esito positivo.

- API AWS: EnableAWSServiceAccess

Disabilitazione dell'accesso attendibile con AWS Control Tower

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Puoi disabilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

> **Important**
>
> La disabilitazione dell'accesso attendibile di AWS Control Tower causa deviazioni nella tua zona di destinazione AWS Control Tower. L'unico modo per correggere questa deviazione è utilizzare la riparazione della zona di destinazione AWS Control Tower. La riabilitazione dell'accesso attendibile in Organizations non risolve il problema della deviazione. Scopri di più sulle deviazioni nella Guida per l'utente di AWS Control Tower.

Puoi disabilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare AWS Control Tower come servizio attendibile con Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal controltower.amazonaws.com
```

Questo comando non produce alcun output se ha esito positivo.

- API AWS: DisableAWSServiceAccess

Amazon Detective e AWS Organizations

Amazon Detective utilizza i dati di registro per generare visualizzazioni che consentono di analizzare, indagare e identificare la causa principale dei risultati sulla sicurezza o delle attività sospette.

L'uso di AWS Organizations consente di garantire che il grafico del comportamento di Detective fornisca visibilità sull'attività per tutti gli account dell'organizzazione.

Quando si concede un accesso attendibile a Detective, il servizio Detective può reagire automaticamente ai cambiamenti nell'appartenenza all'organizzazione. L'amministratore delegato può abilitare qualsiasi account dell'organizzazione come account membro nel grafico del comportamento. Inoltre, Detective può abilitare automaticamente nuovi account dell'organizzazione come account membri. Gli account dell'organizzazione non possono dissociarsi dal grafico del comportamento.

Per ulteriori informazioni, consultare Utilizzo di Amazon Detective nell'organizzazione nella Guida alla gestione di Amazon Detective.

Utilizzare le seguenti informazioni per facilitare l'integrazione di Amazon Detective con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a Detective di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

È possibile eliminare o modificare questo ruolo solo se si disabilita l'accesso attendibile tra Detective e Organizations o se si rimuove l'account membro dall'organizzazione.

- `AWSServiceRoleForDetective`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da Detective concedono l'accesso ai seguenti principali del servizio:

- `detective.amazonaws.com`

Abilitazione dell'accesso attendibile con Detective

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

> **Note**
>
> Quando si designa un amministratore delegato per Amazon Detective, Detective abilita automaticamente l'accesso attendibile per Detective per l'organizzazione.
> Detective richiede l'accesso attendibile a AWS Organizations prima di designare un account membro come amministratore delegato per questo servizio per l'organizzazione.

Puoi abilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

Puoi abilitare l'accesso attendibile tramite la console AWS Organizations.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

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. Nella pagina Services (Servizi), individuare la riga per Amazon Detective, scegliere il nome del servizio, quindi scegliere Enable trusted access (Abilita accesso attendibile).
3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).

4. Per l'amministratore di AWS Organizations, comunicare all'amministratore di Amazon Detective che ora è possibile abilitare quel servizio utilizzando la console per il funzionamento con AWS Organizations.

Disabilitazione dell'accesso attendibile con Detective

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Solo un amministratore nell'account di gestione di AWS Organizations può disabilitare l'accesso attendibile con Amazon Detective.

Puoi disabilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

Puoi disabilitare l'accesso attendibile tramite la console AWS Organizations.

AWS Management Console

Per disabilitare l'accesso al servizio attendibile utilizzando la console Organizations

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. Nella pagina Services (Servizi), individuare la riga di Amazon Detective e scegliere il nome del servizio.
3. Scegli Disable trusted access (Disabilita accesso attendibile).
4. Nella finestra di dialogo di conferma, inserisci **`disable`** nella casella, quindi scegli Disable trusted access (Disabilita accesso attendibile).
5. Per l'amministratore di AWS Organizations, comunicare all'amministratore di Amazon Detective che ora è possibile disabilitare quel servizio utilizzando la console o gli strumenti per il funzionamento con AWS Organizations.

Abilitazione di un account amministratore delegato per Detective

L'account amministratore delegato per Detective è l'account amministratore per un grafico del comportamento di Detective. L'amministratore delegato determina quali account dell'organizzazione abilitare e disabilitare come account membro nel grafico del comportamento. L'amministratore delegato può configurare Detective per abilitare automaticamente nuovi account dell'organizzazione

come account membri quando vengono aggiunti all'organizzazione. Per informazioni su come un amministratore delegato gestisce gli account dell'organizzazione, consultare Gestione degli account dell'organizzazione come account membri nella Guida alla gestione di Amazon Detective.

Solo un amministratore nell'account di gestione dell'organizzazione può configurare un amministratore delegato per Detective.

È possibile specificare un account dell'amministratore delegato dalla console Detective o con l'API oppure tramite la CLI o l'operazione SDK di Organizations.

> **Autorizzazioni minime**
>
> Solo un utente o un ruolo nell'account di gestione di Organizations può configurare un account membro come amministratore delegato per Detective nell'organizzazione

Per configurare un amministratore delegato utilizzando la console o l'API Detective, consultare Designazione di un account amministratore Detective per un'organizzazione nella Guida alla gestione di Amazon Detective.

AWS CLI, AWS API

Se desideri configurare un account di amministratore delegato utilizzando AWS CLI o uno degli SDK AWS, puoi utilizzare anche i seguenti comandi:

- AWS CLI:

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

- SDK AWS: richiama l'operazione `RegisterDelegatedAdministrator` di Organizations e il numero ID dell'account membro e identifica il principale del servizio dell'account `account.amazonaws.com` come parametri.

Disabilitazione di un amministratore delegato per Detective

È possibile rimuovere l'amministratore delegato utilizzando la console o l'API Detective oppure utilizzando `DeregisterDelegatedAdministrator` CLI o l'operazione SDKdi Organizations. Per informazioni su come rimuovere un amministratore delegato utilizzando la console o l'API

Detective o l'API Organizations, consultare Designazione di un account amministratore Detective per un'organizzazione nella Guida alla gestione di Amazon Detective.

Amazon DevOps Guru e AWS Organizations

Amazon DevOps Guru analizza i dati operativi e i parametri e gli eventi delle applicazioni per identificare i comportamenti che si discostano dai normali modelli operativi. Gli utenti ricevono una notifica quando DevOps Guru rileva un problema operativo o un rischio.

L'uso di DevOps Guru consente il supporto multi-account con AWS Organizations in modo da poter designare un account membro per gestire le informazioni dettagliate in tutta l'organizzazione. Questo amministratore delegato può quindi visualizzare, ordinare e filtrare le informazioni da tutti gli account all'interno dell'organizzazione per sviluppare una visione olistica dell'integrità di tutte le applicazioni monitorate all'interno dell'organizzazione senza la necessità di ulteriori personalizzazioni.

Per ulteriori informazioni, consultare Monitoraggio degli account in tutta l'organizzazione nella Guida per l'utente di Amazon DevOps Guru.

Utilizzare le seguenti informazioni per facilitare l'integrazione di Amazon DevOps Guru con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a DevOps Guru di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

È possibile eliminare o modificare questo ruolo solo se si disabilita l'accesso attendibile tra DevOps Guru e Organizations o se si rimuove l'account membro dall'organizzazione.

- `AWSServiceRoleForDevOpsGuru`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da DevOps Guru concedono l'accesso ai seguenti principali del servizio:

- `devops-guru.amazonaws.com`

Per ulteriori informazioni, consultare Utilizzo di ruoli collegati ai servizi per DevOps Guru nella Guida per l'utente di Amazon DevOps Guru.

Abilitazione dell'accesso attendibile con DevOps Guru

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

> **Note**
>
> Quando si designa un amministratore delegato per Amazon DevOps Guru, DevOps Guru abilita automaticamente l'accesso attendibile per DevOps Guru per l'organizzazione. DevOps Guru richiede l'accesso attendibile a AWS Organizations prima di designare un account membro come amministratore delegato per questo servizio per l'organizzazione.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti Amazon DevOps Guru per abilitare l'integrazione con Organizations. Ciò consente ad Amazon DevOps Guru di eseguire qualsiasi configurazione richiesta, ad esempio la creazione di risorse necessarie al servizio. Procedere con questi passaggi solo se non è possibile abilitare l'integrazione utilizzando gli strumenti forniti da Amazon DevOps Guru. Per ulteriori informazioni, consulta questa nota.

È possibile abilitare l'accesso attendibile utilizzando la console AWS Organizations o la console DevOps Guru.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

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. Nella pagina Services (Servizi), individuare la riga per Amazon DevOps Guru, scegliere il nome del servizio, quindi scegliere Enable trusted access (Abilita accesso attendibile).

3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Per l'amministratore di AWS Organizations, comunicare all'amministratore di Amazon DevOps Guru che ora è possibile abilitare quel servizio utilizzando la console per il funzionamento con AWS Organizations.

DevOps Guru console

Abilitazione dell'accesso al servizio attendibile tramite la console DevOps Guru

1. Accedere come amministratore all'account di gestione e aprire la console DevOps Guru: console Amazon DevOps Guru
2. Scegliere Enable trusted access (Abilita accesso sicuro).

Disabilitazione dell'accesso attendibile con DevOps Guru

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Solo un amministratore nell'account di gestione di AWS Organizations può disabilitare l'accesso attendibile con Amazon DevOps Guru.

Puoi disabilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

Puoi disabilitare l'accesso attendibile tramite la console AWS Organizations.

AWS Management Console

Per disabilitare l'accesso al servizio attendibile utilizzando la console Organizations

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. Nella pagina Services (Servizi), individuare la riga di Amazon DevOps Guru e scegliere il nome del servizio.
3. Scegli Disable trusted access (Disabilita accesso attendibile).

4. Nella finestra di dialogo di conferma, inserisci **`disable`** nella casella, quindi scegli Disable trusted access (Disabilita accesso attendibile).
5. Per l'amministratore di AWS Organizations, comunicare all'amministratore di Amazon DevOps Guru che ora è possibile disabilitare quel servizio utilizzando la console o gli strumenti per il funzionamento con AWS Organizations.

Abilitazione di un account amministratore delegato per DevOps Guru

L'account amministratore delegato per DevOps Guru può visualizzare i dati approfonditi di tutti gli account membri che sono registrati con DevOps Guru dall'organizzazione. Per informazioni su come un amministratore delegato gestisce gli account dell'organizzazione, consultare Monitoraggio degli account in tutta l'organizzazione nella Guida per l'utente di Amazon DevOps Guru.

Solo un amministratore nell'account di gestione dell'organizzazione può configurare un amministratore delegato per DevOps Guru.

È possibile specificare un account dell'amministratore delegato dalla console DevOps Guru oppure utilizzando `RegisterDelegatedAdministrator` CLI o l'operazione SDK di Organizations.

> **Autorizzazioni minime**
>
> Solo un utente o un ruolo nell'account di gestione di Organizations può configurare un account membro come amministratore delegato per DevOps Guru nell'organizzazione

DevOps Guru console

Configurazione di un amministratore delegato nella console DevOps Guru

1. Accedere come amministratore all'account di gestione e aprire la console DevOps Guru: console Amazon DevOps Guru
2. Scegliere Registra amministratore delegato. È possibile scegliere l'account di gestione o qualsiasi account membro come amministratore delegato.

AWS CLI, AWS API

Se desideri configurare un account di amministratore delegato utilizzando AWS CLI o uno degli SDK AWS, puoi utilizzare anche i seguenti comandi:

- AWS CLI:

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

- SDK AWS: richiama l'operazione `RegisterDelegatedAdministrator` di Organizations e il numero ID dell'account membro e identifica il principale del servizio dell'account `account.amazonaws.com` come parametri.

Disabilitazione di un amministratore delegato per DevOps Guru

È possibile rimuovere l'amministratore delegato utilizzando la console DevOps Guru oppure utilizzando `DeregisterDelegatedAdministrator` CLI o l'operazione SDKdi Organizations. Per informazioni su come rimuovere un amministratore delegato tramite la console DevOps Guru, consultare Monitoraggio degli account in tutta l'organizzazione nella Guida per l'utente di Amazon DevOps Guru.

AWS Directory Service e AWS Organizations

AWS Directory Service per Microsoft Active Directory, oppure AWS Managed Microsoft AD, ti consente di eseguire Microsoft Active Directory (AD) come servizio gestito. AWS Directory Service semplifica la configurazione e l'esecuzione di directory in AWS Cloud o la connessione delle risorse AWS con una Microsoft Active Directory on-premise esistente. AWS Managed Microsoft AD inoltre, si integra strettamente con AWS Organizations per consentire la condivisione delle directory tra più Account AWS e qualsiasi VPC in una Regione. Per ulteriori informazioni, consulta la Guida per l'amministratore di AWS Directory Service.

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS Directory Service con AWS Organizations.

Abilitazione dell'accesso attendibile con AWS Directory Service

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

È possibile abilitare l'accesso sicuro utilizzando la console AWS Directory Service o la console AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti AWS Directory Service per abilitare l'integrazione con Organizations. Ciò consente a AWS Directory Service di eseguire qualsiasi configurazione richiesta, ad esempio la creazione di risorse necessarie al servizio. Procedi con questi passaggi solo se non è possibile abilitare l'integrazione utilizzando gli strumenti forniti da AWS Directory Service. Per ulteriori informazioni, consulta questa nota.
> Se abiliti l'accesso attendibile utilizzando la console o gli strumenti di AWS Directory Service, non è necessario completare questi passaggi.

Per abilitare l'accesso attendibile tramite la console AWS Directory Service

Per condividere una directory che abilita automaticamente l'accesso attendibile, consulta Condivisione della directory nella Guida per l'amministratore di AWS Directory Service. Per istruzioni dettagliate, consulta Tutorial: Condivisione della directory Microsoft AD gestita da AWS.

Puoi abilitare l'accesso attendibile tramite la console AWS Organizations.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

1. Accedere 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. Nella pagina Services (Servizi), trova la riga per AWS Directory Service, scegli il nome del servizio, quindi scegli Enable trusted access (Abilita accesso attendibile).
3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS Directory Service che ora può abilitare quel servizio utilizzando la console per il funzionamento con AWS Organizations.

Disabilitazione dell'accesso attendibile con AWS Directory Service

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Se disabiliti l'accesso attendibile utilizzando AWS Organizations durante l'utilizzo di AWS Directory Service, tutte le directory condivise in precedenza continuano a funzionare normalmente. Tuttavia, non puoi più condividere nuove directory all'interno dell'organizzazione finché non avrai abilitato nuovamente l'accesso attendibile.

Puoi disabilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

Puoi disabilitare l'accesso attendibile tramite la console AWS Organizations.

AWS Management Console

Per disabilitare l'accesso al servizio attendibile utilizzando la console Organizations

1. Accedere 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. Nella pagina Services (Servizi), individuare la riga per AWS Directory Service e scegliere il nome del servizio.
3. Scegli Disable trusted access (Disabilita accesso attendibile).
4. Nella finestra di dialogo di conferma, inserisci **`disable`** nella casella, quindi scegli Disable trusted access (Disabilita accesso attendibile).
5. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS Directory Service che ora può disabilitare quel servizio utilizzando la console o gli strumenti per il funzionamento con AWS Organizations.

AWS Firewall Manager e AWS Organizations

AWS Firewall Manager è un servizio di gestione della sicurezza utilizzato per configurare e gestire centralmente le regole del firewall e altre protezioni negli Account AWS e nelle applicazioni all'interno dell'organizzazione. Utilizzando Firewall Manager, è possibile distribuire regole AWS WAF, creare protezioni AWS Shield Advanced, configurare e verificare i gruppi di sicurezza Amazon Virtual Private Cloud (Amazon VPC) e distribuire AWS Network Firewall. Utilizza Firewall Manager per configurare le protezioni solo una volta e applicarle automaticamente a tutti gli account e le risorse all'interno della

tua organizzazione, anche se vengono aggiunti nuovi account e risorse. Per ulteriori informazioni su AWS Firewall Manager, consulta la Guida per sviluppatori di AWS Firewall Manager.

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS Firewall Manager con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a Firewall Manager di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra Firewall Manager e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForFMS`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da Firewall Manager concedono l'accesso ai seguenti principali del servizio:

- `fms.amazonaws.com`

Abilitazione dell'accesso attendibile con Firewall Manager

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

È possibile abilitare l'accesso sicuro utilizzando la console AWS Firewall Manager o la console AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti AWS Firewall Manager per abilitare l'integrazione con Organizations. Ciò consente a AWS Firewall Manager di eseguire qualsiasi configurazione richiesta, ad esempio la creazione di risorse necessarie al servizio. Procedi con questi passaggi solo se non è possibile

abilitare l'integrazione utilizzando gli strumenti forniti da AWS Firewall Manager. Per ulteriori informazioni, consulta questa nota.
Se abiliti l'accesso attendibile utilizzando la console o gli strumenti di AWS Firewall Manager, non è necessario completare questi passaggi.

Devi effettuare l'accesso con il tuo account di gestione di AWS Organizations per configurare un account all'interno dell'organizzazione come account amministratore di AWS Firewall Manager. Per ulteriori informazioni, consulta Impostazione dell'account di amministratore AWS Firewall Manager nella Guida per gli sviluppatori di AWS Firewall Manager.

È possibile abilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI o chiamando un'operazione API in un SDK AWS.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

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. Nella pagina Services (Servizi), trova la riga per AWS Firewall Manager, scegli il nome del servizio, quindi scegli Enable trusted access (Abilita accesso attendibile).
3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS Firewall Manager che ora può abilitare quel servizio utilizzando la console per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

Puoi eseguire il comando seguente per abilitare AWS Firewall Manager come servizio attendibile con Organizations.

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

Questo comando non produce alcun output se ha esito positivo.

- API AWS: EnableAWSServiceAccess

Disabilitazione dell'accesso attendibile con Firewall Manager

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

È possibile disabilitare l'accesso attendibile utilizzando la AWS Firewall Manager o gli strumenti AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti AWS Firewall Manager per disabilitare l'integrazione con Organizations. Ciò consente a AWS Firewall Manager di eseguire qualsiasi operazione di pulizia necessaria, ad esempio l'eliminazione di risorse o di ruoli di accesso che non sono più necessari dal servizio. Procedi con questi passaggi solo se non è possibile disabilitare l'integrazione utilizzando gli strumenti forniti da AWS Firewall Manager.
> Se disabiliti l'accesso attendibile utilizzando la console o gli strumenti di AWS Firewall Manager, non è necessario completare questi passaggi.

Per disabilitare l'accesso attendibile tramite la console Firewall Manager

Puoi modificare o revocare l'account amministratore di AWS Firewall Manager seguendo le istruzioni in Designare un account diverso come account amministratore di AWS Firewall Manager nella Guida per gli sviluppatori di AWS Firewall Manager.

Se revochi l'account amministratore, devi accedere all'account di gestione di AWS Organizations e impostare un nuovo account amministratore per AWS Firewall Manager.

È possibile disabilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI Organizations oppure chiamando un'operazione API Organizations in un SDK AWS.

AWS Management Console

Per disabilitare l'accesso al servizio attendibile utilizzando la console Organizations

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. Nella pagina Services (Servizi), individuare la riga per AWS Firewall Manager e scegliere il nome del servizio.
3. Scegli Disable trusted access (Disabilita accesso attendibile).
4. Nella finestra di dialogo di conferma, inserisci **`disable`** nella casella, quindi scegli Disable trusted access (Disabilita accesso attendibile).
5. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS Firewall Manager che ora può disabilitare quel servizio utilizzando la console o gli strumenti per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare AWS Firewall Manager come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal fms.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- API AWS: DisableAWSServiceAccess

Abilitazione di un account di amministratore delegato per Firewall Manager

Quando si designa un account membro come amministratore delegato per l'organizzazione, gli utenti e i ruoli di tale account possono eseguire operazioni amministrative per Firewall Manager che altrimenti possono essere eseguiti solo da utenti o ruoli nell'account di gestione dell'organizzazione. Ciò consente di separare la gestione dell'organizzazione dalla gestione di Firewall Manager.

> **Autorizzazioni minime**
>
> Solo un utente o un ruolo nell'account di gestione di Organizations può configurare un account membro come amministratore delegato per la Gestione dei firewall nell'organizzazione.

Per istruzioni su come designare un account membro come amministratore di Firewall Manager per l'organizzazione, consulta Impostazione dell'account amministratore di AWS Firewall Manager nella Guida per gli sviluppatori di AWS Firewall Manager.

Amazon GuardDuty e AWS Organizations

Amazon GuardDuty è un servizio di monitoraggio continuo della sicurezza che analizza ed elabora una varietà di origini dati, utilizzando feed di intelligence di minacce e il machine learning per identificare attività inattese e potenzialmente non autorizzate e dannose all'interno dell'ambiente AWS. Ciò può includere problemi come le escalation di privilegi, l'utilizzo di credenziali esposte, la comunicazione con indirizzi IP, URL o domini dannosi o la presenza di malware sulle istanze di Amazon Elastic Compute Cloud e sui carichi di lavoro del container.

Puoi semplificare la gestione di GuardDuty utilizzando Organizations per gestire GuardDuty in tutti gli account dell'organizzazione.

Per ulteriori informazioni, consulta Gestione degli account GuardDuty con AWS Organizationsnella Guida per l'utente di Amazon GuardDuty

Utilizza le seguenti informazioni per facilitare l'integrazione di Amazon GuardDuty con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

I seguenti ruoli collegati ai servizi vengono creati automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tali ruoli consentono a GuardDuty di eseguire

le operazioni supportate all'interno degli account dell'organizzazione. Puoi eliminare un ruolo solo se disabiliti l'accesso attendibile tra GuardDuty e Organizations o se rimuovi l'account membro dall'organizzazione.

- Il ruolo collegato al servizio `AWSServiceRoleForAmazonGuardDuty` viene creato automaticamente negli account che hanno integrato GuardDuty con le Organizations. Per ulteriori informazioni, consulta Gestione degli account GuardDuty con Organizations nella Guida per l'utente di Amazon GuardDuty
- Il ruolo collegato al servizio `AmazonGuardDutyMalwareProtectionServiceRolePolicy` viene creato automaticamente negli account che hanno attivato GuardDuty Malware Protection. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi per GuardDuty Malware Protection nella Guida per l'utente di Amazon GuardDuty

Principali del servizio utilizzati dai ruoli collegati ai servizi

- `guardduty.amazonaws.com`, utilizzato dal ruolo collegato ai servizi `AWSServiceRoleForAmazonGuardDuty`.
- `malware-protection.guardduty.amazonaws.com`, utilizzato dal ruolo collegato ai servizi `AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

Abilitazione dell'accesso attendibile con GuardDuty

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Puoi abilitare l'accesso attendibile utilizzando solo Amazon GuardDuty.

Amazon GuardDuty richiede l'accesso attendibile a AWS Organizations prima di designare un account membro come amministratore GuardDuty dell'organizzazione. Se si configura un amministratore delegato utilizzando la console GuardDuty, GuardDuty abilita automaticamente l'accesso attendibile per tuo conto.

Tuttavia, se desideri configurare un account di amministratore delegato utilizzando la AWS CLI o un SDK AWS, devi chiamare esplicitamente l'operazione EnableAWSServiceAccess e fornire il principale del servizio come parametro. Quindi è possibile chiamare EnableOrganizationAdminAccount per delegare l'account amministratore di GuardDuty.

Disabilitazione dell'accesso attendibile con GuardDuty

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Puoi disabilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

Puoi disabilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare Amazon GuardDuty come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal guardduty.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- API AWS: DisableAWSServiceAccess

Abilitazione di un account di amministratore delegato per GuardDuty

Quando si designa un account membro come amministratore delegato per l'organizzazione, gli utenti e i ruoli di tale account possono eseguire operazioni amministrative per GuardDuty che altrimenti possono essere eseguiti solo da utenti o ruoli nell'account di gestione dell'organizzazione. Ciò consente di separare la gestione dell'organizzazione dalla gestione di GuardDuty.

> **Autorizzazioni minime**
>
> Per informazioni sulle autorizzazioni necessarie per designare un account membro come amministratore delegato, consulta Autorizzazioni necessarie per designare un amministratore delegato nella Guida per l'utente di Amazon GuardDuty

Per designare un account membro come amministratore delegato per GuardDuty

Consulta Designare un amministratore delegato e aggiungere account membri (console) e Designare un amministratore delegato e aggiungere account membri (API)

AWS Health e AWS Organizations

AWS Health fornisce una visibilità continua sulle prestazioni delle risorse e sulla disponibilità dei servizi e account AWS. AWS Health crea degli eventi quando le risorse e i servizi AWS sono influenzati da un problema o saranno influenzati dalle modifiche imminenti. Dopo avere abilitato la visualizzazione dell'organizzazione, un utente nell'account di gestione dell'organizzazione può aggregare gli eventi AWS Health in tutti gli account dell'organizzazione. La visualizzazione organizzativa mostra solo gli eventi AWS Health recapitati dopo che la funzionalità è stata abilitata e li conserva per 90 giorni.

Puoi abilitare la visualizzazione organizzativa utilizzando la console AWS Health, la AWS Command Line Interface(AWS CLI), o l'API AWS Health.

Per ulteriori informazioni, consulta Aggregazione di eventi AWS Health nella Guida per l'utente di AWS Health.

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS Health con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a AWS Health di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra AWS Health e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForHealth_Organizations`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da AWS Health concedono l'accesso ai seguenti principali del servizio:

- `health.amazonaws.com`

Abilitazione dell'accesso attendibile con AWS Health

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Quando attivi la caratteristica di visualizzazione organizzativa per AWS Health, viene abilitato automaticamente anche l'accesso attendibile.

È possibile abilitare l'accesso sicuro utilizzando la console AWS Health o la console AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti AWS Health per abilitare l'integrazione con Organizations. Ciò consente a AWS Health di eseguire qualsiasi configurazione richiesta, ad esempio la creazione di risorse necessarie al servizio. Procedi con questi passaggi solo se non è possibile abilitare l'integrazione utilizzando gli strumenti forniti da AWS Health. Per ulteriori informazioni, consulta questa nota.
> Se abiliti l'accesso attendibile utilizzando la console o gli strumenti di AWS Health, non è necessario completare questi passaggi.

Per abilitare l'accesso attendibile tramite la console AWS Health

Puoi abilitare l'accesso attendibile utilizzando AWS Health e una delle seguenti opzioni:

- Tramite la console AWS Health. Per ulteriori informazioni, consulta Visualizzazione organizzativa (console) nella Guida per l'utente di AWS Health.
- Utilizzo della AWS CLI. Per ulteriori informazioni, consulta Visualizzazione organizzativa (CLI) nella Guida per l'utente di AWS Health.
- Chiama l'operazione API EnableHealthServiceAccessForOrganization.

Puoi abilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Puoi eseguire il comando seguente per abilitare AWS Health come servizio attendibile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: EnableAWSServiceAccess

Disabilitazione dell'accesso attendibile con AWS Health

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Dopo avere disabilitato la funzionalità di visualizzazione dell'organizzazione, AWS Health interrompe l'aggregazione degli eventi per tutti gli altri account nell'organizzazione. Ciò, inoltre, disabilita automaticamente l'accesso attendibile.

È possibile disabilitare l'accesso attendibile utilizzando la AWS Health o gli strumenti AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti AWS Health per disabilitare l'integrazione con Organizations. Ciò consente a AWS Health di eseguire qualsiasi operazione di pulizia necessaria, ad esempio l'eliminazione di risorse o di ruoli di accesso che non sono più necessari dal servizio. Procedi con questi passaggi solo se non è possibile disabilitare l'integrazione utilizzando gli strumenti forniti da AWS Health.

Se disabiliti l'accesso attendibile utilizzando la console o gli strumenti di AWS Health, non è necessario completare questi passaggi.

Per abilitare l'accesso attendibile tramite la console AWS Health

Puoi disabilitare l'accesso attendibile con una delle seguenti opzioni:

- Tramite la console AWS Health. Per ulteriori informazioni, consulta Disabilitazione della visualizzazione organizzativa (console) nella Guida per l'utente di AWS Health.
- Utilizzo della AWS CLI. Per ulteriori informazioni, consulta Disabilitazione della visualizzazione organizzativa (CLI) nella Guida per l'utente di AWS Health.
- Chiama l'operazione API DisableHealthServiceAccessForOrganization.

Puoi disabilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare AWS Health come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal health.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: DisableAWSServiceAccess

Abilitazione di un account amministratore delegato per AWS Health

Quando si designa un account membro come amministratore delegato per l'organizzazione, gli utenti e i ruoli di tale account possono eseguire operazioni amministrative per AWS Health che altrimenti

potrebbero essere eseguite solo da utenti o ruoli nell'account di gestione dell'organizzazione. Ciò consente di separare la gestione dell'organizzazione dalla gestione di AWS Health.

Designazione di un account membro come amministratore delegato per AWS Health

Consulta Rimozione di un amministratore delegato dalla tua vista organizzativa

Rimozione di un amministratore delegato per AWS Health

Consulta Rimozione di un amministratore delegato dalla tua vista organizzativa

Amazon Inspector e AWS Organizations

Amazon Inspector è un servizio di gestione delle vulnerabilità automatizzato che scansiona continuamente i carichi di lavoro Amazon EC2 e di container alla ricerca di vulnerabilità software e esposizione alla rete non intenzionale.

Grazie ad Amazon Inspector è possibile gestire più account associati tramite AWS Organizations semplicemente delegando un account amministratore per Amazon Inspector. L'amministratore delegato gestisce Amazon Inspector per l'organizzazione e vengono concesse autorizzazioni speciali per eseguire attività per conto dell'organizzazione come:

- Abilitazione o disabilitazione delle scansioni per gli account membri
- Visualizzazione dei dati di ricerca aggregati dall'intera organizzazione
- Creazione e gestione di regole di soppressione

Per ulteriori informazioni, consultare Gestione di più account con AWS Organizations nella Guida per l'utente di Amazon Inspector.

Utilizza le seguenti informazioni per facilitare l'integrazione di Amazon Inspector con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a Amazon Inspector di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

È possibile eliminare o modificare questo ruolo solo se si disabilita l'accesso attendibile tra Amazon Inspector e Organizations o se si rimuove l'account membro dall'organizzazione.

- `AWSServiceRoleForAmazonInspector2`

Per ulteriori informazioni, consultare Utilizzo di ruoli collegati ai servizi con Amazon Inspector nella Guida per l'utente di Amazon Inspector.

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da Amazon Inspector concedono l'accesso ai seguenti principali del servizio:

- `inspector2.amazonaws.com`

Abilitazione dell'accesso attendibile con Amazon Inspector

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Amazon Inspector richiede l'accesso attendibile a AWS Organizations prima di designare un account membro come amministratore delegato per questo servizio per l'organizzazione.

Quando si designa un amministratore delegato per Amazon Inspector, Amazon Inspector abilita automaticamente l'accesso attendibile per Amazon Inspector per l'organizzazione.

Tuttavia, se si desidera configurare un account da amministratore delegato utilizzando AWS CLI o uno degli SDK AWS, è necessario chiamare esplicitamente l'operazione `EnableAWSServiceAccess` e fornire il principale del servizio come parametro. Quindi è possibile chiamare `EnableDelegatedAdminAccount` per delegare l'account amministratore di Inspector.

Puoi abilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

È possibile emettere il seguente comando per abilitare Amazon Inspector come servizio attendibile con Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal inspector2.amazonaws.com
```

