Guida per l'utente

AWS Organizations

AWS Organizations: Guida per l'utente

Table of Contents

Che cos'è AWS Organizations?

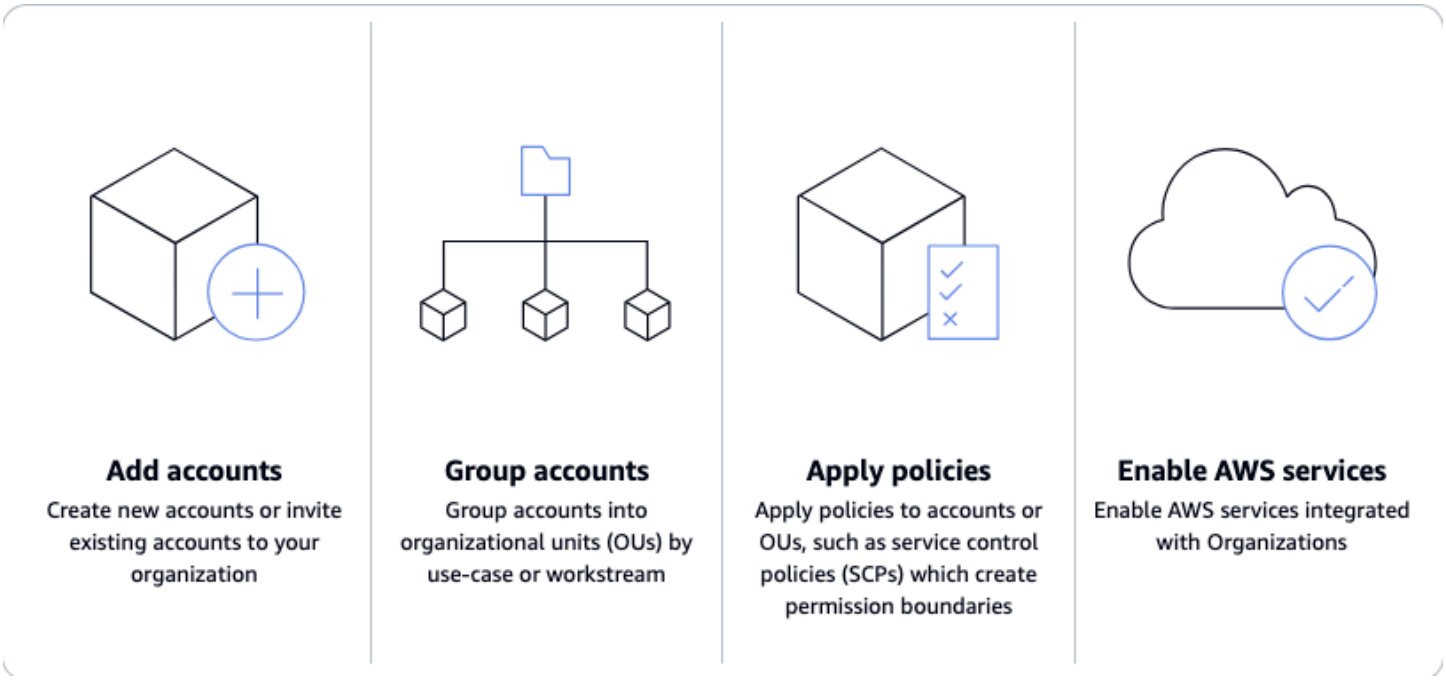
Gestisci centralmente il tuo ambiente man mano che ridimensioni AWS le tue risorse

AWS Organizations ti aiuta a gestire e governare centralmente il tuo ambiente man mano che cresci e scalerai AWS le tue risorse. Utilizzando Organizations, puoi creare account e allocare risorse, raggruppare account per organizzare i flussi di lavoro, applicare politiche di governance e semplificare la fatturazione utilizzando un unico metodo di pagamento per tutti i tuoi account.

Organizations è integrato con altri Servizi AWS in modo da poter definire configurazioni centrali, meccanismi di sicurezza, requisiti di audit e condivisione delle risorse tra gli account dell'organizzazione. Per ulteriori informazioni, consulta Utilizzo AWS Organizations con altri Servizi AWS.

Il diagramma seguente mostra una spiegazione di alto livello di come è possibile utilizzare: AWS Organizations

- Aggiungere account
- Account di gruppo
- Applica le politiche
- Abilita Servizi AWS.



Argomenti

Funzionalità per AWS Organizations

AWS Organizations offre le seguenti funzionalità:

Gestisci i tuoi Account AWS

> Account AWS sono limiti naturali in termini di autorizzazioni, sicurezza, costi e carichi di lavoro. L'utilizzo di un ambiente multi-account è una best practice consigliata per scalare l'ambiente cloud. Puoi semplificare la creazione di account creando nuovi account in modo programmatico utilizzando AWS Command Line Interface (AWS CLI) SDKs APIs, oppure e fornendo centralmente le risorse e le autorizzazioni consigliate a tali account con. AWS CloudFormation StackSets

Definisci e gestisci la tua organizzazione

> Quando crei nuovi account, puoi raggrupparli in unità organizzative (OUs) o gruppi di account che servono una singola applicazione o servizio. Applica le policy relative ai tag per classificare o tenere traccia delle risorse dell'organizzazione e fornisci un controllo degli accessi basato sugli attributi per utenti o applicazioni. Inoltre, puoi delegare la responsabilità del supporto Servizi AWS agli account in modo che gli utenti possano gestirli per conto dell'organizzazione.