Questo comando non produce alcun output se ha esito positivo.

- API AWS: EnableAWSServiceAccess

> **Note**
>
> Se si sta utilizzando l'API `EnableAWSServiceAccess`, è necessario chiamare anche `EnableDelegatedAdminAccount` per delegare l'account amministratore di Inspector.

Disabilitazione dell'accesso attendibile con Amazon Inspector

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Solo un amministratore nell'account di gestione di AWS Organizations può disabilitare l'accesso attendibile con Amazon Inspector.

Puoi disabilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

Puoi disabilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  È possibile emettere il comando seguente per disabilitare Amazon Inspector come servizio attendibile con Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal inspector2.amazonaws.com
```

Questo comando non produce alcun output se ha esito positivo.

- API AWS: DisableAWSServiceAccess

Abilitazione di un account amministratore delegato per Amazon Inspector

Con Amazon Inspector è possibile gestire più account in un'organizzazione utilizzando un amministratore delegato con il servizio AWS Organizations.

L'account di gestione AWS Organizations designa un account all'interno dell'organizzazione come account amministratore delegato per Amazon Inspector. L'amministratore delegato gestisce Amazon Inspector per l'organizzazione e vengono concesse autorizzazioni speciali per eseguire attività per conto dell'organizzazione, ad esempio: abilitazione o disabilitazione delle scansioni per gli account membri, visualizzazione dei dati di ricerca aggregati dall'intera organizzazione e creazione e gestione delle regole di soppressione

Per informazioni su come un amministratore delegato gestisce gli account dell'organizzazione, consultare Comprendere la relazione tra account amministratore e account membro nella Guida per l'utente di Amazon Inspector.

Solo un amministratore nell'account di gestione dell'organizzazione può configurare un amministratore delegato per Amazon Inspector.

È possibile specificare un account dell'amministratore delegato dalla console Amazon Inspector o con l'API oppure tramite la CLI o l'operazione SDK di Organizations.

> **Autorizzazioni minime**
>
> Solo un utente o un ruolo nell'account di gestione di Organizations può configurare un account membro come amministratore delegato per Amazon Inspector nell'organizzazione

Per configurare un amministratore delegato utilizzando la console Amazon Inspector, consultare Fase 1: Abilitazione di Amazon Inspector - Ambiente multi-account nella Guida per l'utente di Amazon Inspector.

> **Note**
>
> Devi chiamare `inspector2:enableDelegatedAdminAccount` in ogni regione in cui utilizzi Amazon Inspector.

AWS CLI, AWS API

Se desideri configurare un account di amministratore delegato utilizzando AWS CLI o uno degli SDK AWS, puoi utilizzare anche i seguenti comandi:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal inspector2.amazonaws.com
```

- SDK AWS: richiama l'operazione `RegisterDelegatedAdministrator` di Organizations e il numero ID dell'account membro e identifica il principale del servizio dell'account `account.amazonaws.com` come parametri.

Disabilitazione di un amministratore delegato per Amazon Inspector

Solo un amministratore nell'account di gestione di AWS Organizations può rimuovere un account dell'amministratore delegato dall'organizzazione.

È possibile rimuovere l'amministratore delegato utilizzando la console Amazon Inspector o l'API oppure utilizzando `DeregisterDelegatedAdministrator` CLI o l'operazione SDK di Organizations. Per rimuovere un amministratore delegato utilizzando la console Amazon Inspector, consultare Rimozione di un amministratore delegato nella Guida per l'utente di Amazon Inspector.

AWS License Manager e AWS Organizations

AWS License Manager ottimizza il processo per trasferire le licenze di fornitore software nel cloud. Quando crei un'infrastruttura cloud su AWS, puoi limitare i costi sfruttando l'opportunità di utilizzare l'opzione BYOL (Bring-Your-Own-License, uso di licenze proprie), ossia riallocando l'inventario delle licenze esistenti per utilizzarle con le risorse cloud. Con controlli basati su regole sul consumo delle licenze, gli amministratori possono impostare limiti più o meno severi su distribuzioni cloud nuove o esistenti, interrompendo prima del tempo utilizzi del server non conformi.

Per ulteriori informazioni su License Manager, consulta la Guida per l'utente di License Manager.

Collegando lo Strumento di gestione delle licenze ad AWS Organizations, puoi:

- Abilitare il rilevamento delle risorse di elaborazione tra più account in tutta l'organizzazione.
- Visualizzare e gestire gli abbonamenti Linux commerciali che possiedi ed esegui su AWS. Per ulteriori informazioni, consulta Abbonamenti Linux nello AWS License Manager.

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS License Manager con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

I seguenti ruoli collegati ai servizi vengono creati automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Questi ruoli consentono allo Strumento di gestione delle licenze di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questi ruoli solo se disabiliti l'accesso attendibile tra lo Strumento di gestione delle licenze e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSLicenseManagerMasterAccountRole`
- `AWSLicenseManagerMemberAccountRole`
- `AWSServiceRoleForAWSLicenseManagerRole`
- `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService`

Per ulteriori informazioni, consulta Strumento di gestione delle licenze: ruolo dell'account di gestione, Strumento di gestione delle licenze: ruolo dell'account membro e Strumento di gestione delle licenze: ruolo degli abbonamenti Linux.

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da License Manager concedono l'accesso ai seguenti principali del servizio:

- `license-manager.amazonaws.com`
- `license-manager.member-account.amazonaws.com`

- `license-manager-linux-subscriptions.amazonaws.com`

Abilitazione dell'accesso attendibile con License Manager

È possibile abilitare l'accesso attendibile utilizzando solo AWS License Manager.

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Per abilitare l'accesso attendibile tramite License Manager

È necessario accedere alla console di License Manager utilizzando il tuo account di gestione AWS Organizations e associarlo al tuo account di License Manager. Per ulteriori informazioni, consulta la sezione Configurazioni nello AWS License Manager.

Disabilitazione dell'accesso attendibile con License Manager

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Puoi disabilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

Puoi disabilitare l'accesso attendibile eseguendo il comando della AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in uno degli SDK AWS.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare AWS License Manager come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal license-manager.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

Per disabilitare l'accesso attendibile per gli abbonamenti Linux, utilizza:

```
$  aws organizations disable-aws-service-access \
    --service-principal license-manager-linux-subscriptions.amazonaws.com
```

- API AWS: DisableAWSServiceAccess

Abilitazione di un account di amministratore delegato per License Manager

Quando si designa un account membro come amministratore delegato per l'organizzazione, gli utenti e i ruoli di tale account possono eseguire operazioni amministrative per License Manager che altrimenti possono essere eseguiti solo da utenti o ruoli nell'account di gestione dell'organizzazione. Ciò consente di separare la gestione dell'organizzazione dalla gestione di License Manager.

Per delegare un account membro come amministratore di License Manager, attieniti alla procedura descritta in Registrazione di un amministratore delegato nella Guida per l'utente di License Manager.

Amazon Macie e AWS Organizations

Amazon Macie è un servizio di sicurezza e privacy dei dati completamente gestito che utilizza il machine learning e la corrispondenza di modelli per individuare, monitorare e aiutare a proteggere i dati sensibili in Amazon Simple Storage Service (Amazon S3). Macie automatizza la scoperta dei dati sensibili, come le informazioni personali di identificazione (PII) e la proprietà intellettuale, per fornire una migliore comprensione dei dati archiviati dall'organizzazione in Amazon S3.

Per ulteriori informazioni, consulta Gestione di account Amazon Macie con AWS Organizations nella Guida per l'utente di Amazon Macie.

Utilizza le seguenti informazioni per facilitare l'integrazione di Amazon Macie con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account dell'amministratore delegato Macie dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a Macie di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare questo ruolo solo se disabiliti l'accesso attendibile tra Macie e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleRorAmazonMacie`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da Macie concedono l'accesso ai seguenti principali del servizio:

- `macie.amazonaws.com`

Abilitazione dell'accesso attendibile con Macie

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Puoi abilitare l'accesso attendibile utilizzando la console Amazon Macie o la console AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti Amazon Macie per abilitare l'integrazione con Organizations. Ciò consente ad Amazon Macie di eseguire qualsiasi configurazione richiesta, ad esempio la creazione di risorse necessarie al servizio. Procedi con questi passaggi solo se non è possibile abilitare l'integrazione utilizzando gli strumenti forniti da Amazon Macie. Per ulteriori informazioni, consulta questa nota.
>
> Se abiliti l'accesso attendibile utilizzando la console o gli strumenti di Amazon Macie, non è necessario completare questi passaggi.

Per abilitare l'accesso attendibile tramite la console Macie

Amazon Macie richiede l'accesso attendibile a AWS Organizations prima di designare un account membro come amministratore Macie dell'organizzazione. Se si configura un amministratore delegato utilizzando la console di gestione Macie, Macie abilita automaticamente l'accesso attendibile per tuo conto.

Per ulteriori informazioni, consulta Integrazione e configurazione di un'organizzazione in Amazon Macie nella Guida per l'utente di Amazon Macie.

Puoi abilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Puoi eseguire il comando seguente per abilitare Amazon Macie come servizio attendibile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: EnableAWSServiceAccess

Abilitazione di un account di amministratore delegato per Macie

Quando si designa un account membro come amministratore delegato per l'organizzazione, gli utenti e i ruoli di tale account possono eseguire operazioni amministrative per Macie che altrimenti possono essere eseguiti solo da utenti o ruoli nell'account di gestione dell'organizzazione. Ciò consente di separare la gestione dell'organizzazione dalla gestione di Macie.

Autorizzazioni minime

Solo un utente o un ruolo nell'account di gestione di Organizations con le seguenti autorizzazioni può configurare un account membro come amministratore delegato per Macie nell'organizzazione:

- `organizations:EnableAWSServiceAccess`
- `macie:EnableOrganizationAdminAccount`

Per designare un account membro come amministratore delegato per Macie

Amazon Macie richiede l'accesso attendibile a AWS Organizations prima di designare un account membro come amministratore Macie dell'organizzazione. Se si configura un amministratore delegato utilizzando la console di gestione Macie, Macie abilita automaticamente l'accesso attendibile per tuo conto.

Per ulteriori informazioni, consulta https://docs.aws.amazon.com/macie/latest/user/macie-organizations.html#register-delegated-admin

Marketplace AWS e AWS Organizations

Marketplace AWS è un catalogo di risorse digitali selezionate che puoi utilizzare per individuare, acquistare, implementare e gestire in modo semplice i servizi e i software di terze parti necessari per creare soluzioni e gestire la tua attività.

Marketplace AWS crea e gestisce le licenze utilizzando AWS License Manager per i tuoi acquisti in Marketplace AWS. Quando condividi (concedi l'accesso a) le tue licenze con altri account dell'organizzazione, Marketplace AWS crea e gestisce nuove licenze per tali account.

Per ulteriori informazioni, consulta Utilizzo dei ruoli collegati ai servizi per Marketplace AWS nella Guida per l'acquirente di Marketplace AWS.

Utilizza le seguenti informazioni per facilitare l'integrazione di Marketplace AWS con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a Marketplace AWS di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra Marketplace AWS e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForMarketplaceLicenseManagement`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da Marketplace AWS concedono l'accesso ai seguenti principali del servizio:

- `license-management.marketplace.amazonaws.com`

Abilitazione dell'accesso attendibile con Marketplace AWS

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

È possibile abilitare l'accesso sicuro utilizzando la console Marketplace AWS o la console AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti Marketplace AWS per abilitare l'integrazione con Organizations. Ciò consente a Marketplace AWS di eseguire qualsiasi configurazione richiesta, ad esempio la creazione di risorse necessarie al servizio. Procedi con questi passaggi solo se non è possibile abilitare l'integrazione utilizzando gli strumenti forniti da Marketplace AWS. Per ulteriori informazioni, consulta questa nota.
> Se abiliti l'accesso attendibile utilizzando la console o gli strumenti di Marketplace AWS, non è necessario completare questi passaggi.

Per abilitare l'accesso attendibile tramite la console Marketplace AWS

Consulta Creazione di un ruolo collegato ai servizi per Marketplace AWS nella Guida per gli acquirenti di Marketplace AWS.

È possibile abilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI o chiamando un'operazione API in un SDK AWS.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

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. Nella pagina Services (Servizi), trova la riga per Marketplace AWS, scegli il nome del servizio, quindi scegli Enable trusted access (Abilita accesso attendibile).

3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di Marketplace AWS che ora può abilitare quel servizio utilizzando la console per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Puoi eseguire il comando seguente per abilitare Marketplace AWS come servizio attendibile con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: EnableAWSServiceAccess

Disabilitazione dell'accesso attendibile con Marketplace AWS

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Puoi abilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

Puoi disabilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare Marketplace AWS come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: DisableAWSServiceAccess

Marketplace AWS Marketplace privato e AWS Organizations

Marketplace AWS è un catalogo digitale curato che puoi utilizzare per trovare, acquistare, distribuire e gestire software, dati e servizi di terze parti necessari per creare soluzioni e gestire le tue attività. Un marketplace privato offre un ampio catalogo di prodotti disponibili in Marketplace AWS, oltre a un controllo approfondito di tali prodotti.

Marketplace AWS Private Marketplace ti consente di creare più esperienze di marketplace private associate all'intera organizzazione, a una o più unità organizzative o a uno o più account dell'organizzazione, ciascuno con il proprio set di prodotti approvati. AWS Gli amministratori possono anche applicare il marchio aziendale a ogni esperienza di marketplace privato con il logo, i messaggi e lo schema di colori dell'azienda o del team.

Per ulteriori informazioni, consulta la sezione Utilizzo dei ruoli per configurare Private Marketplace Marketplace AWSnella GuidaMarketplace AWS all'acquisto.

Utilizza le seguenti informazioni per aiutarti a integrare Marketplace AWS Private Marketplace con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato al servizio viene creato automaticamente nell'account di gestione dell'organizzazione quando si abilita l'accesso affidabile utilizzando la console Private Marketplace AWS Marketplace. Questo ruolo consente a Private Marketplace di eseguire operazioni supportate

all'interno degli account dell'organizzazione all'interno dell'organizzazione. Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso affidabile tra Marketplace AWS Private Marketplace e Organizations e dissocii tutte le esperienze di marketplace privato nella tua organizzazione.

Se abiliti l'accesso affidabile direttamente dalla console Organizations, dalla CLI o dall'SDK, il ruolo collegato al servizio non viene creato automaticamente.

- `AWSServiceRoleForPrivateMarketplaceAdmin`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da Private Marketplace concedono l'accesso ai seguenti principali di servizio:

- `private-marketplace.marketplace.amazonaws.com`

Abilitare l'accesso affidabile con Private Marketplace

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Puoi abilitare l'accesso affidabile utilizzando la console Marketplace AWS Private Marketplace o la AWS Organizations console.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti di Marketplace AWS Private Marketplace per abilitare l'integrazione con Organizations. Ciò consente a Marketplace AWS Private Marketplace di eseguire qualsiasi configurazione richiesta, ad esempio la creazione delle risorse necessarie al servizio. Procedi con questi passaggi solo se non riesci ad abilitare l'integrazione utilizzando gli strumenti forniti da Marketplace AWS Private Marketplace. Per ulteriori informazioni, consulta questa nota.
> Se abiliti l'accesso affidabile utilizzando la console o gli strumenti di Marketplace AWS Private Marketplace, non è necessario completare questi passaggi.

Per abilitare l'accesso affidabile utilizzando la console Private Marketplace

Consulta la sezione Guida introduttiva a Private Marketplace nella GuidaMarketplace AWS all'acquisto.

Puoi abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in uno degli AWS SDK.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

1. Accedi alla consoleAWS 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. Nella pagina Servizi, trova la riga relativa a Marketplace AWS Private Marketplace, scegli il nome del servizio, quindi scegli Abilita accesso affidabile.
3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore di Marketplace AWS Private Marketplace che ora può abilitare quel servizio utilizzando la sua console con cui lavorare AWS Organizations.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  È possibile eseguire il comando seguente per abilitare Marketplace AWS Private Marketplace come servizio affidabile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: Abilita AWSServiceAccess

Disabilitazione dell'accesso affidabile con Private Marketplace

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Puoi disabilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

Puoi disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno degli AWS SDK.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  È possibile eseguire il comando seguente per disabilitare Marketplace AWS Private Marketplace come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal private-marketplace.marketplace.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: disabilita AWSServiceAccess

Abilitazione di un account amministratore delegato per Private Marketplace

L'amministratore dell'account di gestione può delegare le autorizzazioni amministrative di Private Marketplace a un account membro designato noto come amministratore delegato. Per registrare un account come amministratore delegato per il marketplace privato, l'amministratore dell'account di gestione deve assicurarsi che l'accesso affidabile e il ruolo collegato al servizio siano abilitati, scegliere Registra un nuovo amministratore, fornire il numero di account a 12 cifre AWS e scegliere Invia.

Gli account di gestione e gli account amministratore delegato possono eseguire attività amministrative di Private Marketplace, come la creazione di esperienze, l'aggiornamento delle

impostazioni di branding, l'associazione o la dissociazione dei segmenti di pubblico, l'aggiunta o la rimozione di prodotti e l'approvazione o il rifiuto delle richieste in sospeso.

Per configurare un amministratore delegato utilizzando la console Private Marketplace, consulta Creazione e gestione di un marketplace privato nella Guida all'Marketplace AWS acquisto.

Puoi anche configurare un amministratore delegato utilizzando l'`RegisterDelegatedAdministrator`API Organizations. Per ulteriori informazioni, vedere RegisterDelegatedAdministratorOrganizations Command Reference.

Disabilitazione di un amministratore delegato per Private Marketplace

Solo un amministratore dell'account di gestione dell'organizzazione può configurare un amministratore delegato per Private Marketplace.

Puoi rimuovere l'amministratore delegato utilizzando la console o l'API di Private Marketplace oppure utilizzando l'operazione Organizations `DeregisterDelegatedAdministrator` CLI o SDK.

Per disabilitare l'account Private Marketplace come amministratore delegato tramite la console Private Marketplace, consulta Creazione e gestione di un marketplace privato nella Guida all'Marketplace AWS acquisto

AWS Network Manager e AWS Organizations

Network Manager ti consente di gestire centralmente la tua rete core WAN di AWS Cloud e la tua rete di AWS Transit Gateway su account, regioni e posizioni on-premise AWS. Con il supporto multi-account puoi creare un'unica rete globale per qualsiasi tuo AWS e registrare i gateway di transito da più account sulla rete globale utilizzando la console Network Manager.

Con l'accesso attendibile tra Network Manager e Organizations abilitato, gli amministratori delegati registrati e gli account di gestione possono sfruttare il ruolo collegato al servizio implementato negli account membri per descrivere le risorse collegate alle reti globali. Dalla console di Network Manager gli amministratori delegati registrati e gli account di gestione possono assumere i ruoli IAM personalizzati distribuiti negli account membri: `CloudWatch-CrossAccountSharingRole` per il monitoraggio e gli eventi multi-account e `IAMRoleForAWSNetworkManagerCrossAccountResourceAccess`per l'accesso ai ruoli dello switch della console per la visualizzazione e la gestione di risorse multi-account)

Important

- Consigliamo vivamente di utilizzare la console di Network Manager per gestire le impostazioni multi-account (abilitazione/disabilitazione dell'accesso attendibile e registrazione/annullamento della registrazione degli amministratori delegati). La gestione di queste impostazioni dalla console implementa e gestisce automaticamente tutti i ruoli collegati al servizio e i ruoli IAM personalizzati negli account membri necessari per l'accesso a più account.
- Quando si abilita l'accesso attendibile per Network Manager nella console di Network Manager, la console abilita anche il servizio AWS CloudFormation StackSets. Network Manager utilizza StackSets per implementare ruoli IAM personalizzati necessari per la gestione multi-account.

Per ulteriori informazioni sull'integrazione di Network Manager con Organizations, consulta Gestione di più account in Network Manager conAWS Organizations nella Guida per l'utente di Amazon VPC.

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS Network Manager con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

I seguenti ruoli collegati ai servizi vengono creati automaticamente negli account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a Network Manager di eseguire le operazioni supportate all'interno degli account nella tua organizzazione. Se si disabilita l'accesso attendibile, Network Manager non eliminerà questi ruoli dagli account dell'organizzazione. Sarà possibile eliminarli manualmente utilizzando la console IAM.

gestione dell'account

- `AWSServiceRoleForNetworkManager`
- `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`
- `AWSServiceRoleForCloudWatchCrossAccount`

Account membri

- `AWSServiceRoleForNetworkManager`

- `AWSServiceRoleForCloudFormationStackSetsOrgMember`

Quando registri un account membro come amministratore delegato, viene creato automaticamente il seguente ruolo aggiuntivo nell'account dell'amministratore delegato:

- `AWSServiceRoleForCloudWatchCrossAccount`

Principali del servizio utilizzati dai ruoli collegati ai servizi

I ruoli collegati ai servizi possono essere assunti solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo.

- Per il ruolo `AWSServiceRoleForNetworkManager service-linked`, `networkmanager.amazonaws.com` è l'unico principale di servizio che ha accesso.
- Per il ruolo collegato al servizio `AWSServiceRoleForCloudFormationStackSetsOrgMember`, `member.org.stacksets.cloudformation.amazonaws.com` è l'unico principale di servizio che ha accesso.
- Per il ruolo collegato al servizio `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`, `stacksets.cloudformation.amazonaws.com` è l'unico principale di servizio che ha accesso.
- Per il ruolo collegato al servizio `AWSServiceRoleForCloudWatchCrossAccount`, `cloudwatch-crossaccount.amazonaws.com` è l'unico principale di servizio che ha accesso.

L'eliminazione di questi ruoli comprometterà la funzionalità multi-account per Network Manager.

Abilitazione dell'accesso attendibile con Network Manager

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Solo un amministratore nell'account di gestione dell'organizzazione dispone delle autorizzazioni per abilitare l'accesso attendibile con un altro servizio AWS. Assicurati di utilizzare la console di Network Manager per abilitare l'accesso attendibile ed evitare problemi di autorizzazioni. Per ulteriori informazioni, consulta Gestione di più account in Network Manager con AWS Organizations nella Guida per l'utente di Amazon VPC.

Disabilitazione dell'accesso attendibile con Network Manager

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Solo un amministratore nell'account di gestione dell'organizzazione dispone delle autorizzazioni per disabilitare l'accesso attendibile con un altro servizio AWS.

> **Important**
>
> Consigliamo vivamente di utilizzare la console Network Manager per disabilitare l'accesso attendibile. Se disabiliti l'accesso attendibile in qualsiasi altro modo, ad esempio tramite AWS CLI, con un'API o con la console AWS CloudFormation, AWS CloudFormation StackSets e i ruoli IAM personalizzati implementati potrebbero non essere ripuliti correttamente. Per disabilitare l'accesso al servizio attendibile, accedi alla console di Network Manager.

Abilitazione di un account di amministratore delegato per Network Manager

Quando si designa un account membro come amministratore delegato per l'organizzazione, gli utenti e i ruoli di tale account possono eseguire operazioni amministrative per Network Manager che altrimenti potrebbero essere eseguite solo da utenti o ruoli nell'account di gestione dell'organizzazione. Ciò consente di separare la gestione dell'organizzazione dalla gestione di Network Manager.

Per le istruzioni su come designare un account membro come amministratore delegato di Network Manager nell'organizzazione, consulta Registrazione di un amministratore delegato nella Guida per l'utente di Amazon VPC.

AWS Resource Access Manager e AWS Organizations

AWS Resource Access Manager (AWS RAM) consente di condividere le risorse AWS specificate di cui si è proprietari con altri Account AWS. È un servizio centralizzato che offre un'esperienza coerente per la condivisione di diversi tipi di risorse AWS su più account.

Per ulteriori informazioni su AWS RAM, consulta la Guida per l'utente di AWS RAM.

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS Resource Access Manager con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a AWS RAM di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra AWS RAM e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForResourceAccessManager`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da AWS RAM concedono l'accesso ai seguenti principali del servizio:

- `ram.amazonaws.com`

Abilitazione dell'accesso attendibile con AWS RAM

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

È possibile abilitare l'accesso sicuro utilizzando la console AWS Resource Access Manager o la console AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti AWS Resource Access Manager per abilitare l'integrazione con Organizations. Ciò consente a AWS Resource Access Manager di eseguire qualsiasi configurazione richiesta, ad esempio la creazione di risorse necessarie al servizio. Procedi con questi passaggi solo se non è possibile abilitare l'integrazione utilizzando gli strumenti forniti da AWS Resource Access Manager. Per ulteriori informazioni, consulta questa nota.
> Se abiliti l'accesso attendibile utilizzando la console o gli strumenti di AWS Resource Access Manager, non è necessario completare questi passaggi.

Per abilitare l'accesso attendibile tramite la console AWS RAM o la CLI

Consulta Abilitazione della condivisione con AWS Organizations nella Guida per l'utente di AWS RAM.

È possibile abilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI o chiamando un'operazione API in un SDK AWS.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

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. Nella pagina Services (Servizi), trova la riga per AWS Resource Access Manager, scegli il nome del servizio, quindi scegli Enable trusted access (Abilita accesso attendibile).
3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS Resource Access Manager che ora può abilitare quel servizio utilizzando la console per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Puoi eseguire il comando seguente per abilitare AWS Resource Access Manager come servizio attendibile con Organizations.

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

Questo comando non produce alcun output se ha esito positivo.

- API AWS: EnableAWSServiceAccess

Disabilitazione dell'accesso attendibile con AWS RAM

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

È possibile disabilitare l'accesso attendibile utilizzando la AWS Resource Access Manager o gli strumenti AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti AWS Resource Access Manager per disabilitare l'integrazione con Organizations. Ciò consente a AWS Resource Access Manager di eseguire qualsiasi operazione di pulizia necessaria, ad esempio l'eliminazione di risorse o di ruoli di accesso che non sono più necessari dal servizio. Procedi con questi passaggi solo se non è possibile disabilitare l'integrazione utilizzando gli strumenti forniti da AWS Resource Access Manager.
> Se disabiliti l'accesso attendibile utilizzando la console o gli strumenti di AWS Resource Access Manager, non è necessario completare questi passaggi.

Disabilitazione dell'accesso attendibile tramite la console AWS Resource Access Manager o la CLI

Consulta Abilitazione della condivisione con AWS Organizations nella Guida per l'utente di AWS RAM.

È possibile disabilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI Organizations oppure chiamando un'operazione API Organizations in un SDK AWS.

AWS Management Console

Per disabilitare l'accesso al servizio attendibile utilizzando la console Organizations

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. Nella pagina Services (Servizi), individuare la riga per AWS Resource Access Manager e scegliere il nome del servizio.
3. Scegli Disable trusted access (Disabilita accesso attendibile).
4. Nella finestra di dialogo di conferma, inserisci **`disable`** nella casella, quindi scegli Disable trusted access (Disabilita accesso attendibile).
5. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS Resource Access Manager che ora può disabilitare quel servizio utilizzando la console o gli strumenti per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare AWS Resource Access Manager come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ram.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: DisableAWSServiceAccess

Esploratore di risorse AWS e AWS Organizations

Esploratore di risorse AWS è un servizio di ricerca e rilevamento di risorse. Con Esploratore di risorse, puoi esplorare le tue risorse, come le istanze Amazon Elastic Compute Cloud, Flusso di dati Amazon Kinesis o le tabelle Amazon DynamoDB, utilizzando un'esperienza simile a quella dei motori di ricerca Internet. Puoi cercare le tue risorse utilizzando i metadati delle risorse come nomi, tag e ID. Esploratore di risorse funziona in tutte le regioni AWS del tuo account per semplificare i carichi di lavoro tra regioni.

Quando integri Esploratore di risorse con AWS Organizations, puoi raccogliere prove da una fonte più ampia includendo più Account AWS all'interno dell'organizzazione nell'ambito delle valutazioni.

Utilizza le seguenti informazioni per facilitare l'integrazione di Esploratore di risorse AWS con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a Esploratore di risorse di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra Esploratore di risorse e Organizations o se rimuovi l'account membro dall'organizzazione.

Per ulteriori informazioni su come Esploratore di risorse utilizza questo ruolo, consulta Using service-linked roles nella Guida per l'utente di Esploratore di risorse AWS.

- `AWSServiceRoleForResourceExplorer`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da Esploratore di risorse concedono l'accesso ai seguenti principali del servizio:

- `resource-explorer-2.amazonaws.com`

Abilitazione dell'accesso attendibile con Esploratore di risorse AWS

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Esploratore di risorse richiede l'accesso attendibile a AWS Organizations prima di designare un account membro come amministratore delegato dell'organizzazione.

Puoi abilitare l'accesso attendibile utilizzando la console Esploratore di risorse o la console Organizations. Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti Esploratore di risorse per abilitare l'integrazione con Organizations. Ciò consente a Esploratore

di risorse AWS di eseguire qualsiasi configurazione richiesta, ad esempio la creazione di risorse necessarie al servizio.

Abilitazione dell'accesso attendibile tramite la console Esploratore di risorse

Per istruzioni su come abilitare l'accesso attendibile, consulta la pagina Prerequisites to using Resource Explorer nella Guida per l'utente di Esploratore di risorse AWS.

> **Note**
>
> Se si configura un amministratore delegato utilizzando la console Esploratore di risorse AWS, Esploratore di risorse AWS abilita automaticamente l'accesso attendibile per tuo conto.

Puoi abilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Puoi eseguire il comando seguente per abilitare Esploratore di risorse AWS come servizio attendibile con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: EnableAWSServiceAccess

Disabilitazione dell'accesso attendibile con Esploratore di risorse

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Solo un amministratore nell'account di gestione di AWS Organizations può disabilitare l'accesso attendibile con Esploratore di risorse AWS.

È possibile disabilitare l'accesso attendibile utilizzando la Esploratore di risorse AWS o gli strumenti AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti Esploratore di risorse AWS per disabilitare l'integrazione con Organizations. Ciò consente a Esploratore di risorse AWS di eseguire qualsiasi operazione di pulizia necessaria, ad esempio l'eliminazione di risorse o di ruoli di accesso che non sono più necessari dal servizio. Procedi con questi passaggi solo se non è possibile disabilitare l'integrazione utilizzando gli strumenti forniti da Esploratore di risorse AWS.
> Se disabiliti l'accesso attendibile utilizzando la console o gli strumenti di Esploratore di risorse AWS, non è necessario completare questi passaggi.

Puoi disabilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare Esploratore di risorse AWS come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- API AWS: DisableAWSServiceAccess

Abilitazione di un account amministratore delegato per Esploratore di risorse

Utilizza il tuo account amministratore delegato per creare visualizzazioni di risorse multi-account e applicarle a un'unità organizzativa o all'intera organizzazione. Puoi condividere visualizzazioni multi-account con qualsiasi account dell'organizzazione tramite AWS Resource Access Manager creando condivisioni di risorse.

> **Autorizzazioni minime**
>
> Solo un utente o un ruolo nell'account di gestione di Organizations con la seguente autorizzazione può configurare un account membro come amministratore delegato per Esploratore di risorse nell'organizzazione: `resource-explorer:RegisterAccount`

Per istruzioni sull'abilitazione di un account di amministratore delegato per Esploratore di risorse, consulta la pagina Setting Up nella Guida per l'utente di Esploratore di risorse AWS.

Se configuri un amministratore delegato utilizzando la console Esploratore di risorse AWS, Esploratore di risorse abilita automaticamente l'accesso attendibile per tuo conto.

AWS CLI, AWS API

Se desideri configurare un account di amministratore delegato utilizzando AWS CLI o uno degli SDK AWS, puoi utilizzare anche i seguenti comandi:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal resource-explorer-2.amazonaws.com
```

- AWS SDK: richiama l'operazione di `RegisterDelegatedAdministrator` di Organizations, il numero identificativo dell'account membro e identificativo del servizio dell'account `resource-explorer-2.amazonaws.com`come parametri.

Disabilitazione di un amministratore delegato per Esploratore di risorse

Solo un amministratore nell'account di gestione di Organizations o nell'account amministratore delegato di Esploratore di risorse può rimuovere un amministratore delegato per

Esploratore di risorse. È possibile disabilitare l'accesso attendibile utilizzando l'operazione `DeregisterDelegatedAdministrator` dell'SDK o della CLI di Organizations.

AWS Security Hub e AWS Organizations

AWS Security Hub offre una visione completa dello stato di sicurezza AWS e consente di verificare la conformità dell'ambiente agli standard e alle best practice del settore della sicurezza.

Security Hub raccoglie dati sulla sicurezza da tutti i tuoi prodotti Account AWS, dai AWS servizi che utilizzi e dai prodotti partner di terze parti supportati. Ti aiuta ad analizzare le tendenze di sicurezza e identificare i problemi di sicurezza più importanti.

Quando utilizzi sia Security Hub che AWS Organizations insieme, puoi abilitare automaticamente Security Hub per tutti i tuoi account, inclusi i nuovi account man mano che vengono aggiunti. Ciò aumenta la copertura per i controlli e i risultati di Security Hub, che fornisce un quadro più completo e accurato della posizione di sicurezza generale.

Per ulteriori informazioni relative a Security Hub, consulta la Guida per l'utente diAWS Security Hub.

Utilizza le seguenti informazioni per facilitare l'integrazione AWS Security Hub con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a Security Hub di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra Security Hub e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForSecurityHub`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da Security Hub concedono l'accesso ai seguenti principali del servizio:

- `securityhub.amazonaws.com`

Abilitazione dell'accesso attendibile con Security Hub

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Quando si designa un amministratore delegato per Security Hub, Security Hub abilita automaticamente l'accesso attendibile per Security Hub nell'organizzazione.

Abilitazione di un account di amministratore delegato per Security Hub

Quando si designa un account membro come amministratore delegato per l'organizzazione, gli utenti e i ruoli di tale account possono eseguire operazioni amministrative per Security Hub che altrimenti possono essere eseguiti solo da utenti o ruoli nell'account di gestione dell'organizzazione. Ciò consente di separare la gestione dell'organizzazione dalla gestione di Security Hub.

Per ulteriori informazioni, consulta Designazione di un account amministratore di Security Hub nella Guida per l'utente diAWS Security Hub .

Per designare un account membro come amministratore delegato per Security Hub

1. Accedi con il tuo account di gestione di Organizations.
2. Effettua una delle seguenti operazioni:
   - Se nel tuo account di gestione non è abilitato Security Hub, nella console di Security Hub scegli Go to (Vai a) Security Hub.
   - Se il tuo account di gestione ha Security Hub abilitato, nella console di Security Hub, in Generale, scegli Impostazioni.
3. In Delegated Administrator (Amministratore delegato), inserisci l'ID dell'account.

Amazon S3 Storage Lens e AWS Organizations

Consentendo ad Amazon S3 Storage Lens l'accesso attendibile alla tua organizzazione, consenti al servizio di raccogliere e aggregare parametri in tutti gli Account AWS nell'organizzazione. S3 Storage Lens consente di accedere all'elenco degli account che appartengono all'organizzazione e raccoglie e analizza i parametri di archiviazione, utilizzo e attività per tali account.

Per ulteriori informazioni, consulta Utilizzo dei ruoli collegati ai servizi per Amazon S3 Storage Lens nella Guida per l'utente di Amazon S3 Storage Lens.

Utilizza le seguenti informazioni per facilitare l'integrazione di Amazon S3 Storage Lens con AWS Organizations.

Ruolo collegato ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account dell'amministratore delegato dell'organizzazione quando abiliti l'accesso attendibile e all'organizzazione è stata applicata la configurazione di Storage Lens. Tale ruolo consente ad Amazon S3 Storage Lens di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra Amazon S3 Storage Lens e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForS3StorageLens`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da Amazon S3 Storage Lens concedono l'accesso ai seguenti principali del servizio:

- `storage-lens.s3.amazonaws.com`

Abilitazione dell'accesso attendibile con Amazon S3 Storage Lens

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Puoi abilitare l'accesso attendibile utilizzando la console Amazon S3 Storage Lens o la console AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti Amazon S3 Storage Lens per abilitare l'integrazione con Organizations. Ciò consente ad Amazon

S3 Storage Lens di eseguire qualsiasi configurazione richiesta, ad esempio la creazione di risorse necessarie al servizio. Procedi con questi passaggi solo se non è possibile abilitare l'integrazione utilizzando gli strumenti forniti da Amazon S3 Storage Lens. Per ulteriori informazioni, consulta questa nota.
Se abiliti l'accesso attendibile utilizzando la console o gli strumenti di Amazon S3 Storage Lens, non è necessario completare questi passaggi.

Per abilitare l'accesso attendibile tramite la console Amazon S3

Consulta Come abilitare l'accesso attendibile nella Guida per l'utente di Amazon Simple Storage Service.

È possibile abilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI o chiamando un'operazione API in un SDK AWS.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

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. Nella pagina Services (Servizi), trova la riga per Amazon S3 Storage Lens, scegli il nome del servizio, quindi scegli Enable trusted access (Abilita accesso attendibile).
3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di Amazon S3 Storage Lens che ora può abilitare quel servizio utilizzando la console per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Puoi eseguire il comando seguente per abilitare Amazon S3 Storage Lens come servizio attendibile con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal storage-lens.s3.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: EnableAWSServiceAccess

Disabilitazione dell'accesso attendibile con Amazon S3 Storage Lens

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Puoi disabilitare l'accesso attendibile utilizzando solo gli strumenti Amazon S3 Storage Lens.

Puoi disabilitare l'accesso attendibile utilizzando la console Amazon S3, la CLI AWS o uno qualsiasi degli SDK di AWS.

Per disabilitare l'accesso attendibile tramite la console Amazon S3

Consulta Come disabilitare l'accesso attendibile nella Guida per l'utente di Amazon Simple Storage Service.

Abilitazioe di un account di amministratore delegato per Amazon S3 Storage Lens

Quando si designa un account membro come amministratore delegato per l'organizzazione, gli utenti e i ruoli di tale account possono eseguire operazioni amministrative per Amazon S3 Storage Lens che altrimenti possono essere eseguiti solo da utenti o ruoli nell'account di gestione dell'organizzazione. Ciò consente di separare la gestione dell'organizzazione dalla gestione di Amazon S3 Storage Lens.

> **Autorizzazioni minime**
>
> Solo un utente o un ruolo nell'account di gestione di Organizations con la seguente autorizzazione può configurare un account membro come amministratore delegato per Amazon S3 Storage Lens nell'organizzazione: `organizations:RegisterDelegatedAdministrator`

```
organizations:DeregisterDelegatedAdministrator
```

Amazon S3 Storage Lens supporta un massimo di 5 account di amministratore delegato nell'organizzazione.

Per designare un account membro come amministratore delegato per Amazon S3 Storage Lens

Puoi registrare un amministratore delegato utilizzando la console Amazon S3, la AWS CLI o uno qualsiasi degli SDK AWS. Per registrare un account membro come account di amministratore delegato per la tua organizzazione utilizzando la console Amazon S3, consulta Registrazione di un amministratore delegato nella Guida per l'utente di Amazon Simple Storage Service.

Per annullare la registrazione di un amministratore delegato per Amazon S3 Storage Lens

Puoi annullare la registrazione di un amministratore delegato utilizzando la console Amazon S3, la AWS CLI o uno qualsiasi degli SDK AWS. Per annullare la registrazione di un account membro come account di amministratore delegato per la tua organizzazione utilizzando la console Amazon S3, consulta Annullamento della registrazione di un amministratore delegato nella Guida per l'utente di Amazon Simple Storage Service.

Amazon Security Lake e AWS Organizations

Amazon Security Lake centralizza i dati di sicurezza provenienti da origini cloud, on-premise e personalizzate in un data lake archiviato nel tuo account. Grazie all'integrazione con Organizations, puoi creare un data lake che raccoglie log ed eventi nei tuoi account. Per ulteriori informazioni, consulta Gestione di più account con AWS Organizations nella Guida per l'utente di Amazon Security Lake.

Utilizza le seguenti informazioni per aiutarti a integrare Amazon Security Lake con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Questo ruolo consente ad Amazon Security Lake di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso affidabile tra Amazon Security Lake e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForSecurityLake`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da Amazon Security Lake garantiscono l'accesso ai seguenti principali di servizio:

- `securitylake.amazonaws.com`

Abilitare l'accesso affidabile con Amazon Security Lake

Quando abiliti l'accesso attendibile con Security Lake, quest'ultimo può reagire automaticamente ai cambiamenti nell'appartenenza all'organizzazione. L'amministratore delegato può abilitare la raccolta AWS dei log dai servizi supportati in qualsiasi account dell'organizzazione. Per ulteriori informazioni, consulta il ruolo collegato al servizio per Amazon Security Lake nella Guida per l'utente di Amazon Security Lake.

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Puoi abilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

Puoi abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in uno degli AWS SDK.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

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. Nella pagina Servizi, individua la riga di Amazon Security Lake, scegli il nome del servizio, quindi Abilita accesso attendibile.
3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).

4. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore di Amazon Security Lake che ora può abilitare quel servizio utilizzando la sua console con cui lavorare AWS Organizations.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile ai servizi:

- AWS CLI: enable-aws-service-access

  Puoi eseguire il seguente comando per abilitare Amazon Security Lake come servizio attendibile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: Abilita AWSServiceAccess

Disabilitazione dell'accesso affidabile con Amazon Security Lake

Solo un amministratore dell'account di gestione Organizations può disabilitare l'accesso affidabile con Amazon Security Lake.

Puoi disabilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

Puoi disabilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno degli AWS SDK.

AWS Management Console

Per disabilitare l'accesso al servizio attendibile utilizzando la console Organizations

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. Nella pagina Servizi, individua la riga di Amazon Security Lake e scegli il nome del servizio.
3. Scegli Disable trusted access (Disabilita accesso attendibile).
4. Nella finestra di dialogo di conferma, inserisci **`disable`** nella casella, quindi scegli Disable trusted access (Disabilita accesso attendibile).
5. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore di Amazon Security Lake che ora può disabilitare quel servizio utilizzando la console o gli strumenti con cui lavorare AWS Organizations.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare Amazon Security Lake come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal securitylake.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: disabilita AWSServiceAccess

Abilitazione di un account amministratore delegato per Amazon Security Lake

L'amministratore delegato di Amazon Security Lake aggiunge altri account dell'organizzazione come account membro. L'amministratore delegato può abilitare Amazon Security Lake e configurare le impostazioni di Amazon Security Lake per gli account dei membri. L'amministratore delegato può raccogliere i log di un'organizzazione in tutte le AWS regioni in cui Amazon Security Lake è abilitato (indipendentemente dall'endpoint regionale attualmente in uso).

Puoi anche configurare l'amministratore delegato per aggiungere automaticamente nuovi account nell'organizzazione come membri. L'amministratore delegato di Amazon Security Lake ha accesso ai log e agli eventi negli account dei membri associati. Di conseguenza, puoi configurare Amazon

Security Lake per raccogliere dati di proprietà degli account dei membri associati. Puoi anche concedere agli abbonati l'autorizzazione per utilizzare i dati di proprietà degli account membri associati.

Per ulteriori informazioni, consulta Gestione di più account con AWS Organizations nella Guida per l'utente di Amazon Security Lake.

> **Autorizzazioni minime**
>
> Solo un amministratore dell'account di gestione Organizations può configurare un account membro come amministratore delegato per Amazon Security Lake nell'organizzazione.

Puoi specificare un account amministratore delegato utilizzando la console Amazon Security Lake, l'azione `CreateDatalakeDelegatedAdmin` API Amazon Security Lake o il comando `create-datalake-delegated-admin` CLI. In alternativa, puoi utilizzare la CLI `RegisterDelegatedAdministrator` o l'operazione SDK di Organizations. Per istruzioni sull'attivazione di un account amministratore delegato per Amazon Security Lake, consulta Designazione dell'amministratore delegato di Security Lake e aggiunta di account membro nella guida per l'utente di Amazon Security Lake.

AWS CLI, AWS API

Se desideri configurare un account amministratore delegato utilizzando la AWS CLI o uno degli SDK, puoi utilizzare AWS i seguenti comandi:

- AWS CLI:

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

- AWS SDK: richiama l'`RegisterDelegatedAdministrator`operazione Organizations e il numero ID dell'account membro e identifica l'account service principal `account.amazonaws.com` come parametri.

Disabilitazione di un amministratore delegato per Amazon Security Lake

Solo un amministratore dell'account di gestione Organizations o dell'account amministratore delegato di Amazon Security Lake può rimuovere un account amministratore delegato dall'organizzazione.

Puoi rimuovere l'account amministratore delegato utilizzando l'azione dell'`DeleteDatalakeDelegatedAdmin`API Amazon Security Lake, il comando `delete-datalake-delegated-admin` CLI o utilizzando l'operazione Organizations `DeregisterDelegatedAdministrator` CLI o SDK. Per rimuovere un amministratore delegato utilizzando Amazon Security Lake, consulta Rimozione dell'amministratore delegato di Amazon Security Lake nella guida per l'utente di Amazon Security Lake.

AWS Service Catalog e AWS Organizations

Service Catalog consente alle organizzazioni di creare e gestire cataloghi di servizi IT approvati per l'uso in AWS.

L'integrazione di Service Catalog con AWS Organizations semplifica la condivisione dei portfoli e la copia dei prodotti all'interno di un'organizzazione. Gli amministratori di Service Catalog possono fare riferimento a un'organizzazione esistente in AWS Organizations quando condividono un portfolio e possono condividerlo con qualsiasi unità organizzativa (OU) affidabile nella struttura ad albero dell'organizzazione. In questo modo viene meno la necessità di condividere ID di portafogli e per l'account che riceve di fare riferimento manualmente all'ID del portafoglio durante l'importazione. I portfoli condivisi tramite questo meccanismo sono elencati nell'account di condivisione nella visualizzazione di Imported Portfolio (Portfolio importato) in Service Catalog.

Per ulteriori informazioni, consulta Guida per l'amministratore di Catalogo di servizi.

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS Service Catalog con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

AWS Service Catalog non crea alcun ruolo collegati ai servizi come parte dell'abilitazione dell'accesso attendibile.

Principali del servizio utilizzati per concedere le autorizzazioni

Per abilitare l'accesso attendibile, è necessario specificare il principale di servizio seguente:

- `servicecatalog.amazonaws.com`

Abilitazione dell'accesso attendibile con Service Catalog

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

È possibile abilitare l'accesso sicuro utilizzando la console AWS Service Catalog o la console AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti AWS Service Catalog per abilitare l'integrazione con Organizations. Ciò consente a AWS Service Catalog di eseguire qualsiasi configurazione richiesta, ad esempio la creazione di risorse necessarie al servizio. Procedi con questi passaggi solo se non è possibile abilitare l'integrazione utilizzando gli strumenti forniti da AWS Service Catalog. Per ulteriori informazioni, consulta questa nota.
> Se abiliti l'accesso attendibile utilizzando la console o gli strumenti di AWS Service Catalog, non è necessario completare questi passaggi.

Abilitare l'accesso attendibile tramite la CLI di Service Catalog o AWS SDK

Chiama uno dei seguenti comandi o operazioni:

- AWS CLI: aws servicecatalog enable-aws-organizations-access
- SDK AWS: AWSServiceCatalog::EnableAWSOrganizationsAccess

È possibile abilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI o chiamando un'operazione API in un SDK AWS.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

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. Nella pagina Services (Servizi), trova la riga per AWS Service Catalog, scegli il nome del servizio, quindi scegli Enable trusted access (Abilita accesso attendibile).

3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS Service Catalog che ora può abilitare quel servizio utilizzando la console per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Puoi eseguire il comando seguente per abilitare AWS Service Catalog come servizio attendibile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: EnableAWSServiceAccess

Abilitazione dell'accesso attendibile con Service Catalog

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Se si disabilita l'accesso protetto utilizzando AWS Organizations durante l'utilizzo di Service Catalog, non si eliminano le condivisioni attuali, ma si impedisce di creare nuove condivisioni all'interno dell'azienda. Le condivisioni attuali non saranno sincronizzate con la struttura dell'organizzazione se quest'ultima cambia dopo questa operazione.

È possibile disabilitare l'accesso attendibile utilizzando la AWS Service Catalog o gli strumenti AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti AWS Service Catalog per disabilitare l'integrazione con Organizations. Ciò consente a AWS Service Catalog di eseguire qualsiasi operazione di pulizia necessaria, ad esempio l'eliminazione di risorse o di ruoli di accesso che non sono più necessari dal servizio. Procedi con questi passaggi solo se non è possibile disabilitare l'integrazione utilizzando gli strumenti forniti da AWS Service Catalog.
> Se disabiliti l'accesso attendibile utilizzando la console o gli strumenti di AWS Service Catalog, non è necessario completare questi passaggi.

Abilitare l'accesso attendibile tramite la CLI di Service Catalog o AWS SDK

Chiama uno dei seguenti comandi o operazioni:

- AWS CLI: aws servicecatalog disable-aws-organizations-access
- SDK AWS: DisableAWSOrganizationsAccess

È possibile disabilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI Organizations oppure chiamando un'operazione API Organizations in un SDK AWS.

AWS Management Console

Per disabilitare l'accesso al servizio attendibile utilizzando la console Organizations

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. Nella pagina Services (Servizi), individuare la riga per AWS Service Catalog e scegliere il nome del servizio.
3. Scegli Disable trusted access (Disabilita accesso attendibile).
4. Nella finestra di dialogo di conferma, inserisci **`disable`** nella casella, quindi scegli Disable trusted access (Disabilita accesso attendibile).

5. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS Service Catalog che ora può disabilitare quel servizio utilizzando la console o gli strumenti per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare AWS Service Catalog come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal servicecatalog.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- API AWS: DisableAWSServiceAccess

Service Quotas e AWS Organizations

Service Quotas è un servizio AWS che ti consente di visualizzare e gestire le quote da una posizione centrale. Le quote, anche definite limiti, costituiscono il valore massimo per le risorse, le operazioni e gli elementi nell'Account AWS.

Quando Service Quotas è associato ad AWS Organizations, è possibile creare un modello di richiesta quota per richiedere automaticamente un aumento della quota quando vengono creati gli account.

Per ulteriori informazioni su Service Quotas, consulta la Guida per l'utente di Service Quotas.

Utilizza le seguenti informazioni per facilitare l'integrazione di Service Quotas con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a Service Quotas di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra Service Quotas e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForServiceQuotas`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da Service Quotas concedono l'accesso ai seguenti principali del servizio:

- `servicequotas.amazonaws.com`

Abilitazione dell'accesso attendibile con Service Quotas

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Puoi abilitare l'accesso attendibile utilizzando solo Service Quotas.

Puoi abilitare l'accesso attendibile utilizzando la console Service Quotas, la AWS CLI o l'SDK:

- Per abilitare l'accesso attendibile tramite la console Service Quotas

  Accedi con il tuo account di gestione AWS Organizations e quindi configura il modello nella console Service Quotas. Per ulteriori informazioni, consulta l'argomento relativo all'utilizzo del modello di Quota servizio nella Guida per l'utente di Service Quotas.
- Per abilitare l'accesso attendibile tramite la AWS CLI o gli SDK di Service Quotas

  Chiama il seguente comando o operazione:

  - AWS CLI: aws service-quotas associate-service-quota-template
  - SDK AWS: AssociateServiceQuotaTemplate

AWS IAM Identity Center e AWS Organizations

AWS IAM Identity Center fornisce l'accesso Single Sign-On per tutte le applicazioni cloud e tutti gli Account AWS. Si connette con Microsoft Active Directory tramite AWS Directory Service per consentire agli utenti nella directory di accedere a un portale di accesso di AWS personalizzato utilizzando i nomi utente e le password esistenti di Active Directory. Dal portale di accesso AWS, gli utenti hanno accesso alle applicazioni cloud e a tutti gli Account AWS per i quali dispongono delle autorizzazioni.

Per ulteriori informazioni su IAM Identity Center, consulta la Guida per l'utente AWS IAM Identity Center.

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS IAM Identity Center con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a IAM Identity Center di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra IAM Identity Center e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForSSO`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da IAM Identity Center concedono l'accesso ai seguenti principali del servizio:

- `sso.amazonaws.com`

Abilitazione dell'accesso attendibile con IAM Identity Center

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

È possibile abilitare l'accesso sicuro utilizzando la console AWS IAM Identity Center o la console AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti AWS IAM Identity Center per abilitare l'integrazione con Organizations. Ciò consente a AWS IAM Identity Center di eseguire qualsiasi configurazione richiesta, ad esempio la creazione di risorse necessarie al servizio. Procedi con questi passaggi solo se non è possibile abilitare l'integrazione utilizzando gli strumenti forniti da AWS IAM Identity Center. Per ulteriori informazioni, consulta questa nota.
> Se abiliti l'accesso attendibile utilizzando la console o gli strumenti di AWS IAM Identity Center, non è necessario completare questi passaggi.

IAM Identity Center richiede l'accesso attendibile con AWS Organizations per funzionare. L'accesso sicuro viene abilitato quando imposti IAM Identity Center. Per ulteriori informazioni, consulta Nozioni di base: Passaggio 1: abilitare AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center.

È possibile abilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI o chiamando un'operazione API in un SDK AWS.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

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. Nella pagina Services (Servizi), trova la riga per AWS IAM Identity Center, scegli il nome del servizio, quindi scegli Enable trusted access (Abilita accesso attendibile).
3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS IAM Identity Center che ora può abilitare quel servizio utilizzando la console per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Puoi eseguire il comando seguente per abilitare AWS IAM Identity Center come servizio attendibile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: EnableAWSServiceAccess

Disabilitazione dell'accesso attendibile con IAM Identity Center

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

IAM Identity Center richiede l'accesso attendibile con AWS Organizations per funzionare. Se disabiliti l'accesso sicuro utilizzando AWS Organizations durante l'utilizzo di IAM Identity Center, smette di funzionare in quanto non può accedere all'organizzazione. Gli utenti non possono utilizzare IAM Identity Center per accedere gli account. Tutti i ruoli che IAM Identity Center crea rimangono, ma il servizio IAM Identity Center non può accedervi. I ruoli collegati ai servizi di IAM Identity Center rimangono. Se abiliti nuovamente l'accesso sicuro, IAM Identity Center continua a funzionare come prima, senza la necessità di riconfigurare il servizio.

Se rimuovi un account dalla tua organizzazione, IAM Identity Center pulisce automaticamente i metadati e le risorse, ad esempio i ruoli collegati ai servizi. Un account autonomo che viene rimosso da un'organizzazione non funziona più con IAM Identity Center.

Puoi disabilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

È possibile disabilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI Organizations oppure chiamando un'operazione API Organizations in un SDK AWS.

AWS Management Console

Per disabilitare l'accesso al servizio attendibile utilizzando la console Organizations

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. Nella pagina Services (Servizi), individuare la riga per AWS IAM Identity Center e scegliere il nome del servizio.
3. Scegli Disable trusted access (Disabilita accesso attendibile).
4. Nella finestra di dialogo di conferma, inserisci **`disable`** nella casella, quindi scegli Disable trusted access (Disabilita accesso attendibile).
5. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS IAM Identity Center che ora può disabilitare quel servizio utilizzando la console o gli strumenti per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare AWS IAM Identity Center come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal sso.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: DisableAWSServiceAccess

Abilitazione di un account amministratore delegato per IAM Identity Center

Quando si designa un account membro come amministratore delegato per l'organizzazione, gli utenti e i ruoli di tale account possono eseguire operazioni amministrative per IAM Identity

Center che altrimenti potrebbero essere eseguite solo da utenti o ruoli nell'account di gestione dell'organizzazione. Ciò consente di separare la gestione dell'organizzazione dalla gestione di IAM Identity Center.

> **Autorizzazioni minime**
>
> Solo un utente o un ruolo nell'account di gestione di Organizations può configurare un account membro come amministratore delegato per il Centro identità IAM nell'organizzazione.

Per le istruzioni su come abilitare un account amministratore delegato per IAM Identity Center, consulta Amministrazione delegata nella Guida per l'utente di AWS IAM Identity Center.

AWS Systems Manager e AWS Organizations

AWS Systems Manager è una raccolta di funzionalità che consentono visibilità e controllo delle risorse AWS. Le seguenti funzionalità di Systems Manager funzionano con Organizations di Account AWS in tutta l'organizzazione:

- Systems Manager Explorer è un pannello di controllo delle operazioni personalizzabile che riporta informazioni sulle risorse AWS. Puoi sincronizzare i dati delle operazioni tra tutti gli Account AWS dell'organizzazione utilizzando Organizations e Systems Manager Explorer. Per ulteriori informazioni, consulta Systems Manager Explorer nella Guida per l'utente di AWS Systems Manager.
- Systems Manager Change Manager è un framework di gestione delle modifiche aziendali per la richiesta, l'approvazione, l'implementazione e la creazione di report sulle modifiche operative alla configurazione e all'infrastruttura delle applicazioni. Per ulteriori informazioni, consulta AWS Systems Manager Change Manager nella Guida per l'utente di AWS Systems Manager.
- Il Systems Manager OpsCenter fornisce una posizione centrale dove i tecnici operativi e i professionisti dell'IT possono visualizzare, esaminare e risolvere elementi operativi (OpsItems) relativi alle risorse AWS. Quando si utilizza OpsCenter con Organizations, si supporta l'utilizzo di OPSItems da un account di gestione (un account di gestione di Organizations o un account amministratore delegato di Systems Manager) e da un altro account durante una singola sessione. Una volta configurato, gli utenti possono eseguire i seguenti tipi di azioni:
  - Crea, visualizza e aggiorna OPSItems in un altro account.
  - Visualizza informazioni dettagliate sulle risorse AWS specificate in OpsItems in un altro account.

- Avvia i Runbook di automazione di Systems Manager per risolvere i problemi relativi alle risorse di AWS di un altro account.

Per ulteriori informazioni, consulta AWS Systems Manager OpsCenter nella AWS Systems Manager Guida per l'utente.

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS Systems Manager con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a Systems Manager di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra Systems Manager e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForAmazonSSM_AccountDiscovery`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da Systems Manager concedono l'accesso ai seguenti principali del servizio:

- `ssm.amazonaws.com`

Abilitazione dell'accesso attendibile con Systems Manager

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Puoi abilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

È possibile abilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI o chiamando un'operazione API in un SDK AWS.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

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. Nella pagina Services (Servizi), trova la riga per AWS Systems Manager, scegli il nome del servizio, quindi scegli Enable trusted access (Abilita accesso attendibile).
3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS Systems Manager che ora può abilitare quel servizio utilizzando la console per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Puoi eseguire il comando seguente per abilitare AWS Systems Manager come servizio attendibile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: EnableAWSServiceAccess

Disabilitazione dell'accesso attendibile con Systems Manager

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Systems Manager richiede l'accesso attendibile con AWS Organizations per sincronizzare i dati delle operazioni tra gli Account AWS nell'organizzazione. Se disabiliti l'accesso attendibile, Systems Manager non riesce a sincronizzare i dati delle operazioni e segnala un errore.

Puoi disabilitare l'accesso attendibile utilizzando solo gli strumenti di Organizations.

È possibile disabilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI Organizations oppure chiamando un'operazione API Organizations in un SDK AWS.

AWS Management Console

Per disabilitare l'accesso al servizio attendibile utilizzando la console Organizations

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. Nella pagina Services (Servizi), individuare la riga per AWS Systems Manager e scegliere il nome del servizio.
3. Scegli Disable trusted access (Disabilita accesso attendibile).
4. Nella finestra di dialogo di conferma, inserisci **`disable`** nella casella, quindi scegli Disable trusted access (Disabilita accesso attendibile).
5. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS Systems Manager che ora può disabilitare quel servizio utilizzando la console o gli strumenti per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare AWS Systems Manager come servizio attendibile con Organizations.

```
$ aws organizations disable-aws-service-access \
```

```
    --service-principal ssm.amazonaws.com
```

Questo comando non produce alcun output se ha esito positivo.

- API AWS: DisableAWSServiceAccess

Abilitazione di un account di amministratore delegato per Systems Manager

Quando si designa un account membro come amministratore delegato per l'organizzazione, gli utenti e i ruoli di tale account possono eseguire operazioni amministrative per Systems Manager che altrimenti possono essere eseguiti solo da utenti o ruoli nell'account di gestione dell'organizzazione. Ciò consente di separare la gestione dell'organizzazione dalla gestione di Systems Manager.

Se utilizzi Change Manager in un'organizzazione, utilizzi un account di amministratore delegato. Questo è l'Account AWS che è stato designato come account per la gestione di modelli di modifica, richieste di modifica, runbook di modifica e flussi di lavoro di approvazione in Change Manager. L'account delegato gestisce le attività di modifica all'interno dell'organizzazione. Quando imposti l'organizzazione per l'utilizzo con Change Manager, è necessario specificare quale dei tuoi account svolge questo ruolo. Non deve essere l'account di gestione dell'organizzazione. L'account di amministratore delegato non è necessario se si utilizza Change Manager con un solo account.

Per designare un account membro come amministratore delegato, consulta i seguenti argomenti nella Guida per l'utente di AWS Systems Manager:

- Per Explorer e OpsCenter, vedere Configurazione di un amministratore delegato.
- Per Change Manager, consulta Impostazione di un'organizzazione e di un account delegato per Change Manager.

Policy di tag e AWS Organizations

Le policy di tag sono un tipo di policy in AWS Organizations che può semplificare la standardizzazione dei tag tra le risorse degli account dell'organizzazione. Per ulteriori informazioni sulle policy di tag, consulta Policy di tag.

Utilizza le seguenti informazioni per facilitare l'integrazione delle policy di tag con AWS Organizations.

Principali del servizio utilizzati dai ruoli collegati ai servizi

Organizations interagisce con i tag associati alle risorse utilizzando il principale del servizio seguente.

- `tagpolicies.tag.amazonaws.com`

Abilitazione dell'accesso attendibile per le policy di tag

È possibile abilitare l'accesso attendibile abilitando le policy di tag nell'organizzazione oppure utilizzando la console AWS Organizations.

> **Important**
>
> Ti consigliamo vivamente di abilitare l'accesso attendibile abilitando le policy di tag. Ciò consente a Organizations di eseguire le attività di configurazione richieste.

È possibile abilitare l'accesso attendibile per le policy di tag abilitando il tipo di policy di tag nella console AWS Organizations. Per ulteriori informazioni, consultare Abilitazione di un tipo di policy.

È possibile abilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI o chiamando un'operazione API in un SDK AWS.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

1. Accedere 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. Nella pagina Services (Servizi), trova la riga per tag policies (policy di tag), scegli il nome del servizio, quindi scegli Enable trusted access (Abilita accesso attendibile).
3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore delle policy di tag che ora può abilitare quel servizio utilizzando la console per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  È possibile eseguire il comando seguente per abilitare le policy di tag come servizio attendibile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.

- API AWS: EnableAWSServiceAccess

Disabilitazione dell'accesso attendibile con le policy di tag

È possibile disabilitare l'accesso attendibile per le policy di tag disabilitando il tipo di policy di tag nella console AWS Organizations. Per ulteriori informazioni, consultare Disabilitazione di un tipo di policy.

AWS Trusted Advisor e AWS Organizations

AWS Trusted Advisor analizza l'ambiente AWS e fornisce suggerimenti nel caso in cui vi siano opportunità di risparmiare denaro, migliorare la disponibilità e le prestazioni del sistema o colmare le lacune legate alla sicurezza. Se integrato con Organizations, è possibile ricevere i risultati dei controlli Trusted Advisor di tutti gli account dell'organizzazione e scaricare i report per visualizzare i riepiloghi dei controlli e le risorse interessate.

Per ulteriori informazioni, consulta Visualizzazione organizzativa per AWS Trusted Advisor nella Guida per l'utente di AWS Support.

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS Trusted Advisor con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a Trusted Advisor di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra Trusted Advisor e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForTrustedAdvisorReporting`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da Trusted Advisor concedono l'accesso ai seguenti principali del servizio:

- `reporting.trustedadvisor.amazonaws.com`

Abilitazione dell'accesso attendibile con Trusted Advisor

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

È possibile abilitare l'accesso attendibile utilizzando solo AWS Trusted Advisor.

Per abilitare l'accesso attendibile tramite la console Trusted Advisor

Consulta Abilitazione della visualizzazione organizzativa nella Guida per l'utente di AWS Support.

Disabilitazione dell'accesso attendibile con Trusted Advisor

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Dopo avere disabilitato questa funzionalità, Trusted Advisor interrompe la registrazione delle informazioni di controllo per tutti gli altri account dell'organizzazione. Non è possibile visualizzare o scaricare report esistenti o creare nuovi report.

È possibile disabilitare l'accesso attendibile utilizzando la AWS Trusted Advisor o gli strumenti AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti AWS Trusted Advisor per disabilitare l'integrazione con Organizations. Ciò consente a AWS Trusted Advisor di eseguire qualsiasi operazione di pulizia necessaria, ad esempio l'eliminazione di risorse o di ruoli di accesso che non sono più necessari dal servizio. Procedi con questi passaggi solo se non è possibile disabilitare l'integrazione utilizzando gli strumenti forniti da AWS Trusted Advisor.
> Se disabiliti l'accesso attendibile utilizzando la console o gli strumenti di AWS Trusted Advisor, non è necessario completare questi passaggi.

Per abilitare l'accesso attendibile tramite la console Trusted Advisor

Consulta Disabilitazione della visualizzazione organizzativa nella Guida per l'utente di AWS Support.

Puoi disabilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare AWS Trusted Advisor come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal reporting.trustedadvisor.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- API AWS: DisableAWSServiceAccess

Abilitazione di un account amministratore delegato per Trusted Advisor

Quando si designa un account membro come amministratore delegato per l'organizzazione, gli utenti e i ruoli dell'account designato possono gestire i metadati dell'Account AWS per altri account membri dell'organizzazione. Se non si abilita un account amministratore delegato, queste attività possono essere eseguite solo dall'account di gestione dell'organizzazione. Ciò consente di separare la gestione dell'organizzazione dalla gestione dei dettagli dell'account.

> **Autorizzazioni minime**
>
> Solo un utente o un ruolo nell'account di gestione di Organizations può configurare un account membro come amministratore delegato per Trusted Advisor nell'organizzazione

Per le istruzioni su come abilitare un account amministratore delegato per Trusted Advisor, consulta Register delegated administrators (Registrare amministratori delegati) nella Guida per l'utente di AWS Support.

AWS CLI, AWS API

Se desideri configurare un account di amministratore delegato utilizzando AWS CLI o uno degli SDK AWS, puoi utilizzare anche i seguenti comandi:

- AWS CLI:

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

- SDK AWS: richiama l'operazione `RegisterDelegatedAdministrator` di Organizations e il numero ID dell'account membro e identifica il principale del servizio dell'account `account.amazonaws.com` come parametri.

Disattivazione di un amministratore delegato per Trusted Advisor

È possibile rimuovere l'amministratore delegato utilizzando la console Trusted Advisor oppure utilizzando CLI `DeregisterDelegatedAdministrator` o l'operazione SDK di Organizations. Per informazioni su come disattivare account amministratore delegato per Trusted Advisor utilizzando

la console Trusted Advisor, consulta Deregister delegated administrators (Annullare la registrazione degli amministratori delegati) nella Guida per l'utente di AWS Support.

AWS Well-Architected Tool e AWS Organizations

Lo AWS Well-Architected Tool aiuta a documentare lo stato dei carichi di lavoro e a confrontarli con quelli più recenti best practice architettoniche di AWS.

L'utilizzo del AWS Well-Architected Tool con Organizations permette ai clienti dello AWS Well-Architected Tool e di Organizations di semplificare il processo di condivisione delle risorse dello AWS Well-Architected Tool con altri membri della loro organizzazione.

Per ulteriori informazioni, consulta Sharing your AWS Well-Architected Tool resources (Condivisione delle risorse dello) nella AWS Well-Architected Tool User Guide (Guida dell'utente dello).

Utilizza le seguenti informazioni per facilitare l'integrazione di AWS Well-Architected Tool con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a AWS WA Tool di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra AWS WA Tool e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForWellArchitected`

La policy del ruolo di servizio è `AWSWellArchitectedOrganizationsServiceRolePolicy`

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da AWS WA Tool concedono l'accesso ai seguenti principali del servizio:

- `wellarchitected.amazonaws.com`

Abilitazione dell'accesso attendibile con AWS WA Tool

Consente l'aggiornamento dello AWS WA Tool per riflettere le modifiche gerarchiche in un'organizzazione.

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

È possibile abilitare l'accesso sicuro utilizzando la console AWS Well-Architected Tool o la console AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti AWS Well-Architected Tool per abilitare l'integrazione con Organizations. Ciò consente a AWS Well-Architected Tool di eseguire qualsiasi configurazione richiesta, ad esempio la creazione di risorse necessarie al servizio. Procedi con questi passaggi solo se non è possibile abilitare l'integrazione utilizzando gli strumenti forniti da AWS Well-Architected Tool. Per ulteriori informazioni, consulta questa nota.
> Se abiliti l'accesso attendibile utilizzando la console o gli strumenti di AWS Well-Architected Tool, non è necessario completare questi passaggi.

Per abilitare l'accesso attendibile tramite la console AWS WA Tool

Consulta Sharing your AWS Well-Architected Tool resources (Condivisione delle risorse dello), nella AWS Well-Architected Tool User Guide (Guida dell'utente dello).

È possibile abilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI o chiamando un'operazione API in un SDK AWS.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

1. Accedere 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. Nella pagina Services (Servizi), trova la riga per AWS Well-Architected Tool, scegli il nome del servizio, quindi scegli Enable trusted access (Abilita accesso attendibile).

3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di AWS Well-Architected Tool che ora può abilitare quel servizio utilizzando la console per il funzionamento con AWS Organizations.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Puoi eseguire il comando seguente per abilitare AWS Well-Architected Tool come servizio attendibile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: EnableAWSServiceAccess

Disabilitazione dell'accesso attendibile con AWS WA Tool

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

È possibile disabilitare l'accesso attendibile utilizzando la AWS Well-Architected Tool o gli strumenti AWS Organizations.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti AWS Well-Architected Tool per disabilitare l'integrazione con Organizations. Ciò consente a AWS Well-Architected Tool di eseguire qualsiasi operazione di pulizia necessaria, ad esempio

l'eliminazione di risorse o di ruoli di accesso che non sono più necessari dal servizio. Procedi con questi passaggi solo se non è possibile disabilitare l'integrazione utilizzando gli strumenti forniti da AWS Well-Architected Tool.
Se disabiliti l'accesso attendibile utilizzando la console o gli strumenti di AWS Well-Architected Tool, non è necessario completare questi passaggi.

Per abilitare l'accesso attendibile tramite la console AWS WA Tool

Consulta Sharing your AWS Well-Architected Tool resources (Condivisione delle risorse dello), nella AWS Well-Architected Tool User Guide (Guida dell'utente dello).

Puoi disabilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare AWS Well-Architected Tool come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal wellarchitected.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- API AWS: DisableAWSServiceAccess

Amazon VPC IP Address Manager (IPAM) e AWS Organizations

Amazon VPC IP Address Manager (IPAM) è una caratteristica del VPC che semplifica la pianificazione, il tracciamento e il monitoraggio degli indirizzi IP per i carichi di lavoro AWS.

Usare AWS Organizations permette di monitorare l'utilizzo degli indirizzi IP in tutta l'organizzazione e condividi i pool di indirizzi IP tra gli account membri.

Per ulteriori informazioni, consulta Integrazione di IPAM con AWS Organizations nella Guida per l'utente IPAM di Amazon VPC.

Utilizza le seguenti informazioni per facilitare l'integrazione di IP Address Manager (IPAM) di Amazon VPC con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato al servizio viene creato automaticamente nell'account di gestione dell'organizzazione e in ciascun account membro quando si integra IPAM con AWS Organizations utilizzando la console IPAM o utilizzando la API di IPAM`EnableIpamOrganizationAdminAccount`.

- `AWSServiceRoleForIPAM`

Per ulteriori informazioni, consulta Ruoli collegati ai servizi per IPAM nella Guida per l'utente IPAM di Amazon VPC.

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da IPAM concedono l'accesso ai seguenti principali del servizio:

- `ipam.amazonaws.com`

Abilitare l'accesso sicuro con IPAM

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

> **Note**
>
> Quando si designa un amministratore delegato per IPAM, viene abilitato automaticamente l'accesso attendibile per IPAM nell'organizzazione.
> IPAM richiede l'accesso attendibile a AWS Organizations prima di designare un account membro come amministratore delegato per questo servizio per l'organizzazione.

Puoi abilitare l'accesso attendibile utilizzando solo gli strumenti di Amazon VPC IP Address Manager (IPAM).

Se si integra IPAM con AWS Organizations utilizzando la console IPAM o l'API di IPAM`EnableIpamOrganizationAdminAccount`, viene concesso automaticamente l'accesso attendibile a IPAM. La concessione di un accesso attendibile crea il ruolo collegato ai servizi `AWSServiceRoleForIPAM` nell'account di gestione e in tutti gli account membri dell'organizzazione. IPAM utilizza il ruolo collegato al servizio per monitorare i CIDR associati alle risorse di rete EC2 nell'organizzazione e per archiviare le metriche relative a IPAM in Amazon CloudWatch. Per ulteriori informazioni, consulta Ruoli collegati ai servizi per IPAM nella Guida per l'utente IPAM di Amazon VPC.

Per istruzioni su come abilitare l'accesso attendibile, consulta Integrazione di IPAM con AWS Organizations nella Guida per l'utente IPAM di Amazon VPC.

> **Note**
>
> Non è possibile abilitare l'accesso attendibile con IPAM utilizzando la console di AWS Organizations o con l'API `EnableAWSServiceAccess`.

Disabilitare l'accesso sicuro con IPAM

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Solo un amministratore nell'account di gestione di AWS Organizations può disabilitare l'accesso attendibile utilizzando l'API di AWS Organizations `disable-aws-service-access`.

Per informazioni sulla disabilitazione delle autorizzazioni dell'account IPAM e sull'eliminazione del ruolo collegato ai servizi, consulta Ruoli collegati ai servizi per IPAM nella Guida per l'utente IPAM di Amazon VPC.

Puoi disabilitare l'accesso attendibile eseguendo il comando AWS CLI di Organizations oppure chiamando un'operazione API di Organizations in un SDK AWS.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi AWS CLI oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Puoi eseguire il comando seguente per disabilitare IP Address Manager (IPAM) di Amazon VPC come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ipam.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- API AWS: DisableAWSServiceAccess

Abilitazione di un account amministratore delegato per IPAM

L'account amministratore delegato per IPAM è responsabile della creazione dei pool di indirizzi IPAM e IP, della gestione e del monitoraggio dell'utilizzo degli indirizzi IP nell'organizzazione e della condivisione dei pool di indirizzi IP tra gli account membri. Per ulteriori informazioni, consulta Integrazione di IPAM con AWS Organizations nella Guida per l'utente IPAM di Amazon VPC.

Solo un amministratore nell'account di gestione dell'organizzazione può configurare un amministratore delegato per IPAM.

È possibile specificare un account amministratore delegato dalla console IPAM o utilizzando l'API di `enable-ipam-organization-admin-account`. Per ulteriori informazioni, consultare enable-ipam-organization-admin-account in Riferimento ai comandi di AWS AWS CLI.

> **Autorizzazioni minime**
>
> Solo un utente o un ruolo nell'account di gestione di Organizations può configurare un account membro come amministratore delegato per IPAM nell'organizzazione

Per configurare un amministratore delegato utilizzando la console IPAM, consultare Integrazione di IPAM con AWS Organizations nella Guida per l'utente di IPAM per Amazon VPC.

Disattivazione di un amministratore delegato per IPAM

Solo un amministratore nell'account di gestione dell'organizzazione può configurare un amministratore delegato per IPAM.

Per rimuovere un amministratore delegato utilizzando AWS AWS CLI, consultare disable-ipam-organization-admin-account in Riferimento ai comandi di AWS AWS CLI.

Per disabilitare un account IPAM dell'amministratore delegato tramite la console IPAM, consultare Integrazione di IPAM con AWS Organizations nella Guida per l'utente di IPAM per Amazon VPC.

Sistema di analisi della reperibilità Amazon VPC e AWS Organizations

Reachability Analyzer è uno strumento di analisi della configurazione che consente di eseguire test di connettività tra una risorsa di origine e una risorsa di destinazione nei cloud privati virtuali (VPC).

L'utilizzo di AWS Organizations con Reachability Analyzer consente di tracciare i percorsi tra gli account delle organizzazioni.

Per ulteriori informazioni, consulta Analisi tra account per Reachability Analyzer nella Guida per l'utente di Reachability Analyzer.

Utilizza le seguenti informazioni per facilitare l'integrazione di Reachability Analyzer con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Il seguente ruolo collegato ai servizi viene creato automaticamente nell'account di gestione dell'organizzazione quando abiliti l'accesso attendibile. Tale ruolo consente a Reachability Analyzer di eseguire le operazioni supportate all'interno degli account dell'organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra Reachability Analyzer e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForReachabilityAnalyzer`

Per ulteriori informazioni, consulta Analisi tra account per Reachability Analyzer nella Guida per l'utente di Reachability Analyzer.

Principali del servizio utilizzati dai ruoli collegati ai servizi

Il ruolo collegato ai servizi nella sezione precedente può essere assunto solo dai principali del servizio autorizzati dalle relazioni di attendibilità definite per il ruolo. I ruoli collegati ai servizi utilizzati da Reachability Analyzer concedono l'accesso ai seguenti principali del servizio:

- `reachabilityanalyzer.networkinsights.amazonaws.com`

Abilitazione dell'accesso attendibile con Reachability Analyzer

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Quando designi un amministratore delegato per Reachability Analyzer, viene abilitato automaticamente l'accesso attendibile per Reachability Analyzer nell'organizzazione.

Reachability Analyzer richiede l'accesso attendibile a AWS Organizations prima di designare un account membro come amministratore delegato per questo servizio per l'organizzazione.

Important

- Puoi abilitare l'accesso attendibile utilizzando la console Reachability Analyzer o la console Organizations. Consigliamo vivamente di utilizzare, tuttavia, la console Reachability Analyzer o l'API `EnableMultiAccountAnalysisForAwsOrganization` per abilitare l'integrazione con Organizations. Ciò consente a Reachability Analyzer di eseguire qualsiasi configurazione richiesta, ad esempio la creazione di risorse necessarie al servizio.
- La concessione di un accesso attendibile crea il ruolo collegato ai servizi `AWSServiceRoleForReachabilityAnalyzer` nell'account di gestione e in tutti gli account membri dell'organizzazione. Reachability Analyzer utilizza il ruolo collegato ai servizi per consentire alla gestione e all'amministratore delegato di eseguire analisi di connettività tra qualsiasi risorsa dell'organizzazione. Reachability Analyzer è in grado di scattare istantanee (snapshot) degli elementi di rete degli account di un'organizzazione per rispondere alle domande di connettività.
- Per ulteriori informazioni e per le istruzioni su come abilitare l'accesso attendibile tramite Reachability Analyzer, consulta Analisi tra account per Reachability Analyzer nella Guida per l'utente di Reachability Analyzer.

È possibile abilitare l'accesso attendibile utilizzando la console AWS Organizations, eseguendo un comando AWS CLI o chiamando un'operazione API in un SDK AWS.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

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. Nella pagina Servizi, trova la riga per il sistema di analisi della reperibilità VPC, scegli il nome del servizio, quindi seleziona Abilita un accesso attendibile.
3. Nella finestra di dialogo di conferma, abilita Show the option to enable trusted access (Mostra l'opzione per abilitare l'accesso attendibile), inserisci **`enable`** nella casella, quindi scegli Enable trusted access (Abilita accesso attendibile).
4. Se sei l'amministratore solo di AWS Organizations, comunica all'amministratore di Reachability Analyzer che ora può abilitare quel servizio utilizzando la console in modo che funzioni con AWS Organizations.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Puoi utilizzare i seguenti comandi della AWS CLI oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Puoi emettere il comando seguente per abilitare Reachability Analyzer come servizio attendibile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.

- API AWS: EnableAWSServiceAccess

Disabilitazione dell'accesso attendibile con Reachability Analyzer

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Puoi disabilitare l'accesso attendibile utilizzando la console Reachability Analyzer (scelta consigliata) o la console Organizations. Per disabilitare l'accesso attendibile utilizzando la console Reachability Analyzer, consulta Analisi tra account per Reachability Analyzer nella Guida per l'utente di Reachability Analyzer.

Abilitazione dell'account di un amministratore delegato per Reachability Analyzer

L'account amministratore delegato è in grado di eseguire analisi di connettività su qualsiasi risorsa dell'organizzazione. Per ulteriori informazioni, consulta Integrazione di Reachability Analyzer conAWS Organizations nella Guida per l'utente di Reachability Analyzer.

Solo un amministratore nell'account di gestione dell'organizzazione può configurare un amministratore delegato per Reachability Analyzer.

Puoi specificare un account amministratore delegato dalla console Reachability Analyzer o utilizzando l'API di `RegisterDelegatedAdministrator`. Per ulteriori informazioni, consulta RegisterDelegatedAdministrator in Riferimento ai comandi di Organizations.

> **Autorizzazioni minime**
>
> Solo un utente o un ruolo nell'account di gestione di Organizations può configurare un account membro come amministratore delegato per il Sistema di analisi della reperibilità nell'organizzazione

Per configurare un amministratore delegato utilizzando la console Reachability Analyzer, consulta Integrazione di Reachability Analyzer conAWS Organizations nella Guida per l'utente di Reachability Analyzer.

Disabilitazione di un amministratore delegato per Reachability Analyzer

Solo un amministratore nell'account di gestione dell'organizzazione può configurare un amministratore delegato per Reachability Analyzer.

Puoi rimuovere l'amministratore delegato utilizzando la console Reachability Analyzer o l'API oppure utilizzando la CLI `DeregisterDelegatedAdministrator` o l'operazione SDK di Organizations.

Per disabilitare l'account Reachability Analyzer dell'amministratore delegato, consulta Analisi tra account per Reachability Analyzer nella Guida per l'utente di Reachability Analyzer.

Amministratore delegato per i servizi AWS che funzionano con Organizations

Consigliamo di utilizzare l'account di gestione AWS Organizations e i relativi utenti e ruoli solo per le attività che devono essere eseguite da tale account. Consigliamo anche di archiviare tutte le risorse AWS in altri account membro nell'organizzazione ed escluderle dall'account di gestione. Questo perché le funzionalità di sicurezza come le policy di controllo dei servizi (SCP) di Organizations non limitano gli utenti o i ruoli nell'account di gestione. Inoltre, la separazione delle risorse dall'account di gestione può aiutare a comprendere gli addebiti sulle fatture.

Molti servizi AWS che si integrano con Organizations consentono di ridurre l'utilizzo dell'account di gestione. Questi servizi consentono di registrare uno o più account membro come amministratori in grado di gestire tutti gli account dell'organizzazione utilizzati nel servizio. Questi account sono denominati amministratori delegati per quel servizio specifico. Registrando un account membro come amministratore delegato per un servizio AWS, consenti a tale account di disporre di autorizzazioni amministrative per quel servizio, nonché delle autorizzazioni per le operazioni di sola lettura per Organizations.

Prima di registrare un account come amministratore delegato per un servizio:

- Verifica che il servizio supporti gli amministratori delegati. Consulta la tabella in AWS servizi che puoi utilizzare con AWS Organizations per scoprire quali servizi supportano gli amministratori delegati.
- Abilita l'accesso attendibile per tale servizio.

> **Note**
>
> Per informazioni su come abilitare un amministratore delegato per un servizio, fai riferimento alla tabella in AWS servizi che puoi utilizzare con AWS Organizations e seleziona il link Ulteriori informazioni nella colonna Supporta amministratore delegato per tale servizio.

Autorizzazioni concesse agli account amministratore delegato

Ogni account amministratore delegato specifico del servizio dispone delle autorizzazioni concesse da tale servizio. Per ulteriori informazioni, consulta la tabella in AWS servizi che puoi utilizzare con AWS Organizations e seleziona il link Ulteriori informazioni nella colonna Supporta Amministratore delegatoper tale servizio.

Un account amministratore delegato dispone anche delle seguenti autorizzazioni di sola lettura:

- `DescribeAccount`
- `DescribeCreateAccountStatus`
- `DescribeEffectivePolicy`
- `DescribeHandshake`
- `DescribeOrganization`
- `DescribeOrganizationalUnit`
- `DescribePolicy`
- `DescribeResourcePolicy`
- `ListAccounts`
- `ListAccountsForParent`
- `ListAWSServiceAccessForOrganization`
- `ListChildren`
- `ListCreateAccountStatus`
- `ListDelegatedAdministrators`
- `ListDelegatedServicesForAccount`
- `ListHandshakesForAccount`
- `ListHandshakesForOrganization`
- `ListOrganizationalUnitsForParent`
- `ListParents`
- `ListPolicies`
- `ListPoliciesForTarget`
- `ListRoots`
- `ListTagsForResource`

- `ListTargetsForPolicy`

Queste autorizzazioni consentono di visualizzare, ma non modificare, i seguenti elementi della console:

- Struttura dell'organizzazione, tutti gli account e le unità organizzative e le policy organizzative
- Appartenenze
- Tutti gli account e le unità organizzative.
- Policy organizzative

Sicurezza in AWS Organizations

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

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

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per ulteriori informazioni sui programmi di conformità applicabili AWS Organizations, consulta AWS Services in Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione consente di comprendere come applicare il modello di responsabilità condivisa quando si usa Organizations. I seguenti argomenti illustrano come configurare Organizations per soddisfare gli obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le risorse della tua Organizations.

Argomenti

AWS PrivateLink per AWS Organizations

Con AWS PrivateLink for AWS Organizations, puoi accedere al AWS Organizations servizio dall'interno del Virtual Private Cloud (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 sui VPC, consulta la Guida per l'utente di Amazon VPC.

Per connettere il tuo Amazon VPC AWS Organizations, devi prima definire un endpoint VPC di interfaccia (endpoint di interfaccia). Gli endpoint di interfaccia sono rappresentati da una o più interfacce di rete elastiche (ENI) a cui vengono assegnati indirizzi IP privati dalle sottoreti nel VPC. Le richieste dal tuo VPC agli endpoint AWS Organizations over interface rimangono sulla rete Amazon.

Per informazioni generali sugli endpoint di interfaccia, consulta Accedere a un AWS servizio utilizzando un endpoint VPC di interfaccia nella Amazon VPC User Guide.

Argomenti

- Limitazioni e restrizioni di AWS PrivateLinkAWS Organizations
- Creazione di un endpoint VPC
- Creazione di una policy di endpoint VPC per l' AWS Organizations

Limitazioni e restrizioni di AWS PrivateLinkAWS Organizations

Le limitazioni VPC si applicano a for. AWS PrivateLink AWS Organizations Per ulteriori informazioni, consulta Accedere a un AWS servizio utilizzando un endpoint e AWS PrivateLink quote VPC di interfaccia nella Amazon VPC User Guide. Inoltre, si applicano le limitazioni seguenti:

- Disponibile solo nella regione `us-east-1`
- Non supporta Transport Layer Security (TLS) 1.1

Creazione di un endpoint VPC

Puoi creare un AWS Organizations endpoint nel tuo VPC utilizzando la console Amazon VPC, AWS Command Line Interface il () o.AWS CLI AWS CloudFormation

Per informazioni sulla creazione e configurazione di un endpoint utilizzando la console Amazon VPC o la AWS CLI, consulta Create a VPC endpoint nella Amazon VPC User Guide. Per informazioni sulla creazione e configurazione di un endpoint utilizzando AWS CloudFormation, consulta la risorsa AWS: :EC2: :VPCEndpoint nella Guida per l'utente.AWS CloudFormation

Quando crei un AWS Organizations endpoint, usa quanto segue come nome del servizio:

```
com.amazonaws.us-east-1.organizations
```

Se per l'accesso sono necessari moduli crittografici convalidati FIPS 140-2 AWS, utilizzate il seguente nome di servizio FIPS: AWS Organizations

```
com.amazonaws.us-east-1.organizations-fips
```

Creazione di una policy di endpoint VPC per l' AWS Organizations

Puoi allegare una policy per gli endpoint al tuo endpoint VPC che controlla l'accesso a Organizations. La policy specifica le informazioni riportate di seguito:

- Il principale che può eseguire operazioni.
- Le azioni che possono essere eseguite.
- Le risorse sui cui si possono eseguire azioni.

Per ulteriori informazioni, consulta Controlla l'accesso agli endpoint VPC utilizzando le policy degli endpoint nella Amazon VPC User Guide.

Esempio: policy di endpoint VPC per le operazioni dell' AWS Organizations

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "Organizations:DescribeAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

AWS Identity and Access Management e AWS Organizations

L'accesso a AWS Organizations richiede credenziali. Queste credenziali devono disporre delle autorizzazioni per accedere alle risorse AWS, ad esempio un bucket Amazon Simple Storage Service

(Amazon S3), un'istanza Amazon Elastic Compute Cloud (Amazon EC2) o un'unità organizzativa (UO) AWS Organizations. Le sezioni che seguono forniscono informazioni su come utilizzare AWS Identity and Access Management (IAM) per proteggere l'accesso alla tua organizzazione e controllare chi può amministrarla.

Per determinare chi può amministrare determinate parti della tua organizzazione, AWS Organizations utilizza lo stesso modello di autorizzazioni basate su IAM di altri servizi AWS. In qualità di amministratore dell'account di gestione di un'organizzazione, puoi concedere autorizzazioni basate su IAM per svolgere attività AWS Organizations collegando policy a utenti, gruppi e ruoli nell'account di gestione. Queste policy specificano le operazioni che possono eseguire tali principali. Puoi collegare una policy di autorizzazione IAM a un gruppo di cui è membro l'utente o direttamente a un utente o a un ruolo. Come best practice, ti consigliamo di collegare le policy ai gruppi invece che agli utenti. Inoltre, puoi scegliere di concedere autorizzazioni complete di amministratore ad altri utenti.

Per la maggior parte delle operazioni di amministratore di AWS Organizations, devi collegare le autorizzazioni agli utenti o ai gruppi nell'account di gestione. Se un utente in un account membro deve eseguire operazioni di amministratore per la tua organizzazione, devi concedere le autorizzazioni AWS Organizations a un ruolo IAM nell'account di gestione e abilitare l'utente nell'account membro affinché assuma il ruolo. Per informazioni generali sulle policy di autorizzazione IAM, consulta Panoramica delle policy IAM nella Guida per l'utente di IAM.

Argomenti

Autenticazione

Puoi accedere ad AWS utilizzando uno dei seguenti tipi di identità:

- Utente root dell'Account AWS - Quando si effettua la registrazione su AWS, si forniscono un indirizzo e-mail e una password associati all'Account AWS. Si tratta delle tue credenziali root, che forniscono accesso completo a tutte le risorse AWS.

> **Important**
>
> Durante la registrazione di un Account AWS, viene creato un Utente root dell'account AWS. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWSnell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

- Utente IAM - Un utente IAM è semplicemente un'identità nell'Account AWS che dispone di autorizzazioni personalizzate specifiche (ad esempio, autorizzazioni per creare un file system in Amazon Elastic File System). Puoi utilizzare nome utente e password IAM per accedere a pagine Web AWS sicure come AWS Management Console, forum di discussione AWS o AWS Support Center.

  Oltre a un nome utente e una password, puoi generare chiavi di accesso per ciascun utente. Puoi utilizzare queste chiavi quando accedi in modo sistematico ai servizi AWS tramite uno dei diversi SDK o utilizzando la AWS Command Line Interface (AWS CLI). L'SDK e gli strumenti AWS CLI utilizzano le chiavi di accesso per firmare crittograficamente la tua richiesta. Se non utilizzi gli strumenti AWS, devi firmare la richiesta tu stesso. AWS Organizations supporta Signature Version 4, un protocollo di autenticazione delle richieste API in entrata. Per ulteriori informazioni sull'autenticazione delle richieste, consulta Signing AWS API request nella IAM User Guide.
- Ruolo IAM - Un ruolo IAM è un'altra identità IAM che puoi creare nell'account che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una specifica persona. Un ruolo IAM consente di ottenere le chiavi di accesso temporanee che possono accedere ai servizi e alle risorse AWS. I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:
  - Accesso di utenti federati - Invece di creare un utente IAM, puoi utilizzare le identità degli utenti preesistenti da AWS Directory Service, la directory di utente aziendale o un provider di identità Web. Sono noti come utenti federati. AWS assegna un ruolo a un utente federato quando è richiesto l'accesso tramite un provider di identità. Per ulteriori informazioni sugli utenti federati, consulta la sezione relativa a utenti federati e ruoli nella Guida per l'utente di IAM.
  - Accesso tra account - Puoi utilizzare un ruolo IAM nel tuo account per concedere a un altro Account AWS le autorizzazioni per accedere alle risorse del tuo account. Per un esempio, consulta Tutorial: Delegate l'accesso attraverso l'Account AWSutilizzo dei ruoli IAM nella IAM User Guide.

- Accesso al servizio AWS - Puoi utilizzare un ruolo IAM nel tuo account per concedere a un servizio AWS le autorizzazioni per accedere alle risorse del tuo account. Ad esempio, puoi creare un ruolo che consente ad Amazon Redshift di accedere a un bucket Amazon S3 per tuo conto e quindi caricare i dati archiviati nel bucket in un cluster Amazon Redshift. Per ulteriori informazioni, consultare Creazione di un ruolo per delegare le autorizzazioni a un servizio AWS nella Guida per l'utente di IAM.
- Applicazioni eseguite su Amazon EC2 - Invece di archiviare le chiavi di accesso nell'istanza EC2 per l'uso da parte delle applicazioni eseguite sull'istanza ed effettuare richieste API AWS, puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per queste applicazioni. Per assegnare un ruolo AWS a un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Controllo accessi

Anche se disponi di credenziali valide per autenticare le richieste, non puoi amministrare le risorse AWS Organizations o accedervi se non disponi delle autorizzazioni. Ad esempio, devi avere le autorizzazioni per creare una UO o per collegare una policy di controllo dei servizi (SCP) a un account.

Nelle sezioni seguenti viene descritto come gestire le autorizzazioni per AWS Organizations.

- Gestione delle autorizzazioni di accesso per l'organizzazione AWS
- Utilizzo delle policy basate su identità (policy IAM) per AWS Organizations
- Controllo dell'accesso basato su attributi con tag e AWS Organizations

Gestione delle autorizzazioni di accesso per l'organizzazione AWS

Tutte le risorse AWS, inclusi root, UO, account e policy in un'organizzazione, sono di proprietà di un Account AWS e le autorizzazioni per creare o accedere a una risorsa sono governate dalle policy di autorizzazione. Per un'organizzazione, l'account di gestione possiede tutte le risorse. L'amministratore di un account può controllare l'accesso alle risorse AWS collegando le policy di autorizzazione alle identità IAM (utenti, gruppi e ruoli).

> **Note**
>
> Un amministratore account (o un utente amministratore) è un utente con autorizzazioni di amministratore. Per ulteriori informazioni, consulta Best Practice di sicurezza in IAM nella Guida per l'utente di IAM.

Quando concedi le autorizzazioni, puoi specificare gli utenti che le riceveranno e le risorse per cui le ricevono, nonché le operazioni specifiche da consentire su tali risorse.

Per impostazione predefinita, utenti, gruppi e ruoli IAM non dispongono di autorizzazioni. In qualità di amministratore dell'account di gestione di un'organizzazione, puoi svolgere attività amministrative o delegare autorizzazioni di amministratore ad altri utenti o ruoli IAM nell'account di gestione. Per eseguire questa operazione, è possibile collegare una policy di autorizzazioni IAM a un utente, gruppo o ruolo IAM. Come impostazione predefinita, un utente non ha alcuna autorizzazione; questo a volta si chiama rifiuto implicito. La policy sostituisce il rifiuto implicito con un permesso esplicito che specifica quali operazioni l'utente può eseguire e le risorse su cui possono eseguire le azioni. Se le autorizzazioni sono concesse a un ruolo, gli utenti in altri account dell'organizzazione possono assumere quel ruolo.

Risorse e operazioni AWS Organizations

Questa sezione illustra come i concetti AWS Organizations vengono mappati ai concetti IAM equivalenti.

Risorse

In AWS Organizations, puoi controllare l'accesso alle seguenti risorse:

- Root e UO che costituiscono la struttura gerarchica di un'organizzazione
- Account membri dell'organizzazione
- Policy collegate alle entità dell'organizzazione
- Handshake utilizzati per modificare lo stato dell'organizzazione

Ognuna di queste risorse dispone di un Amazon Resource Name (ARN) univoco associato. Puoi controllare l'accesso a una risorsa specificando il suo nome ARN nell'elemento `Resource` di una policy di autorizzazione IAM. Per un elenco completo dei formati ARN per le risorse utilizzate

inAWS Organizations, vedere Tipi di risorse definiti da AWS Organizations nel Service Authorization Reference.

Operazioni

AWS fornisce un insieme di operazioni da utilizzare con le risorse in un'organizzazione. Esse ti consentono di eseguire operazioni quali creare, elencare, modificare, eliminare le risorse e accedere ai loro contenuti. Puoi fare riferimento alla maggior parte delle operazioni nell'elemento `Action` di una policy IAM per controllare gli utenti che possono utilizzarle. Per un elenco delle AWS Organizations operazioni che possono essere utilizzate come autorizzazioni in una policy IAM, consulta Actions defined by AWS Organizations nel Service Authorization Reference.

Quando combini un elemento `Action` e un elemento `Resource` in una sola policy di autorizzazione `Statement`, puoi controllare esattamente le risorse per le quali quel particolare insieme di operazioni può essere utilizzato.

Chiavi di condizione

AWS fornisce chiavi di condizione sulle quali puoi eseguire query per fornire un controllo più granulare per determinate operazioni. Puoi fare riferimento a queste chiavi di condizione nell'elemento `Condition` di una policy IAM per specificare le circostanze aggiuntive da soddisfare affinché l'istruzione possa essere considerata una corrispondenza.

Le chiavi di condizione seguenti sono particolarmente utili con AWS Organizations:

- `aws:PrincipalOrgID` - Semplifica la determinazione dell'elemento `Principal` in una policy basata su risorse. Questa chiave globale fornisce un'alternativa per elencare tutti gli ID account per tutti gli Account AWS all'interno di un'organizzazione. Invece di elencare tutti gli account che sono membri di un'organizzazione, puoi specificare l'ID organizzazione nell'elemento `Condition`.

  > **Note**
  >
  > Questa condizione globale vale anche per l'account di gestione di un'organizzazione.

  Per ulteriori informazioni, consulta la descrizione delle chiavi contestuali `PrincipalOrgID` in condizione AWS globale nella Guida per l'utente IAM.
- `aws:PrincipalOrgPaths` - Utilizza questa chiave di condizione per abbinare i membri di un root dell'organizzazione specifica, di un'unità organizzativa o dei relativi elementi figlio. La chiave

di condizione `aws:PrincipalOrgPaths` restituisce vero quando il principale (utente root, utente o ruolo IAM) che effettua la richiesta si trova nel percorso dell'organizzazione specificato. Un percorso è una rappresentazione in testo della struttura di un'entità AWS Organizations. Per ulteriori informazioni sui percorsi, consulta Understand the AWS Organizations entity path nella IAM User Guide. Per ulteriori informazioni sull'utilizzo di questa chiave di condizione, consulta aws:PrincipalOrgPaths nella IAM User Guide.

Ad esempio, il seguente elemento condizione corrisponde i membri di una delle due unità organizzative nella stessa organizzazione.

```
            "Condition": {
                "ForAnyValue:StringLike": {
                    "aws:PrincipalOrgPaths": [
                        "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
                        "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-jkl0-awsddddd/"
                    ]
                }
            }
```

- `organizations:PolicyType` - Puoi utilizzare questa chiave di condizione per limitare le operazioni API relative alle policy di Organizations per operare solo su policy Organizations del tipo specificato. Puoi applicare questa chiave di condizione a qualsiasi istruzione delle policy che include un'operazione che interagisce con le policy di Organizations.

  Puoi utilizzare i seguenti valori con questa chiave di condizione:

  - `AISERVICES_OPT_OUT_POLICY`
  - `BACKUP_POLICY`
  - `SERVICE_CONTROL_POLICY`
  - `TAG_POLICY`

  Ad esempio, la seguente policy consente all'utente di eseguire qualsiasi operazione di Organizations. Tuttavia, se l'utente esegue un'operazione che accetta un argomento della policy, l'operazione è consentita solo se la policy specificata è una policy di tagging. L'operazione non riesce se l'utente specifica qualsiasi altro tipo di policy.

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

```
            "Sid": "IfTaggingAPIThenAllowOnOnlyTaggingPolicies",
            "Effect": "Allow",
            "Action": "organizations:*",
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [ "TAG_POLICY" ]
                }
            }
        }
    ]
}
```

- `organizations:ServicePrincipal`— Disponibile come condizione se si utilizzano le AWSServiceAccess operazioni Abilita AWSServiceAccess o Disabilita per abilitare o disabilitare l'accesso affidabile con altri AWS servizi. Puoi utilizzare `organizations:ServicePrincipal` per limitare le richieste effettuate da tali operazioni a un elenco di nomi principali dei servizi approvati.

  Ad esempio, la seguente policy consente all'utente di specificare solo AWS Firewall Manager durante l'abilitazione e la disabilitazione dell'accesso sicuro con AWS Organizations.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyAWSFirewallIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [ "fms.amazonaws.com" ]
                }
            }
        }
    ]
}
```

Per un elenco di tutte le chiavi di condizione AWS Organizations specifiche che possono essere utilizzate come autorizzazioni in una policy IAM, consulta Condition keys for AWS Organizations nel Service Authorization Reference.

Informazioni sulla proprietà delle risorse

L'Account AWS possiede le risorse che vengono create nell'account, indipendentemente da chi ha creato le risorse. Nello specifico, il proprietario della risorsa è l'Account AWS dell'entità principale (ovvero l'utente root, un utente IAM o un ruolo IAM) che autentica la richiesta di creazione della risorsa. Per un'organizzazione AWS, si tratta sempre dell'account di gestione. Non puoi chiamare dagli account membri la maggior parte delle operazioni che creano o accedono alle risorse dell'organizzazione. Negli esempi seguenti viene illustrato il funzionamento:

- Se utilizzi le credenziali dell'account root dell'account di gestione per creare un'UO, il tuo account di gestione è il proprietario della risorsa. In AWS Organizations, la risorsa è la UO.
- Se crei un utente IAM nell'account di gestione e concedi a tale utente le autorizzazioni per creare un'UO, l'utente può creare un'UO. Tuttavia, è l'account di gestione, al quale appartiene l'utente, il proprietario della risorsa UO.
- Se crei un ruolo IAM nell'account di gestione con le autorizzazioni per creare un'UO, chiunque possa assumere il ruolo può creare un'UO. L'account di gestione a cui appartiene il ruolo (non l'utente che lo assume) è il proprietario della risorsa UO.

Gestione dell'accesso alle risorse

La policy delle autorizzazioni descrive chi ha accesso a cosa. Nella sezione seguente vengono descritte le opzioni disponibili per la creazione di policy relative alle autorizzazioni.

> **Note**
>
> Questa sezione riguarda l'utilizzo di IAM nel contesto AWS Organizations. Non vengono fornite informazioni dettagliate sul servizio IAM. Per la documentazione IAM completa, consulta la Guida per l'utente IAM. Per informazioni sulla sintassi e le descrizioni delle policy IAM, consulta il riferimento alla policy IAM JSON nella IAM User Guide.

Le policy collegate a un'identità IAM sono denominate policy basate su identità (policy IAM). Le policy collegate a una risorsa vengono definite policy basate su risorse. AWS Organizations supporta solo le policy basate su identità (policy IAM).

Argomenti

Policy di autorizzazione basate su identità (policy IAM)

Puoi collegare policy alle identità IAM per consentire a tali identità di eseguire operazioni sulle risorse AWS. Ad esempio, puoi eseguire le operazioni seguenti:

- Collegare una policy di autorizzazione a un utente o a un gruppo nel tuo account - Per concedere delle autorizzazioni a un utente per creare una risorsa AWS Organizations, come una policy di controllo dei servizi (SCP) o un'UO, puoi collegare una policy di autorizzazioni a un utente o a un gruppo a cui appartiene l'utente. L'utente o il gruppo devono trovarsi nell'account di gestione dell'organizzazione.
- Collegare una policy di autorizzazione a un ruolo (assegnazione di autorizzazioni tra account) - Puoi collegare una policy di autorizzazione basata su identità a un ruolo IAM per concedere l'accesso tra account a un'organizzazione. Ad esempio, l'amministratore dell'account di gestione può creare un ruolo per concedere autorizzazioni tra account a un utente nell'account membro, come segue:
  1. L'amministratore dell'account di gestione crea un ruolo IAM e collega una policy di autorizzazione al ruolo che concede le autorizzazioni alle risorse dell'organizzazione.
  2. L'amministratore dell'account di gestione collega una policy di attendibilità al ruolo che identifica l'ID dell'account membro come `Principal` per tale ruolo.
  3. L'amministratore dell'account membro può quindi delegare le autorizzazioni per assegnare il ruolo a qualsiasi utente nell'account membro. In questo modo, gli utenti nell'account membro possono creare o accedere alle risorse nell'account di gestione e nell'organizzazione. Il principale nella policy di attendibilità può essere anche un principale del servizio AWS se vuoi concedere le autorizzazioni a un servizio AWS affinché assuma il ruolo.

  Per ulteriori informazioni sull'uso di IAM per delegare le autorizzazioni, consulta Gestione degli accessi nella Guida per l'utente di IAM.

Di seguito sono riportati esempi di policy che consentono a un utente di eseguire l'operazione `CreateAccount` nella tua organizzazione.

```
{
```

```
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Stmt1OrgPermissions",
         "Effect":"Allow",
         "Action":[
            "organizations:CreateAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

È anche possibile definire un ARN parziale nell'elemento `Resource` della policy per indicare il tipo di risorsa.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowCreatingAccountsOnResource",
         "Effect":"Allow",
         "Action":"organizations:CreateAccount",
         "Resource":"arn:aws:organizations::*:account/*"
      }
   ]
}
```

Puoi anche negare la creazione di account che non includono tag specifici per l'account che si sta creando.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyCreatingAccountsOnResourceBasedOnTag",
         "Effect":"Deny",
         "Action":"organizations:CreateAccount",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/key":"value"
```

```
            }
         }
      }
   ]
}
```

Per ulteriori informazioni su utenti, gruppi, ruoli e autorizzazioni, consulta le identità IAM (users, user groups, and roles) nella IAM User Guide.

Policy basate su risorse

Alcuni servizi, come ad esempio Amazon S3, supportano policy di autorizzazione basate su risorse. Ad esempio, puoi collegare una policy a un bucket Amazon S3 per gestire le autorizzazioni di accesso al bucket. Attualmente, AWS Organizations non supporta le policy basate su risorse.

Specifica degli elementi della policy: operazioni, condizioni, effetti e risorse

Per ogni risorsa AWS Organizations, il servizio definisce un insieme di operazioni API che in qualche modo possono interagire con la risorsa o manipolarla. Per concedere le autorizzazioni per queste operazioni, AWS Organizations definisce un insieme di operazioni che puoi specificare in una policy. Ad esempio, per la risorsa UO, AWS Organizations definisce operazioni come la seguente:

- `AttachPolicy` e `DetachPolicy`
- `CreateOrganizationalUnit` e `DeleteOrganizationalUnit`
- `ListOrganizationalUnits` e `DescribeOrganizationalUnit`

In alcuni casi, l'esecuzione di un'operazione API potrebbe richiedere le autorizzazioni necessarie per più di un'azione e per più di una risorsa.

Di seguito sono elencati gli elementi base che puoi utilizzare in una policy di autorizzazione IAM:

- Action (Operazione) - Utilizza questa parola chiave per identificare le operazioni (azioni) che vuoi consentire o rifiutare. Ad esempio, a seconda dell'elemento `Effect` specificato, `organizations:CreateAccount` consente o rifiuta all'utente le autorizzazioni per eseguire l'operazione AWS Organizations `CreateAccount`. Per ulteriori informazioni, consulta IAM JSON Policy elements: Action in the IAM User Guide.
- Risorsa - Utilizza questa parola chiave per specificare l'ARN della risorsa a cui si applica l'istruzione della policy. Per ulteriori informazioni, consulta IAM JSON Policy elements: Resource in the IAM User Guide.

- Condizione - Utilizza questa parola chiave per specificare una condizione che deve essere soddisfatta per l'istruzione di policy da applicare. `Condition` in genere specifica ulteriori circostanze che devono essere vere affinché la policy corrisponda. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Effetto - Utilizza questa parola chiave per specificare se l'istruzione di policy consente o rifiuta l'operazione sulla risorsa. Se non concedi esplicitamente l'accesso a una risorsa (o la consenti), l'accesso viene implicitamente rifiutato. Puoi anche rifiutare esplicitamente l'accesso a una risorsa per essere certo che un utente non possa eseguire un'operazione specifica sulla risorsa specifica, anche quando tale accesso è assegnato da un'altra policy. Per ulteriori informazioni, consulta IAM JSON Policy elements: Effect in the IAM User Guide.
- Principale - Nelle policy basate su identità (policy IAM), l'utente a cui la policy è collegata è automaticamente e implicitamente il principale. Per le policy basate su risorse, specifichi l'utente, l'account, il servizio o un'altra entità che desideri riceva le autorizzazioni (si applica solo alle policy basate su risorse). Attualmente, AWS Organizations supporta solo le policy basate su identità e non su risorse.

Per ulteriori informazioni sulla sintassi e le descrizioni delle policy IAM, consulta il riferimento alla policy IAM JSON nella IAM User Guide.

Utilizzo delle policy basate su identità (policy IAM) per AWS Organizations

In qualità di amministratore dell'account di gestione di un'organizzazione, puoi controllare l'accesso alle risorse AWS collegando le policy di autorizzazione alle identità AWS Identity and Access Management (IAM) (utenti, gruppi e ruoli) all'interno dell'organizzazione. Quando si concedono le autorizzazioni, è necessario specificare gli utenti che le riceveranno e le risorse per cui si concedono, nonché le operazioni specifiche da consentire su tali risorse. Se le autorizzazioni sono concesse a un ruolo, tale ruolo può essere assunto da utenti in altri account nell'organizzazione.

Per impostazione predefinita, un utente non dispone di autorizzazioni di alcun tipo. Tutte le autorizzazioni devono essere concesse esplicitamente da una policy. Se un'autorizzazione non è concessa in modo esplicito, viene implicitamente rifiutata. Se un'autorizzazione viene negata esplicitamente, verranno ignorate eventuali altre policy che l'hanno concessa. In altre parole, un utente dispone solo delle autorizzazioni concesse esplicitamente e non negate esplicitamente.

Oltre alle tecniche di base descritte in questo argomento, è possibile controllare l'accesso all'organizzazione utilizzando i tag applicati alle risorse dell'organizzazione: il root dell'organizzazione,

le unità organizzative (UO), gli account e le policy. Per ulteriori informazioni, consulta Controllo dell'accesso basato su attributi con tag e AWS Organizations.

Concessione delle autorizzazioni complete di amministratore a un utente

È possibile creare una policy IAM che conceda autorizzazioni piene di amministratore AWS Organizations a un utente IAM nell'organizzazione. È possibile modificare questa policy utilizzando l'editor di policy JSON nella console IAM.

Come utilizzare l'editor di policy JSON per creare una policy

1. Accedi a AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione a sinistra, seleziona Policies (Policy).

   Se è la prima volta che selezioni Policy, verrà visualizzata la pagina Benvenuto nelle policy gestite. Seleziona Inizia.
3. Nella parte superiore della pagina, scegli Crea policy.
4. Nella sezione Editor di policy, scegli l'opzione JSON.
5. Inserisci il documento di policy JSON seguente:

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

6. Seleziona Avanti.

> **Note**
>
> È possibile alternare le opzioni dell'editor Visivo e JSON in qualsiasi momento. Se tuttavia si apportano modifiche o si seleziona Successivo nell'editor Visivo, IAM potrebbe ristrutturare la policy in modo da ottimizzarla per l'editor visivo. Per ulteriori informazioni, consulta Modifica della struttura delle policy nella Guida per l'utente di IAM.

7. Nella pagina Rivedi e crea, inserisci un valore in Nome policy e Descrizione (facoltativo) per la policy in fase di creazione. Rivedi Autorizzazioni definite in questa policy per visualizzare le autorizzazioni concesse dalla policy.
8. Seleziona Crea policy per salvare la nuova policy.

Per ulteriori informazioni sulla creazione di una policy IAM, consulta Creating IAM policies nella IAM User Guide.

Concessione di un accesso limitato mediante operazioni

Se vuoi concedere delle autorizzazioni limitate anziché complete, puoi creare una policy che elenca le autorizzazioni singole che vuoi concedere nell'elemento `Action` della policy delle autorizzazioni IAM. Come illustrato nell'esempio seguente, puoi usare dei caratteri jolly (*) per concedere solo le autorizzazioni `Describe*` e `List*`, sostanzialmente fornendo l'accesso in sola lettura all'organizzazione.

> **Note**
>
> In una policy di controllo dei servizi (SCP), il carattere jolly (*) in un elemento `Action` può essere utilizzato unicamente da solo o al termine della stringa. Non può trovarsi all'inizio o al centro della stringa. Pertanto, `"servicename:action*"` è valida, ma `"servicename:*action"` e `"servicename:some*action"` non sono entrambe valide nelle SCP.

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

Per un elenco di tutte le autorizzazioni disponibili per l'assegnazione in una policy IAM, consulta Actions defined by AWS Organizations nel Service Authorization Reference.

Concessione dell'accesso a risorse specifiche

Oltre a limitare l'accesso a operazioni specifiche, puoi anche limitare l'accesso a entità specifiche nell'organizzazione. Gli elementi `Resource` negli esempi trattati nelle sezioni precedenti specificano tutti il carattere jolly "*", che significa "qualsiasi risorsa alla quale può accedere questa operazione". In alternativa, puoi sostituire il carattere "*" con l'Amazon Resource Name (ARN) delle entità specifiche a cui vuoi consentire l'accesso.

Esempio: concessione delle autorizzazioni a una singola UO

La prima istruzione della policy seguente consente a un utente IAM l'accesso in lettura all'intera organizzazione, ma la seconda istruzione consente all'utente di eseguire operazioni amministrative di AWS Organizations solo all'interno di una singola unità organizzativa specificata. Questo non si estende ad alcuna unità organizzativa figlia. Non viene concesso alcun accesso alla fatturazione. Nota che ciò non consente l'accesso amministrativo agli Account AWS nell'unità organizzativa. Concede solo le autorizzazioni per eseguire operazioni AWS Organizations sugli account all'interno dell'unità organizzativa specificata:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "organizations:*",
      "Resource": "arn:aws:organizations::<masterAccountId>:ou/o-<organizationId>/ou-
<organizationalUnitId>"
    }
  ]
}
```

È possibile ottenere gli ID per l'unità organizzativa e l'organizzazione dalla console AWS Organizations o chiamando le API `List*`. L'utente o il gruppo a cui applichi questa policy può eseguire qualsiasi operazione (`"organizations:*"`) su qualsiasi entità direttamente contenuta

nell'unità organizzativa specificata. L'unità organizzativa è identificata dall'Amazon Resource Name (ARN).

Per ulteriori informazioni sugli ARN per varie risorse, vedere Tipi di risorse definiti da AWS Organizations nel Service Authorization Reference.

Garantire la possibilità di abilitare l'accesso attendibile a principali del servizio limitati

Puoi utilizzare l'elemento `Condition` di un'istruzione di policy per limitare ulteriormente le circostanze alle quali corrisponde l'istruzione di policy.

Esempio: concessione delle autorizzazioni per abilitare l'accesso attendibile a un servizio specificato

Nell'istruzione seguente viene illustrato come limitare la possibilità di abilitare l'accesso attendibile solo ai servizi specificati. Se l'utente tenta di chiamare l'API con un principale di servizio diverso da quello per AWS IAM Identity Center, questa policy non corrisponde e la richiesta viene negata:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals" : {
                    "organizations:ServicePrincipal" : "sso.amazonaws.com"
                }
            }
        }
    ]
}
```

Per ulteriori informazioni sugli ARN per varie risorse, vedere Tipi di risorse definiti da AWS Organizations nel Service Authorization Reference.

Controllo dell'accesso basato su attributi con tag e AWS Organizations

Il controllo degli accessi basato sugli attributi consente di utilizzare attributi gestiti dall'amministratore, come tag associati sia alle risorse AWS sia alle identità AWS, per controllare l'accesso a quelle risorse. Ad esempio, puoi specificare che un utente può accedere a una risorsa quando sia l'utente sia la risorsa hanno lo stesso valore per un determinato tag.

Le risorse taggabili AWS Organizations includono Account AWS, il root, le unità organizzative (UO) o le policy dell'organizzazione. Quando si associano tag alle risorse di Organizations, è possibile utilizzarli per controllare chi può accedere a tali risorse. Lo puoi fare aggiungendo elementi `Condition` alle istruzioni della policy delle autorizzazioni AWS Identity and Access Management (IAM) che controllano se determinate chiavi e valori di tag sono presenti prima di consentire l'operazione. Ciò consente di creare una policy IAM che afferma efficacemente "Consenti all'utente di gestire solo le unità organizzative che dispongono di un tag con una chiave `X` e un valore `Y`" oppure "Consenti all'utente di gestire solo le unità organizzative che dispongono di un tag con una chiave `Z` che ha lo stesso valore della chiave di tag associata all'utente `Z`".

Puoi basare i tuoi test di `Condition` su diversi tipi di riferimenti tag in una policy IAM.

- Controllo dei tag associati alle risorse specificate nella richiesta
- Controllo dei tag associati all'utente o al ruolo IAM che effettua la richiesta
- Controllare i tag che sono inclusi come parametri nella richiesta

Per ulteriori informazioni sull'utilizzo dei tag per il controllo degli accessi nelle policy, consulta Controllo dell'accesso a e per utenti e ruoli IAM mediante i tag delle risorse. Per la sintassi completa delle policy di autorizzazione IAM, consulta la Documentazione di riferimento della policy JSON di IAM

Controllo dei tag associati alle risorse specificate nella richiesta

Quando effettui una richiesta utilizzando la AWS Management Console, la AWS Command Line Interface (AWS CLI) o un SDK AWS, puoi specificare le risorse a cui desideri accedere con tale richiesta. Se stai tentando di elencare le risorse disponibili di un determinato tipo, leggere o scrivere su una risorsa, oppure modificare o aggiornare una risorsa, è necessario specificare la risorsa a cui accedere come parametro nella richiesta. Tali richieste sono controllate dalle policy delle autorizzazioni IAM collegate agli utenti e ai ruoli. In queste policy è possibile confrontare i tag associati alla risorsa richiesta e scegliere di consentire o negare l'accesso in base alle chiavi e ai valori di tali tag.

Per controllare un tag associato alla risorsa, fai riferimento al tag in un elemento `Condition` anteponendo al nome della chiave tag la seguente stringa: `aws:ResourceTag/`

Ad esempio, la seguente policy consente all'utente o al ruolo di eseguire qualsiasi operazione AWS Organizations a meno che quella risorsa abbia un tag con chiave `department` e valore `security`. Se la chiave e il valore sono presenti, la policy nega esplicitamente l'operazione `UntagResource`.

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

        },
        {
            "Effect" : "Deny",
            "Action" : "organizations:UntagResource",
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "aws:ResourceTag/department" : "security"
                }
            }
        }
    ]
}
```

Per ulteriori informazioni sull'utilizzo di questo elemento, consulta Controllo dell'accesso alla risorsa e aws:ResourceTag nella Guida per l'utente di IAM.

Controllo dei tag associati all'utente o al ruolo IAM che effettua la richiesta

Puoi controllare le operazioni consentite alla persona che effettua la richiesta (il principale) in base ai tag collegati all'utente o ruolo IAM di tale persona. Per eseguire questa operazioni, usa la chiave di condizione `aws:PrincipalTag/`*`key-name`* per specificare quale tag e valore devono essere associati all'utente o al ruolo chiamante.

L'esempio seguente mostra come consentire un'operazione solo quando il tag specificato (`cost-center`) ha lo stesso valore sia sul principale che chiama l'operazione, sia sulla risorsa a cui si accede dall'operazione. In questo esempio, l'utente chiamante può avviare e arrestare un'istanza Amazon EC2 solo se l'istanza è contrassegnata con lo stesso valore `cost-center` dell'utente.

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

```
            "ec2:startInstances",
            "ec2:stopInstances"
        ],
        "Resource": "*",
        "Condition": {"StringEquals":
            {"ec2:ResourceTag/cost-center": "${aws:PrincipalTag/cost-center}"}}
    }
}
```

Per ulteriori informazioni sull'utilizzo di questo elemento, consulta Controllo dell'accesso per i principali IAM e `aws:PrincipalTag` nella Guida per l'utente di IAM.

Controllare i tag che sono inclusi come parametri nella richiesta

Sono diverse le operazioni che ti consentono di specificare i tag come parte della richiesta. Ad esempio, quando si crea una risorsa è possibile specificare i tag associati alla nuova risorsa. È possibile specificare un elemento `Condition` che utilizza `aws:TagKeys` per permettere o negare l'operazione in base al fatto che una chiave di tag specifica, o un set di chiavi, sia incluso nella richiesta. A questo operatore di confronto non interessa quale valore contiene il tag. Controlla solo se è presente un tag con la chiave specificata.

Per controllare la chiave di tag o un elenco di chiavi, specifica un elemento `Condition` con la sintassi seguente:

```
"aws:TagKeys": [ "tag-key-1", "tag-key-2", ... , "tag-key-n" ]
```

Puoi utilizzare `ForAllValues:` per anteporre un operatore di confronto per assicurarti che tutte le chiavi nella richiesta debbano corrispondere a una delle chiavi specificate nella policy. Ad esempio, la seguente policy autorizza qualsiasi operazione di Organizations solo se tutte e tre le chiavi di tag specificate sono presenti nella richiesta.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAllValues:StringEquals": {
                "aws:TagKeys": [
                    "department",
```

```
                    "costcenter",
                    "manager"
                ]
            }
        }
    }
}
```

In alternativa, puoi utilizzare `ForAnyValue:` per anteporre un operatore di confronto per assicurarti che almeno una delle chiavi nella richiesta debba corrispondere a una delle chiavi specificate nella policy. Ad esempio, la seguente policy autorizza qualsiasi operazione di Organizations solo se almeno una delle chiavi di tag specificate è presente nella richiesta.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "stage",
                    "region",
                    "domain"
                ]
            }
        }
    }
}
```

Sono diverse le operazioni che ti consentono di specificare i tag nella richiesta. Ad esempio, quando si crea una risorsa è possibile specificare i tag associati alla nuova risorsa. È possibile confrontare una coppia chiave-valore di tag nella policy con una coppia chiave-valore inclusa nella richiesta. Per fare ciò, fai riferimento al tag in un elemento `Condition` anteponendo al nome della chiave tag la seguente stringa: `aws:RequestTag/`*`key-name`*, quindi specifica il valore del tag che deve essere presente.

Ad esempio, la seguente policy di esempio nega qualsiasi richiesta da parte dell'utente o del ruolo di creare un Account AWS se alla richiesta manca il tag `costcenter` o assegna a tale tag un valore diverso da `1`, `2` oppure `3`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/costcenter": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/costcenter": [
                        "1",
                        "2",
                        "3"
                    ]
                }
            }
        }
    ]
}
```

Per ulteriori informazioni sull'utilizzo di questi elementi, consulta aws:TagKeys e aws:RequestTag nella Guida per l'utente di IAM.

Registrazione e monitoraggio in AWS Organizations

Come best practice, dovresti monitorare la tua organizzazione per accertarti che le modifiche vengano registrate. Questo aiuta a garantire che qualsiasi modifica imprevisti possa essere controllata e che le modifiche indesiderate possano essere sottoposte a rollback. AWS Organizations attualmente supporta due servizi AWS che ti consentono di monitorare l'organizzazione e le attività che avvengono al suo interno.

Argomenti

Registrazione delle chiamate API AWS Organizations con AWS CloudTrail

AWS Organizations è integrato con AWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o un servizio AWS in AWS Organizations. CloudTrail acquisisce tutte le chiamate API per AWS Organizations come eventi, incluse le chiamate dalla console AWS Organizations e dalle chiamate di codice alle API AWS Organizations. Se viene creato un trail, è possibile abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon S3, inclusi gli eventi per AWS Organizations. Se non si configura un trail, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia eventi). Le informazioni raccolte da CloudTrail consentono di determinare la richiesta effettuata ad AWS Organizations, l'indirizzo IP da cui è partita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

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

> **Important**
>
> È possibile visualizzare tutte le informazioni di CloudTrail solo per AWS Organizations nella Regione Stati Uniti orientali (Virginia settentrionale). Se non vedi l'attività AWS Organizations nella console CloudTrail, impostala su Stati Uniti orientali (Virginia settentrionale) utilizzando il menu nell'angolo superiore destro. Se interroghi CloudTrail con il comando AWS CLI o gli strumenti SDK, indirizza la query all'endpoint Stati Uniti orientali (Virginia settentrionale).

Informazioni su AWS Organizations in CloudTrail

CloudTrail è abilitato sul tuo Account AWS al momento della sua creazione. Quando si verifica un'attività su AWS Organizations, questa viene registrata in un evento CloudTrail insieme ad altri eventi di servizio AWS nella Cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nell'Account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia eventi di CloudTrail.

Per una registrazione continua degli eventi nell'Account AWS che includa gli eventi per AWS Organizations, crea un trail. Un percorso abilita la distribuzione da parte di CloudTrail dei file di

log in un bucket Amazon S3. Quando la registrazione di CloudTrail è abilitata nell'Account AWS, le chiamate API effettuate alle operazioni AWS Organizations vengono tracciate in file di log di CloudTrail, dove vengono scritte con altri record del servizio AWS. Puoi configurare altri servizi AWS per analizzare con maggiore dettaglio e agire sui dati dell'evento raccolti nei registri di CloudTrail. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- Servizi e integrazioni CloudTrail supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail

Tutte le operazioni AWS Organizations vengono registrate da CloudTrail e sono documentate nella documentazione di riferimento delle API di AWS Organizations. Ad esempio, le chiamate a `CreateAccount` (incluso l'evento `CreateAccountResult`), `ListHandshakesForAccount`, `CreatePolicy` e `InviteAccountToOrganization` generano voci nei file di log di CloudTrail.

Ogni voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni sull'identità dell'utente nella voce di log ti permettono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o utente IAM
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo IAM o un utente federato
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta l'argomento relativo all'elemento userIdentity di CloudTrail.

Comprensione delle voci dei file di log di AWS Organizations

Un trail è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato. I file di log di CloudTrail possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, sulla data e sull'ora dell'operazione, sui parametri richiesti e così via. I file di log CloudTrail non sono una traccia di pila ordinata delle chiamate API pubbliche e di conseguenza non devono apparire in base a un ordine specifico.

Esempio di voci di log: CreateAccount

L'esempio seguente mostra una voce di log di CloudTrail per una chiamata `CloseAccount` di esempio, che viene generata quando l'API viene invocata e il flusso di lavoro per la chiusura dell'account avvia l'elaborazione in background.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2022-03-18T18:17:06Z"
            }
        }
    },
    "eventTime": "2022-03-18T18:17:06Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CloseAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)...",
    "requestParameters": {
        "accountId": "555555555555"
    },
    "responseElements": null,
    "requestID": "e28932f8-d5da-4d7a-8238-ef74f3d5c09a",
    "eventID": "19fe4c10-f57e-4cb7-a2bc-6b5c30233592",
    "readOnly": false,
    "eventType": "AwsApiCall",
```

```
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

L'esempio seguente mostra una voce di log di CloudTrail per una chiamata `CloseAccountResult` dopo il corretto completamento del flusso di lavoro in background per la chiusura dell'account.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "organizations.amazonaws.com"
  },
  "eventTime": "2022-03-18T18:17:06Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CloseAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "organizations.amazonaws.com",
  "userAgent": "organizations.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "closeAccountStatus": {
      "accountId": "555555555555",
      "state": "SUCCEEDED",
      "requestedTimestamp": "Mar 18, 2022 6:16:58 PM",
      "completedTimestamp": "Mar 18, 2022 6:16:58 PM"
    }
   },
   "eventCategory": "Management"
}
```

Esempio di voci di log: CreateAccount

L'esempio seguente mostra una voce di log di CloudTrail per una chiamata `CreateAccount` di esempio, che viene generata quando l'API viene invocata e il flusso di lavoro per la creazione dell'account avvia l'elaborazione in background.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-09-16T21:16:45Z"
            }
        }
    },
    "eventTime": "2018-06-21T22:06:27Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Windows NT 10.0; Win64; x64)...",
    "requestParameters": {
        "tags": [],
        "email": "****",
        "accountName": "****"
    },
    "responseElements": {
        "createAccountStatus": {
            "accountName": "****",
```

```
            "state": "IN_PROGRESS",
            "id": "car-examplecreateaccountrequestid111",
            "requestedTimestamp": "Sep 16, 2020 9:20:50 PM"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

L'esempio seguente mostra una voce di log di CloudTrail per una chiamata `CreateAccount`dopo il corretto completamento del flusso di lavoro in background per la creazione dell'account.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "..."
  },
  "eventTime": "2020-09-16T21:20:53Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "....",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "SUCCEEDED",
      "accountName": "****",
      "accountId": "444455556666",
      "requestedTimestamp": "Sep 16, 2020 9:20:50 PM",
      "completedTimestamp": "Sep 16, 2020 9:20:53 PM"
    }
  }
}
```

L'esempio seguente mostra una voce di log di CloudTrail generata dopo che un flusso di lavoro `CreateAccount` in background non completa la creazione dell'account.

```
  {
  "eventVersion": "1.06",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2018-06-21T22:06:27Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "FAILED",
      "accountName": "****",
      "failureReason": "EMAIL_ALREADY_EXISTS",
      "requestedTimestamp": Jun 21, 2018 10:06:27 PM,
      "completedTimestamp": Jun 21, 2018 10:07:15 PM
    }
  }
}
```

Esempio di voce di log: CreateOrganizationalUnit

Nell'esempio seguente viene mostrata una voce di log di CloudTrail per una chiamata `CreateOrganizationalUnit` di esempio.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
```

```
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:40:11Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateOrganizationalUnit",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "name": "OU-Developers-1",
        "parentId": "r-a1b2"
    },
    "responseElements": {
        "organizationalUnit": {
            "arn": "arn:aws:organizations::111111111111:ou/o-aa111bb222/ou-
examplerootid111-exampleouid111",
            "id": "ou-examplerootid111-exampleouid111",
            "name": "test-cloud-trail"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Esempio di voce di log: InviteAccountToOrganization

Nell'esempio seguente viene mostrata una voce di log di CloudTrail per una chiamata `InviteAccountToOrganization` di esempio.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
```

```
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:41:17Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "InviteAccountToOrganization",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "notes": "This is a request for Mary's account to join Diego's organization.",
        "target": {
            "type": "ACCOUNT",
            "id": "111111111111"
        }
    },
    "responseElements": {
        "handshake": {
            "requestedTimestamp": "Jan 18, 2017 9:41:16 PM",
            "state": "OPEN",
            "arn": "arn:aws:organizations::111111111111:handshake/o-aa111bb222/invite/
h-examplehandshakeid111",
            "id": "h-examplehandshakeid111",
            "parties": [
                {
                    "type": "ORGANIZATION",
                    "id": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "id": "222222222222"
                }
            ],
            "action": "invite",
            "expirationTimestamp": "Feb 2, 2017 9:41:16 PM",
            "resources": [
                {
                    "resources": [
                        {
                            "type": "MASTER_EMAIL",
                            "value": "diego@example.com"
                        },
                        {
```

```
                            "type": "MASTER_NAME",
                            "value": "Management account for organization"
                        },
                        {
                            "type": "ORGANIZATION_FEATURE_SET",
                            "value": "ALL"
                        }
                    ],
                    "type": "ORGANIZATION",
                    "value": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "value": "222222222222"
                },
                {
                    "type": "NOTES",
                    "value": "This is a request for Mary's account to join Diego's
 organization."
                }
            ]
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Esempio di voce di log: AttachPolicy

Nell'esempio seguente viene mostrata una voce di log di CloudTrail per una chiamata `AttachPolicy` di esempio. La risposta indica che la chiamata non è riuscita perché il tipo di policy richiesto non è abilitato nella root in cui si è verificato il tentativo di richiesta di collegamento.

```
{
    "eventVersion": "1.06",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:42:44Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "AttachPolicy",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "errorCode": "PolicyTypeNotEnabledException",
    "errorMessage": "The given policy type ServiceControlPolicy is not enabled on the
 current view",
    "requestParameters": {
        "policyId": "p-examplepolicyid111",
        "targetId": "ou-examplerootid111-exampleouid111"
    },
    "responseElements": null,
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```


Amazon EventBridge

AWS Organizations può funzionare con Amazon EventBridge, precedentemente Eventi Amazon CloudWatch per segnalare gli eventi quando in un'organizzazione si verificano delle operazioni specificate dall'amministratore. Ad esempio, data la sensibilità di tali operazioni, la maggior parte degli amministratori desidera essere avvisata ogni volta che un utente crea un nuovo account nell'organizzazione o quando un amministratore di un account membro tenta di lasciare l'organizzazione. È possibile configurare delle regole EventBridge che cercano tali operazioni e inviare gli eventi generati alle destinazioni definite dagli amministratori. I target possono essere un argomento Amazon SNS che invia e-mail o messaggi di testo agli abbonati. È anche possibile creare una funzione AWS Lambda che registra i dettagli dell'operazione per un'analisi successiva.

Per un tutorial che mostra come abilitare EventBridge per monitorare le attività chiave nell'organizzazione, consulta Tutorial: Monitoraggio delle modifiche importanti all'organizzazione con Amazon EventBridge.

Per ulteriori informazioni su EventBridge, incluso come configurarlo e abilitarlo, consulta la Guida per l'utente di Amazon EventBridge.

Convalida della conformità per AWS Organizations

Per sapere se il Servizio AWS è coperto da programmi di conformità specifici, consulta i Servizi AWS coperti dal programma di conformità e scegli il programma di conformità desiderato. Per informazioni generali, consulta Programmi per la conformità di AWS.

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

La responsabilità di conformità durante l'utilizzo dei Servizi AWS è determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle normative vigenti. Per semplificare il rispetto della conformità, AWS mette a disposizione le seguenti risorse:

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

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

- Risorse per la conformità AWS: una raccolta di cartelle di lavoro e guide suddivise per settore e area geografica.
- Guide alla conformità per i clienti AWS: acquisisci nozioni sul modello di responsabilità condivisa attraverso la lente di conformità. Le guide riassumono le best practice per la protezione dei Servizi AWS e tracciano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con le regole nella Guida per gli sviluppatori di AWS Config: il servizio AWS Config valuta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti.
- AWS Security Hub: questo Servizio AWS fornisce una visione completa dello stato di sicurezza all'interno di AWS. La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse

AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.

- AWS Audit Manager: questo Servizio AWS aiuta a effettuare un audit costante dell'utilizzo di AWS per semplificare la gestione dei rischi e della conformità alle normative e agli standard di settore.

Resilienza in AWS Organizations

L'infrastruttura globale di AWS è progettata attorno a Regioni AWS e zone di disponibilità. Regioni AWS fornisce più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e velocità effettiva elevata. Con le zone di disponibilità, è possibile progettare e gestire le applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo.

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

Sicurezza dell'infrastruttura in AWS Organizations

Come servizio gestito, AWS Organizations è protetto dalla sicurezza di rete globale AWS. Per informazioni sui servizi di sicurezza AWS e su come AWS protegge l'infrastruttura, consulta la pagina Sicurezza del cloud AWS. Per progettare l'ambiente AWS utilizzando le best practice per la sicurezza dell'infrastruttura, consulta la pagina Protezione dell'infrastruttura nel Pilastro della sicurezza di AWS Well-Architected Framework.

Utilizza le chiamate API pubblicate di AWS per accedere a Organizations tramite la rete. I clienti devono supportare quanto segue:

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

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare AWS Security

Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Se si richiedono moduli crittografici convalidati FIPS 140-2 quando si accede ad AWS tramite una CLI o un'API, utilizzare un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

AWS OrganizationsRiferimento

Utilizza gli argomenti di questa sezione per trovare informazioni di riferimento dettagliate per vari aspetti di AWS Organizations.

Argomenti

Quote per AWS Organizations

In questa sezione vengono specificate le quote che interessano AWS Organizations.

Linee guida per la denominazione

Di seguito sono riportate le linee guida per i nomi creati in AWS Organizations, inclusi i nomi degli account, delle unità organizzative (OU), delle radici e delle politiche:

- Devono essere composti da caratteri Unicode
- La lunghezza massima della stringa dei nomi varia in base all'oggetto. Per visualizzare il limite effettivo per ciascuno di essi, consulta la documentazione di riferimento delle API di AWS Organizations e cerca l'operazione API che crea l'oggetto. Guarda i dettagli per il parametro `Name` dell'organizzazione. Ad esempio: Account name (Nome account) oppure OU name (Nome UO).

Valori massimi e minimi

Di seguito sono riportati i valori massimi predefiniti per le entità in AWS Organizations.

> **Note**
>
> È possibile richiedere un aumento di alcuni di questi valori utilizzando il metodo Console Service Quotas.
> Organizations è un servizio globale ospitato fisicamente nella Regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`). Pertanto, è necessario utilizzare `us-east-1` per accedere alle quote di Organizations quando si utilizza la console Service Quotas, AWS CLI il o AWS un SDK.

Numero di membri di un'organizzazione Account AWS	10 — Il numero massimo di default di account consentiti in un'organizzazione. Se sono necessari altri, richiedi un aumento utilizzando Console Service Quotas. Un invito inviato a un account rientra nel calcolo di questa quota. Il conteggio viene annullato se l'account invitato rifiuta, l'account di gestione annulla l'invito o l'invito scade. Gli account e le organizzazioni appena creati potrebbero avere una quota inferiore a quella predefinita di 10 account.
Numero di radici in un'organizzazione	1
Numero di UO in un'organizzazione	1000
Numero di policy di ciascun tipo in un'organizzazione	1000 per tipo di policy
Dimensione massima di un documento di policy	Policy di controllo dei servizi: 5.120 caratteri Policy di rifiuto dei servizi di IA: 2.500 caratteri Policy di backup: 10.000 caratteri Policy di tag: 10.000 caratteri Nota: se si salva la policy utilizzando lo spazio bianco aggiuntivo (ad esempio spazi e interruzioni di riga) tra gli elementi JSON e al di fuori delle virgolette, viene rimosso e non conteggiato. AWS Management Console Se salvate la policy utilizzando un'operazione SDK o il AWS CLI, la policy viene salvata esattamente come avete fornito e non viene effettuata alcuna rimozione automatica dei caratteri.
Nidificazione massima UO in una radice	Cinque livelli di UO sotto una radice.

Numero massimo di tentativi di inviti che è possibile eseguire in un periodo di 24 ore	20 o il numero massimo di account consentiti nella tua organizza zione, a seconda di quale dei due è maggiore. Gli inviti accettati non rientrano nel calcolo di questa quota. Non appena un invito viene accettato, è possibile inviare un altro invito lo stesso giorno. Se il numero massimo di account consentiti nell'organizzazione è inferiore a 20, si ottiene l'eccezione "limite di account superato" se si tenta di invitare più account di quelli ammessi dall'organizzazion e. Tuttavia, è possibile annullare gli inviti e inviarne di nuovi fino a un massimo di 20 tentativi in un giorno.
Numero di account membri che è possibile creare simultaneamente	5 - Non appena ne termina una, è possibile avviarne un'altra, ma solo cinque possono essere in corso simultaneamente.
Numero di account membri che è possibile chiudere in un periodo di 30 giorni	10% degli account dei membri di un'organizzazione, con un massimo di 1000. • < 100 account: puoi chiudere fino a 10 account membri • 100 - 10.000 account: puoi chiudere fino al 10% dei tuoi account membri • > 10.000 account: puoi chiudere fino a 1000 account membri Ad esempio, se disponi di 10.500 account membri, puoi chiudere fino a 1000 (non 1050) account in un periodo di 30 giorni. Una volta raggiunta questa quota, potrai chiudere altri account nella console AWS Billing o attendere che la quota venga ripristinata. Per ulteriori informazioni, consulta Cosa è necessario sapere prima di chiudere l'account nella Guida alla gestione degli AWS account.
Numero di account membri che è possibile chiudere simultane amente	3 - È possibile elaborare contemporaneamente la chiusura di un massimo di tre account. Non appena una procedura di chiusura finisce, è possibile chiudere un altro account.

Numero di entità alle quali è possibile collegare una policy	Illimitato
Numero di tag che è possibile collegare a un root, un'UO o un account	50
Dimensione massima della policy di delega basata sulle risorse	40.000 caratteri

Tempi di scadenza per gli handshake

Di seguito sono riportati i timeout per le strette di mano. AWS Organizations

Invito a far parte di un'organizzazione	15 giorni
Richiesta di abilitazione di tutte le funzionalità in un'organizzazione	90 giorni
Handshake eliminato e non più visibile negli elenchi	30 giorni dopo il completamento dell'handshake

Numero di policy che è possibile collegare a un'entità

I valori minimo e massimo dipendono dal tipo di policy e dall'entità a cui colleghi la policy. La seguente tabella mostra ogni tipo di policy e il numero di entità a cui è possibile collegare ogni tipo.

> **Note**
>
> Questi numeri si applicano solo alle policy direttamente collegate a un'unità organizzativa o a un account. Le policy che interessano un'unità organizzativa o un account per ereditarietà non rientrano nel conteggio di questi limiti.

Tipo di policy	Numero minimo di collegamenti a un'entità	Numero massimo di collegamenti al root	Numero massimo di collegamenti per UO	Numero massimo di collegamenti per account
Policy di controllo dei servizi	1 - Ogni entità deve avere almeno una SCP sempre collegata . Non è possibile rimuovere l'ultima SCP da un'entità.	5	5	5
Policy di rifiuto dei servizi di IA	0	5	5	5
Policy di backup	0	10	10	10
Policy di tag	0	10	10	10

> **Note**
>
> Al momento, è possibile disporre di una sola root in un'organizzazione.

Limiti di limitazione

La tabella seguente elenca le AWS Organizations API per categoria di gestione e mostra le rispettive percentuali di limitazione a livello di account e organizzazione.

AWS Organizations API	Limite per account (rate, burst)	Limite per organizzazione (rate, burst)
Gestione dell'account		
CloseAccount	.05, 1	
CreateAccount, CreateGovCloudAccount	0,1, 3	
DescribeAccount	20, 30	24, 36
DescribeCreateAccountStatus	2, 2	2, 3
LeaveOrganization	1, 1	
ListCreateAccountStatus	5, 8	6, 10
Gestione delle strette di mano		
AcceptHandshake, DescribeHandshake	1, 1	
CancelHandshake	2, 3	
DeclineHandshake	1, 3	
InviteAccountToOrganization	3, 5	
ListHandshakesForAccount, ListHandshakesForOrganization	5, 8	6, 10
Gestione dell'organizzazione		
CreateOrganization, DeleteOrganization, EnableFullControl	1, 1	
CreateOrganizationalUnit, DescribeOrganization	1, 2	

AWS Organizations API	Limite per account (rate, burst)	Limite per organizzazione (rate, burst)
MoveAccount, UpdateOrganizationalUnit, DeleteOrganizationalUnit	2, 3	
DescribeOrganizationalUnit	2, 2	2, 3
ListAccounts	8, 12	9, 15
ListChildren	6, 10	7, 12
ListParents, ListAccountsForParent, ListOrganizationalUnitsForParent	5, 8	6, 10
ListRoots	1, 2	1, 3
ListTagsForResource	10, 15	12, 18
RemoveAccountFromOrganization	2, 2	
TagResource, UntagResource	4, 6	
Gestione delle politiche		
CreatePolicy, DeletePolicy, AttachPolicy, DetachPolicy	2, 3	
DescribePolicy	2, 2	2, 3
DisablePolicyType, EnablePolicyType	1, 1	
ListPolicies, ListPoliciesForTarget, ListTargetsForPolicy	5, 8	6, 10
UpdatePolicy	2, 3	

AWS Organizations API	Limite per account (rate, burst)	Limite per organizzazione (rate, burst)
Gestione di servizi		
AbilitaAWSServiceAccess, disabilita AWSServiceAccess	1, 2	
ElencoAWSServiceAccessForOrganization, ListDelegatedServicesForAccount	1, 3	1, 4
ListDelegatedAdministrators	5, 8	6, 10
RegisterDelegatedAdministrator, DeregisterDelegatedAdministrator	1, 2	

AWS Policy gestite disponibili per l'uso con AWS Organizations

Questa sezione identifica le policy gestite da AWS fornite che puoi utilizzare per gestire la tua organizzazione. Non puoi modificare né eliminare una policy gestita da AWS, ma puoi collegarla alle entità nella tua organizzazione, o distaccarla, in base alle esigenze.

Policy gestite da AWS Organizations per l'uso con AWS Identity and Access Management (IAM)

Una policy gestita IAM è fornita e gestita da AWS. Una policy gestita fornisce autorizzazioni per le attività comuni che è possibile assegnare agli utenti collegando la policy gestita all'utente o all'oggetto ruolo IAM appropriato. Non occorre scrivere la policy da sé, e quando AWS aggiorna la policy come appropriato per supportare nuovi servizi, si ottengono automaticamente e immediatamente i vantaggi dell'aggiornamento. Puoi vedere l'elenco delle policy gestite da AWS nella pagina Policies (Policy)sulla console IAM. Utilizza il menu a discesa Filter policies (Filtra policy) per selezionare AWS managed (Gestito da).

Puoi utilizzare le seguenti policy gestite per concedere autorizzazioni a utenti e ruoli della tua organizzazione.

Nome policy	Descrizione	ARN
AWSOrganizationsFullAccess	Fornisce tutte le autorizzazioni necessarie per creare e amministrare completamente un'organizzazione. Il contenuto di questa dichiarazione di policy è riportato nel frammento seguente:	arn:aws:iam: :aws:policy/AWSOrganizationsFullAccess

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSOrganizationsFullAccess",
            "Effect": "Allow",
            "Action": "organizations:*",
            "Resource": "*"
        },
        {
            "Sid": "AWSOrganizationsFullAccessAccount",
            "Effect": "Allow",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact",
                "account:GetAlternateContact",
                "account:GetContactInformation",
                "account:PutContactInformation",
                "account:ListRegions",
                "account:EnableRegion",
                "account:DisableRegion"
```

Nome policy	Descrizione	ARN

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "AWSOrgan
izationsFullAccessCreateSLR
",
            "Effect": "Allow",
            "Action":
 "iam:CreateServiceLinkedRol
e",
            "Resource": "*",
            "Condition": {
                "StringEq
uals": {
                    "iam:AWSS
erviceName": "organiza
tions.amazonaws.com"
                }
            }
        }
    ]
}
```

Nome policy	Descrizione	ARN
AWSOrganizationsReadOnlyAccess	Consente l'accesso in sola lettura alle informazioni sull'organizzazione. Non consente all'utente di apportare modifiche. Il contenuto di questa dichiarazione di policy è riportato nel frammento seguente:	arn:aws:iam: :aws:policy/AWSOrganizationsReadOnlyAccess

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "AWSOrganizationsReadOnly",
         "Effect":"Allow",
         "Action":[
            "organizations:Describe*",
            "organizations:List*"
         ],
         "Resource": "*"
      },
      {
         "Sid": "AWSOrganizationsReadOnlyAccount",
         "Effect":"Allow",
         "Action":[
            "account:GetAlternateContact",
            "account:GetContactInformation",
            "account:ListRegions"
         ],
         "Resource": "*"
      }
   ]
}
```

Aggiornamenti alle policy gestite da AWS di Organizations

La seguente tabella fornisce dettagli sugli aggiornamenti alle policy gestite da AWS da quando questo servizio ha iniziato a tenere traccia delle modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivi il feed RSS nella pagina della cronologia dei documenti di AWS Organizations.

Modifica	Descrizione	Data
AWSOrganizationsFullAccess— aggiornato per includere elementi che descrivono la dichiarazione politica. `Sid`	Organizations ha aggiunto `Sid` elementi per la policy `AWSOrganizationsFullAccess` gestita.	6 febbraio 2024
AWSOrganizationsReadOnlyAccess— aggiornato per includere `Sid` elementi che descrivono la dichiarazione politica.	Organizations ha aggiunto `Sid` elementi per la policy `AWSOrganizationsReadOnlyAccess` gestita.	6 febbraio 2024
AWSOrganizationsFullAccess— aggiornato per consentire le autorizzazioni API dell'account necessarie per l'attivazione o la disabilitazione Regioni AWS tramite la console Organizations.	Organizations ha aggiunto l'operazione `account:ListRegions`, `account:EnableRegion` e `account:DisableRegion` alla policy per consentire l'accesso in scrittura per abilitare o disabilitare le regioni per un account.	22 dicembre 2022
AWSOrganizationsReadOnlyAccess— aggiornato per consentire le autorizzazioni API dell'account necessarie per l'elenco Regioni AWS tramite la console Organizations.	Organizations ha aggiunto l'operazione `account:ListRegions` alla policy per consentire l'accesso per visualizzare le regioni di un account.	22 dicembre 2022
AWSOrganizationsFullAccess— aggiornato per consentire le autorizzazioni API dell'account necessarie per aggiungere o	Organizations ha aggiunto l'operazione `account:GetContactInformation` e `account:PutContactInformation` alla policy per consentire l'accesso in	21 ottobre 2022

Modifica	Descrizione	Data
modificare i contatti dell'account tramite la console Organizations.	scrittura e modificare i contatti di un account.	
AWSOrganizationsReadOnlyAccess— aggiornato per consentire le autorizzazioni API dell'account necessarie per visualizzare i contatti dell'account tramite la console Organizations.	Organizations ha aggiunto l'operazione `account:GetContactInformation` alla policy per consentire l'accesso per visualizzare i contatti di un account.	21 ottobre 2022
AWSOrganizationsFullAccess— aggiornato per consentire la creazione di un'organizzazione.	Organizations ha aggiunto l'autorizzazione `CreateServiceLinkedRole` alla policy per abilitare la creazione del ruolo collegato ai servizi richiesto per creare un'organizzazione. L'autorizzazione è limitata alla creazione di un ruolo che può essere utilizzato solo dal servizio `organizations.amazonaws.com` .	24 agosto 2022
AWSOrganizationsFullAccess— aggiornato per consentire le autorizzazioni API dell'account necessarie per aggiungere, modificare o eliminare contatti alternativi all'account tramite la console Organizations.	Organizations ha aggiunto le operazioni `account:GetAlternateContact` , `account:DeleteAlternateContact` , `account:PutAlternateContact` alla policy per consentire l'accesso in scrittura e modificare i contatti alternativi di un account.	7 febbraio 2022

Modifica	Descrizione	Data
AWSOrganizationsReadOnlyAccess— aggiornato per consentire le autorizzazioni API dell'account necessarie per visualizzare i contatti alternativi dell'account tramite la console Organizations.	Organizations ha aggiunto l'operazione `account:GetAlternateContact` alla policy per consentire l'accesso per visualizzare i contatti alternativi di un account.	7 febbraio 2022

Policy di controllo dei servizi gestite da AWS Organizations

Le policy di controllo dei servizi (SCP) sono simili alle policy di autorizzazione IAM, ma sono una caratteristica di AWS Organizations piuttosto che di IAM. È possibile utilizzare le SCP per specificare le autorizzazioni massime per le entità interessate. Puoi collegare le SCP alle root, alle unità organizzative (UO) o agli account nella tua organizzazione. Puoi creare le tue policy oppure utilizzare quelle definite da IAM. Puoi consultare l'elenco delle policy della tua organizzazione nella pagina Policies (Policy) della console Organizations.

> **Important**
>
> Ogni root, UO e account deve avere almeno una SCP sempre collegata.

Nome policy	Descrizione	ARN
• Completo AWSAccess	Concede all'account di gestione AWS Organizations l'accesso agli account membri.	arn:aws:organizations: :aws:policy/service_control_policy/p-FullAWSAccess

Risoluzione dei problemi di AWS Organizations

Se si verificano dei problemi durante l'utilizzo di AWS Organizations, consulta gli argomenti in questa sezione.

Argomenti

Risoluzione dei problemi generali

Utilizzare le informazioni di seguito per diagnosticare e risolvere i problemi relativi all'accesso negato e altri problemi comuni che possono verificarsi durante l'utilizzo di AWS Organizations.

Argomenti

Visualizzo un messaggio di accesso negato quando effettuo una richiesta a AWS Organizations.

- Verifica di disporre delle autorizzazioni necessarie per chiamare l'operazione e le risorse richieste. Un amministratore deve concedere le autorizzazioni collegando una policy IAM al tuo utente, gruppo o ruolo. Se le dichiarazioni di policy che concedono tali autorizzazioni includono eventuali condizioni, ad esempio limitazioni relative a indirizzo IP o ora del giorno, sarà inoltre necessario che tali requisiti siano soddisfatti, quando invii la richiesta. Per informazioni sulla visualizzazione o sulla modifica delle policy per un utente, un gruppo o un ruolo, consulta la sezione Utilizzo delle policy nella Guida per l'utente IAM.
- Se si stanno firmando manualmente richieste API (senza utilizzare gli AWS SDK), verificare di aver firmato correttamente la richiesta.

Visualizzo un messaggio di accesso negato quando effettuo una richiesta con credenziali di sicurezza provvisorie.

- Verifica che l'utente o il ruolo utilizzato per effettuare la richiesta disponga delle autorizzazioni corrette. Le autorizzazioni per le credenziali di sicurezza provvisorie sono derivate da un ruolo o un utente . Le autorizzazioni sono pertanto limitate a quelle concesse al ruolo o all'utente . Per ulteriori informazioni su come sono determinate le autorizzazioni per le credenziali di sicurezza provvisorie, consulta Controllo delle autorizzazioni per le credenziali di sicurezza provvisorie nella Guida per l'utente di IAM.
- Verificare che le richieste vengano firmate correttamente e che il formato della richiesta sia valido. Per ulteriori informazioni, consulta la documentazione del kit di strumenti dell'SDK scelto. In alternativa, consulta Utilizzo di credenziali di sicurezza provvisorie per richiedere l'accesso alle risorse AWS nella Guida per l'utente di IAM.
- Verifica che le credenziali di sicurezza provvisorie non siano scadute. Per ulteriori informazioni, consulta Richiesta di credenziali di sicurezza provvisorie nella Guida per l'utente di IAM.

Visualizzo un messaggio di accesso negato quando provo a lasciare un'organizzazione come account membro, oppure quando cerco di rimuovere un account membro come account di gestione

- È possibile rimuovere un account membro solo dopo avere abilitato l'accesso dell'utente IAM per la fatturazione nell'account membro. Per ulteriori informazioni, consulta Attivazione dell'accesso alla console di gestione fatturazione e costi nella Guida per l'utente di AWS Billing.
- È possibile rimuovere un account dall'organizzazione solo se l'account dispone delle informazioni richieste per operare come account standalone. Quando si crea un account in un'organizzazione utilizzando la console, le API o i comandi di AWS CLI di AWS Organizations, queste informazioni non vengono raccolte automaticamente. Se si desidera rendere standalone un account, è necessario accettare il Contratto clienti AWS, scegliere un piano di supporto, fornire e verificare le informazioni di contatto richieste e fornire un metodo di pagamento corrente. AWS utilizza il metodo di pagamento per addebitare le attività di AWS fatturabili (non il piano gratuito AWS) effettuate durante il periodo in cui l'account non era collegato a un'organizzazione. Per ulteriori informazioni, consulta Abbandono di un'organizzazione da un account membro.

Visualizzo un messaggio di "quota superata" quando cerco di aggiungere un account alla mia organizzazione

Esiste un numero massimo di account di cui è possibile disporre in un'organizzazione. Rientrano nella quota anche gli account eliminati o chiusi.

In questo calcolo relativo al numero massimo di account rientrano anche gli inviti a unirsi all'organizzazione. Il conteggio viene annullato se l'account invitato rifiuta, l'account di gestione annulla l'invito o l'invito scade.

- Prima di chiudere o eliminare un Account AWS, rimuovilo dall'organizzazione in modo tale che non venga più conteggiato nella quota.
- Per ulteriori informazioni su come richiedere un aumento delle quote, consulta Valori massimi e minimi.

Mentre aggiungo o rimuovo account visualizzo un messaggio che riporta come questa operazione richieda un periodo di attesa

Alcune operazioni richiedono un periodo di attesa. Ad esempio, non è possibile rimuovere immediatamente gli account appena creati. Prova a ripetere l'operazione dopo qualche giorno. Se riscontri problemi con le quote dell'account durante l'aggiunta e la rimozione degli account, consulta Valori massimi e minimi per informazioni su come richiedere un aumento della quota.

Quando cerco di aggiungere un account alla mia organizzazione visualizzo un messaggio, il quale riporta che l'inizializzazione dell'organizzazione è in corso

Se si riceve questo errore ed è trascorsa più di un'ora dal momento in cui stata creata l'organizzazione, contattare AWS Support.

Ricevo un messaggio "Gli inviti sono disabilitati" quando provo ad invitare un account all'organizzazione.

Ciò si verifica quando si abilitano tutte le funzionalità nell'organizzazione. Questa operazione può richiedere del tempo e richiede che tutti gli account membri rispondano. Fino al completamento dell'operazione, non è possibile invitare nuovi account a unirsi all'organizzazione.

Le modifiche apportate non sono sempre immediatamente visibili

Poiché AWS Organizations è un servizio a cui si accede da computer in data center presenti in tutto il mondo, utilizza un modello di elaborazione distribuito denominato consistenza finale. Qualsiasi modifica effettuata su AWS Organizations impiega del tempo affinché risulti visibile da tutti gli endpoint possibili. Alcuni dei ritardi sono dovuti al tempo necessario per inviare i dati da un server all'altro o da una zona di replica all'altra. AWS Organizations utilizza inoltre sistemi di caching per migliorare le prestazioni ed è possibile che questo aumenti ulteriormente il tempo richiesto in quanto la modifica potrebbe risultare visibile solo dopo il timeout dei dati memorizzati nella cache.

Progetta le tue applicazioni globali per verificare questi potenziali ritardi e per assicurarti che funzionino come previsto, anche quando una modifica apportata in una posizione non è immediatamente visibile in un'altra.

Per ulteriori informazioni sull'impatto di questo problema su alcuni altri servizi AWS, consulta le risorse seguenti:

- Gestione della consistenza dei dati nella Guida per gli sviluppatori di Amazon Redshift Database
- Modello di consistenza dati di Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service
- Post relativo a come garantire la consistenza quando si utilizzano Amazon S3 e Amazon Elastic MapReduce (EMR) per flussi di lavoro ETL nel blog dei Big Data AWS.
- Consistenza finale di EC2 nella documentazione di riferimento delle API di Amazon EC2.

Risoluzione dei problemi relativi alle policy AWS Organizations

Utilizza le informazioni di seguito per diagnosticare e risolvere errori comuni che si verificano nelle policy di AWS Organizations.

Policy di controllo dei servizi

Le policy di controllo dei servizi (SCP) su AWS Organizations sono simili alle policy IAM e condividono una sintassi comune. Questa sintassi inizia con le regole di JavaScript Object Notation (JSON). JSON descrive un oggetto con coppie di nomi e valori che costituiscono l'oggetto. La grammatica delle policy IAM si basa sulla definizione di nomi e valori che abbiano significato (e che possano essere compresi) dai servizi AWS che utilizzano le policy per concedere le autorizzazioni.

AWS Organizations utilizza un sottoinsieme della sintassi e della grammatica di IAM. Per informazioni dettagliate, consulta Sintassi delle SCP.

Errori di policy comuni

- Più di un oggetto della policy
- Più di un elemento Statement
- Il documento della policy supera le dimensioni massime

Più di un oggetto della policy

Un'SCP deve essere costituita da un solo oggetto JSON. È possibile denotare un oggetto racchiudendolo tra parentesi graffe { }. Sebbene sia possibile nidificare altri oggetti all'interno di un oggetto JSON incorporando ulteriori parentesi graffe { } all'interno della coppia esterna, una policy può contenere solo una coppia più esterna di parentesi graffe { }. L'esempio seguente è sbagliato perché contiene due oggetti al livello superiore (evidenziati in *rosso*):

```
{
```

```
  "Version": "2012-10-17",
  "Statement":
  {
     "Effect":"Allow",
     "Action":"ec2:Describe*",
     "Resource":"*"
  }
}
{
  "Statement": {
     "Effect": "Deny",
     "Action": "s3:*",
     "Resource": "*"
  }
}
```

Tuttavia, è possibile soddisfare l'intenzione dell'esempio precedente utilizzando una corretta grammatica della policy. Anziché includere due oggetti di policy completi, ciascuno con il proprio elemento `Statement`, è possibile combinare i due blocchi in un singolo elemento `Statement`. L'elemento `Statement` dispone di una matrice di due oggetti come valore, come mostrato nell'esempio seguente:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":" *"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

In questo esempio non è possibile comprimere ulteriormente l'istruzione `Statement` con un altro elemento, perché i due elementi hanno effetti diversi. Generalmente, è possibile combinare le istruzioni solo quando gli elementi `Effect` e `Resource` di ogni istruzione sono identici.

Più di un elemento Statement

Questo errore potrebbe apparentemente sembrare una variazione dell'errore nella sezione precedente. Tuttavia, sintatticamente si tratta di un altro tipo di errore. L'esempio seguente include un solo oggetto della policy, come indicato dalla singola coppia di parentesi graffe { } al livello più alto. Tuttavia, quell'oggetto contiene due elementi `Statement` al suo interno.

Una SCP deve contenere solo un elemento `Statement` che includa il nome (`Statement`), che appare sulla sinistra di una colonna, seguito dal rispettivo valore sulla destra. Il valore di un elemento `Statement` deve essere un oggetto, contrassegnato da parentesi graffe {}, che contiene un elemento `Effect`, un elemento `Action` e un elemento `Resource`. L'esempio seguente è sbagliato perché contiene due elementi `Statement` nell'oggetto della policy:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "ec2:Describe*",
    "Resource": "*"
  },
  "Statement": {
    "Effect": "Deny",
    "Action": "s3:*",
    "Resource": "*"
  }
}
```

Poiché un oggetto del valore può essere una matrice di oggetti a valore multiplo, è possibile risolvere questo problema combinando i due elementi `Statement` in un unico elemento con una matrice di oggetto, come riportato nell'esempio seguente:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":"*"
    },
    {
      "Effect": "Deny",
```

```
      "Action": "s3:*",
      "Resource": "*"
    }
 ]
}
```

Il valore dell'elemento `Statement` è una matrice di oggetti. La matrice nell'esempio è costituita da due oggetti, ognuno dei quali è un valore corretto di un elemento `Statement`. Ogni oggetto nella matrice è separato da virgole.

Il documento della policy supera le dimensioni massime

La dimensione massima di un documento SCP è 5.120 caratteri. Questa dimensione massima include tutti i caratteri, incluso lo spazio vuoto. Per ridurre la dimensione dell'SCP è possibile rimuovere tutti gli spazi vuoti (come spazi e interruzioni di riga) che sono al di fuori delle virgolette.

Chiamata dell'API tramite richieste di query HTTP

Questa sezione contiene informazioni generali sull'uso dell'API Query per AWS Organizations. Per ulteriori informazioni sulle operazioni delle API e sugli errori, consulta la documentazione di riferimento delle API di AWS Organizations.

> **Note**
>
> Invece di effettuare chiamate dirette all'API Query di AWS Organizations puoi usare uno degli SDK AWS. Gli SDK AWS sono costituiti da librerie e codice di esempio per diversi linguaggi di programmazione e piattaforme (Java, Ruby, .NET, iOS, Android e altri ancora). Gli SDK rappresentano un sistema molto comodo per creare un accesso programmatico a AWS Organizations e AWS. Ad esempio, gli SDK si occupano di attività quali la firma crittografica delle richieste, la gestione degli errori e la ripetizione automatica delle richieste. Per ulteriori informazioni sugli SDK AWS, inclusi i dettagli su come scaricarli e installarli, consulta Strumenti per Amazon Web Services.

L'API Query per AWS Organizations permette di chiamare operazioni del servizio. Le richieste dell'API Query sono richieste HTTPS che devono contenere un parametro `Action` per indicare l'operazione da eseguire. AWS Organizations supporta richieste GET e POST per tutte le operazioni. 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. Benché questo limite dipenda dal browser, un limite tipico è 2048 byte. Di conseguenza, per le richieste API Query che richiedono dimensioni maggiori, devi usare una richiesta POST.

La risposta è un documento XML. Per ulteriori informazioni sulla risposta, consulta le pagine delle singole operazioni nella documentazione di riferimento delle API di AWS Organizations.

Argomenti

Endpoints

AWS Organizations dispone di un singolo endpoint API globale ospitato nella Regione Stati Uniti orientali (Virginia settentrionale).

Per ulteriori informazioni sugli AWS endpoint e le aree per tutti i servizi, vedere Endpoint regionali nel. Riferimenti generali di AWS

HTTPS obbligatorio

Poiché l'API Query restituisce informazioni sensibili, ad esempio le credenziali di sicurezza, devi usare HTTPS per crittografare tutte le richieste API.

Firma delle richieste API AWS Organizations

Le richieste devono essere firmate usando un ID chiave di accesso e una Secret Access Key. Sconsigliamo vivamente di usare le credenziali Utente root dell'account AWS per le attività quotidiane con AWS Organizations. È possibile utilizzare le credenziali di un utente o un ruolo.

Per firmare le richieste API, devi usare AWS Signature Version 4. Per ulteriori informazioni sull'utilizzo di Signature Version 4, consulta Firma delle richieste API AWS nella Guida per l'utente di IAM.

AWS Organizations non supporta le versioni precedenti, ad esempio Signature Version 2.

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'uso del servizio IAM per semplificare la protezione delle risorse AWS, incluse quelle in AWS Organizations
- Credenziali di sicurezza temporanee in IAM: descrive come creare e usare credenziali di sicurezza temporanee.

Cronologia dei documenti per AWS Organizations

La tabella seguente descrive i principali aggiornamenti della documentazione per AWS Organizations.

- Versione API: 28-11-2016

Modifica	Descrizione	Data
Dichiarazioni politiche aggiornate	Aggiunti nuovi `Sid` elementi alle dichiarazioni politiche AWS Organizations gestite.	6 febbraio 2024
Nuovo argomento relativo all'account di gestione chiusa	Sono stati aggiunti collegamenti a considerazioni e passaggi dettagliati che spiegano come chiudere un account di gestione.	1 febbraio 2024
Best practice aggiornate	Sono state aggiunte nuove informazioni alla sezione delle best practice per facilitare l'allineamento con le best practice IAM.	12 giugno 2023
Politiche aggiornate AWSOrganizationsFullAccess e AWSOrganizationsReadOnlyAccess gestite	Entrambe le policy gestite sono state aggiornate per consentire l'accesso in scrittura o lettura ai contatti per gli account.	21 ottobre 2022
È stata aggiornata la politica AWSOrganizationsFullAccess gestita	La policy gestita è stata aggiornata in modo da consentire la creazione di un'organizzazione aggiungendo l'autorizzazione necessaria per creare il ruolo collegato ai	24 agosto 2022

	servizi necessario a una nuova organizzazione.	
Le organizzazioni chiudono la capacità dell'account dalla console AWS Organizations	I principali nell'account di gestione possono chiudere gli account membri dalla console AWS Organizations e proteggerli dalla chiusura accidentale utilizzando le policy IAM.	29 marzo 2022
Annuncio aggiornato per aggiornare i contatti alternativi con la console AWS Organizations	Organizations adesso consente di aggiornare i contatti alternativi per gli account all'interno dell'organizzazione utilizzando la console AWS Organizations. Annunciare nuove funzionalità e fare riferimento a Riferimento per la gestione degli account per le istruzioni.	8 febbraio 2022
Aggiornamenti delle policy gestite da Organizations - Aggiornamento a una policy esistente	Sono state aggiornate AWSOrganizationsFullAccess e AWSOrganizationsReadOnlyAccess gestite le politiche per consentire le autorizzazioni API dell'account necessarie per aggiornare o visualizzare i contatti alternativi dell'account tramite la AWS Organizations console.	7 febbraio 2022

Integrazione delle organizzazioni con Amazon DevOps Guru	Puoi integrare Amazon DevOps Guru con AWS Organizations per monitorare lo stato delle applicazioni in modo olistico su tutti gli account della tua organizzazione e ottenere informazioni dettagliate.	3 gennaio 2022
Integrazione di Organizations con Amazon Detective	È possibile integrare Amazon Detective con AWS Organizations per garantire che il grafico del comportamento di Detective fornisca visibilità sull'attività per tutti gli account dell'organizzazione.	16 dicembre 2021
L'integrazione di Organizations con AWS Config ora supporta l'aggregazione di dati da più account e Regioni.	Puoi utilizzare un account di amministratore delegato per aggregare i dati di configurazione e conformità delle risorse provenienti da tutti gli account membri dell'organizzazione. Per ulteriori informazioni, consulta Aggregazione di dati da più account e Regioni nella Guida per gli sviluppatori di AWS Config.	16 giugno 2021

L'integrazione di Organizations con AWS Firewall Manager ora include il supporto per un amministratore delegato	Ora puoi designare un account membro dell'organizzazione come amministratore di Firewall Manager per l'intera organizzazione. Ciò consente una migliore separazione delle autorizzazioni dall'account di gestione dell'organizzazione.	30 aprile 2021
Le policy di backup di Organizations ora supportano il backup continuo	Puoi utilizzare la funzionalità di backup continui di AWS Backup con le policy di backup dell'organizzazione.	10 marzo 2021
L'integrazione di Organizations con AWS CloudFormation StackSets ora include il supporto per un amministratore delegato	Ora puoi designare un account membro della tua organizzazione come AWS CloudFormation StackSets amministratore dell'intera organizzazione. Ciò consente una migliore separazione delle autorizzazioni dall'account di gestione dell'organizzazione.	18 febbraio 2021
Continua a invitare gli account mentre abiliti tutte le funzionalità	AWS ha aggiornato il processo di abilitazione di tutte le caratteristiche in un'organizzazione. Ora puoi continuare a invitare altri account a unirsi all'organizzazione mentre attendi che gli account attuali rispondano ai loro inviti.	3 febbraio 2021

Introduce la versione 2.0 della console di AWS Organizations	AWS ha introdotto una nuova versione della console AWS. Tutta la documentazione è stata aggiornata in modo da riflettere il nuovo modo di eseguire le attività.	21 gennaio 2021
Organizations ora supporta l'integrazione con Marketplace AWS	Ora puoi abilitare Marketplace AWS per condividere con maggiore facilità le licenze software in tutti gli account dell'organizzazione.	3 dicembre 2020
Organizations ora supporta l'integrazione con Amazon S3 Lens	Amazon S3 Lens supporta sia l'accesso attendibile sia l'amministratore delegato con Organizations. Per informazioni dettagliate, consulta Amazon S3 Storage Lens nella Guida per l'utente di Amazon Simple Storage Service.	18 novembre 2020
Copie di backup tra account	Quando si utilizzano policy di backup per eseguire il backup delle risorse nell'organizzazione, ora è possibile archiviare copie del backup in altri Account AWS all'interno dell'organizzazione.	18 novembre 2020
Regioni AWS in Cina ora supporta AWS Resource Access Manager come servizio attendibile di Organizations	Ora puoi utilizzare le caratteristiche AWS RAM che si integrano con Organizations come servizio attendibile quando utilizzi Organizzazioni e AWS RAM in Cina.	18 novembre 2020

Organizations ora supporta l'integrazione con AWS Security Hub	Puoi abilitare Security Hub in tutti gli account dell'organizzazione e designare uno degli account membri dell'organizzazione come account di amministratore delegato per Security Hub.	12 novembre 2020
Rinominato l'account principale	AWS Organizations ha cambiato il nome "account principale" in "account di gestione". Si tratta solo di un aggiornamento del nome, senza modifiche della funzionalità.	20 ottobre 2020
Nuovi sezione e argomenti relativi alle best practice	Aggiunta una nuova sezione sulle best practice per AWS Organizations. La nuova sezione include argomenti che illustrano le best practice per l'account di gestione e gli utenti root dell'account membro e per la gestione delle password.	6 ottobre 2020
Aggiunta la nuova sezione delle best practice e le prime due pagine	È disponibile una nuova sezione per gli argomenti che descrivono le best practice perAWS Organizations. Questo aggiornamento include un argomento per le best practice per l'account di gestione di un'organizzazione e un argomento per le best practice per gli account membri.	2 ottobre 2020

Le policy di backup delle Organizations ora supportano backup coerenti con le applicazioni nelle istanze EC2 di Windows utilizzando VSS (Volume Shadow Copy Service)	Le policy di backup supportano una nuova sezione `advanced_backup_settings `. La prima voce in questa nuova sezione è un'impostazione `ec2` chiamata `WindowsVSS` che puoi abilitare o disabilitare. Per informazioni dettagliate, consulta Creazione di un backup Windows abilitato per VSS nella Guida per gli sviluppatori di AWS Backup.	24 settembre 2020
Organizations: supporti tag-on-create e controllo degli accessi basato su tag	Puoi aggiungere i tag alle risorse di Organizations al momento della creazione della risorsa. Puoi utilizzare policy di tag per standardizzare l'utilizzo dei tag nelle risorse di Organizations. Puoi utilizzare le policy IAM per limitare l'accesso solo alle risorse che hanno le chiavi e i valori di tag specificati.	15 settembre 2020
Aggiunto AWS Health come servizio attendibile	Puoi aggregare gli eventi AWS Health tra gli account nell'organizzazione.	4 agosto 2020

Policy di rifiuto dei servizi di Intelligenza Artificiale (IA)	Puoi usare le policy di rifiuto dei servizi di IA per controllare se i servizi di IA AWS possono memorizzare e utilizzare i contenuti dei clienti elaborati da tali servizi (contenuti IA) per lo sviluppo e il miglioramento continuo di servizi e tecnologie AWS di intelligenza artificiale.	8 luglio 2020
Aggiunte policy di backup e integrazione con AWS Backup	Puoi utilizzare policy di backup per creare e applicare policy di backup in tutti gli account dell'organizzazione.	24 giugno 2020
Supporta l'amministrazione delegata per IAM Access Analyzer	Consente di delegare l'accesso amministrativo per Access Analyzer nell'orga nizzazione a un account membro designato.	30 marzo 2020
Integrazione con AWS CloudFormation StackSets	È possibile creare un set di stack gestito dal servizio per distribuire le istanze dello stack agli account gestiti da AWS Organizations.	11 febbraio 2020
Integrazione con Compute Optimizer	Compute Optimizer è stato aggiunto come servizio che può funzionare con gli account nell'organizzazione.	4 febbraio 2020
Policy di tag	Puoi utilizzare le policy di tag per semplificare la standardi zzazione dei tag tra le risorse degli account dell'orga nizzazione.	26 novembre 2019

Integrazione con Systems Manager	Puoi sincronizzare i dati delle operazioni tra tutti gli Account AWS dell'organizzazione in Systems Manager Explorer.	26 novembre 2019
Leggi: PrincipalOrgPaths	La nuova chiave di condizion e globale controlla il percorso AWS Organizations per l'utente IAM, il ruolo IAM o l'utente root dell'Account AWS che effettua la richiesta.	20 novembre 2019
Integrazione con le regole di AWS Config	È possibile usare le operazioni API di AWS Config per gestire le regole AWS Config per tutti gli Account AWS della tua organizzazione.	8 luglio 2019
Nuovo servizio per l'accesso sicuro	Service Quotas è stato aggiunto come servizio che può funzionare con gli account nell'organizzazione.	24 giugno 2019
Integrazione con AWS Control Tower	AWS Control Tower è stato aggiunto come servizio che può funzionare con gli account nell'organizzazione.	24 giugno 2019
Integrazione con AWS Identity and Access Management	IAM fornisce dati sull'ultimo accesso al servizio per le entità dell'organizzazione (root dell'organizzazione, UO e account). È possibile utilizzar e questi dati per limitare l'accesso solo ai servizi AWS di cui hai bisogno.	20 giugno 2019

Applicare tag agli account	È possibile applicare e rimuovere tag dagli account dell'organizzazione e visualizzare i tag in un account nella tua organizzazione.	6 giugno 2019
Risorse, condizioni, e l'elemento `NotAction` nelle policy di controllo dei servizi (SCP)	È ora possibile specificare le risorse, le condizioni, e l'elemento `NotAction` nelle policy SCP per negare l'accesso tra gli account nell'organizzazione o nell'unità organizzativa.	25 marzo 2019
Nuovi servizi per l'accesso sicuro	AWS License Manager e Service Catalog sono stati aggiunti come servizi che possono funzionare con gli account nell'organizzazione.	21 dicembre 2018
Nuovi servizi per l'accesso sicuro	AWS CloudTrail e AWS RAM sono stati aggiunti come servizi che possono funzionare con gli account nell'organizzazione.	4 dicembre 2018
Nuovo servizio per l'accesso sicuro	AWS Directory Service è stato aggiunto come servizio che può funzionare con gli account nell'organizzazione.	25 settembre 2018
Verifica dell'indirizzo e-mail	È necessario dimostrare di essere il proprietario dell'indirizzo e-mail associato all'account di gestione, prima di poter invitare gli account esistenti nell'organizzazione.	20 settembre 2018

CreateAccount notifiche	`CreateAccount` le notifiche vengono pubblicate nei CloudTrail registri dell'account di gestione.	28 giugno 2018
Nuovo servizio per l'accesso sicuro	AWS Artifact è stato aggiunto come servizio che può funzionare con gli account nell'organizzazione.	20 giugno 2018
Nuovi servizi per l'accesso sicuro	AWS Config e AWS Firewall Manager sono stati aggiunti come servizi che possono funzionare con gli account nell'organizzazione.	18 aprile 2018
Accesso sicuro ai servizi	Ora è possibile abilitare o disabilitare l'accesso di determinati servizi AWS affinché funzionino negli account nell'organizzazion e. IAM Identity Center è il servizio di affidabilità supportat o iniziale.	29 marzo 2018
Ora rimozione dell'account self-service	Ora è possibile rimuovere gli account creati da AWS Organizations senza contattar e AWS Support.	19 dicembre 2017
Aggiunto supporto per il nuovo servizio AWS IAM Identity Center	AWS Organizations ora supporta l'integrazione con AWS IAM Identity Center (IAM Identity Center).	7 dicembre 2017

Aggiunta da AWS di un ruolo collegato al servizio a tutti gli account dell'organizzazione	Un ruolo collegato al servizio denominato `AWSServiceRoleForOrganizations` viene aggiunto a tutti gli account in un'organizzazione per consentire l'integrazione tra AWS Organizations e altri servizi AWS.	11 ottobre 2017
Possibilità di rimuovere gli account creati	I clienti possono ora rimuovere gli account creati dalla propria organizzazione, con l'aiuto di AWS Support.	15 giugno 2017
Avvio del servizio	La versione iniziale della documentazione AWS Organizations che ha accompagnato il lancio del nuovo servizio.	17 febbraio 2017

Glossario per AWS

Per la terminologia AWS più recente, consultare il glossario AWS nella documentazione di riferimento per Glossario AWS.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.