Proteggi e monitora i tuoi account

> Puoi fornire centralmente strumenti e accessi al tuo team di sicurezza per gestire le esigenze di sicurezza per conto dell'organizzazione. Ad esempio, puoi fornire un accesso di sicurezza in sola lettura tra gli account, rilevare e mitigare le minacce con Amazon GuardDuty, esaminare l'accesso non intenzionale alle risorse con IAM Access Analyzer e proteggere i dati sensibili con Amazon Macie.

Controlla l'accesso e le autorizzazioni

Configura AWS IAM Identity Centerper fornire l'accesso Account AWS e le risorse tramite Active Directory e personalizza le autorizzazioni in base a ruoli lavorativi separati. Puoi anche applicare le politiche dell'organizzazione a utenti, account o OUs. Ad esempio, le politiche di controllo dei servizi (SCPs) consentono di controllare l'accesso a AWS risorse, servizi e regioni all'interno dell'organizzazione. Le politiche di controllo delle risorse (RCPs) consentono di impedire centralmente l'uso non intenzionale delle AWS risorse. Le politiche delle applicazioni di chat ti consentono di controllare l'accesso agli account della tua organizzazione da applicazioni di chat come Slack e Microsoft Teams.

Condividi le risorse tra gli account

Puoi condividere AWS risorse all'interno della tua organizzazione utilizzando AWS Resource Access Manager (AWS RAM). Ad esempio, puoi creare le tue sottoreti Amazon Virtual Private Cloud (Amazon VPC) una sola volta e condividerle all'interno dell'organizzazione. Puoi anche concordare centralmente le licenze software con AWS License Managere condividere un catalogo di servizi IT e prodotti personalizzati tra più account con. AWS Service Catalog

Verifica la conformità del tuo ambiente

Puoi eseguire l'attivazione AWS CloudTrailsu più account, il che crea un registro di tutte le attività nel tuo ambiente cloud che non può essere disattivato o modificato dagli account dei membri. Inoltre, puoi impostare politiche per applicare i backup alla cadenza specificata o definire le impostazioni di configurazione consigliate per le risorse tra diversi account e con AWS Backup. Regioni AWS AWS Config

Gestisci centralmente la fatturazione e i costi

Organizations fornisce un'unica fattura consolidata. Inoltre, è possibile visualizzare l'utilizzo delle risorse di tutti gli account e tenere traccia dei costi utilizzando AWS Cost Explorere ottimizzare l'utilizzo delle risorse di elaborazione utilizzando. AWS Compute Optimizer

Casi d'uso per AWS Organizations

Di seguito sono riportati alcuni casi d'uso per AWS Organizations:

Automatizza la creazione Account AWS e la categorizzazione dei carichi di lavoro

Puoi automatizzare la creazione di nuovi carichi di lavoro Account AWS per avviare rapidamente. Aggiungi gli account a gruppi definiti dall'utente per l'applicazione istantanea delle politiche di

sicurezza, le implementazioni di infrastrutture touchless e il controllo. Crea gruppi separati per classificare gli account di sviluppo e produzione e utilizzali AWS CloudFormation StackSetsper fornire servizi e autorizzazioni a ciascun gruppo.

Definisci e applica le politiche di audit e conformità

È possibile applicare politiche di controllo del servizio (SCPs) per garantire che gli utenti eseguano solo le azioni che soddisfano i requisiti di sicurezza e conformità. Crea un registro centrale di tutte le azioni eseguite nell'organizzazione utilizzando AWS CloudTrail. Visualizza e applica le configurazioni standard delle risorse tra account e Regioni AWS utilizzi. AWS Config Applica automaticamente backup regolari utilizzando. AWS Backup Utilizzalo AWS Control Towerper applicare regole di governance preconfezionate per la sicurezza, le operazioni e la conformità per i tuoi carichi di lavoro. AWS

Fornisci strumenti e accesso ai tuoi team di sicurezza incoraggiando al contempo lo sviluppo

Crea un gruppo di sicurezza e offrigli l'accesso in sola lettura a tutte le tue risorse per identificare e mitigare i problemi di sicurezza. Puoi consentire a quel gruppo di gestire Amazon GuardDuty in modo che possa monitorare e mitigare attivamente le minacce ai tuoi carichi di lavoro e IAM Access Analyzer per identificare rapidamente gli accessi non intenzionali alle tue risorse.

Condividi risorse comuni tra più account

Organizations semplifica la condivisione di risorse centrali critiche tra i tuoi account. Ad esempio, puoi condividere la tua centrale AWS Directory Service for Microsoft Active Directoryin modo che le applicazioni possano accedere al tuo archivio di identità centrale.

Condividi le risorse centrali critiche tra i tuoi account

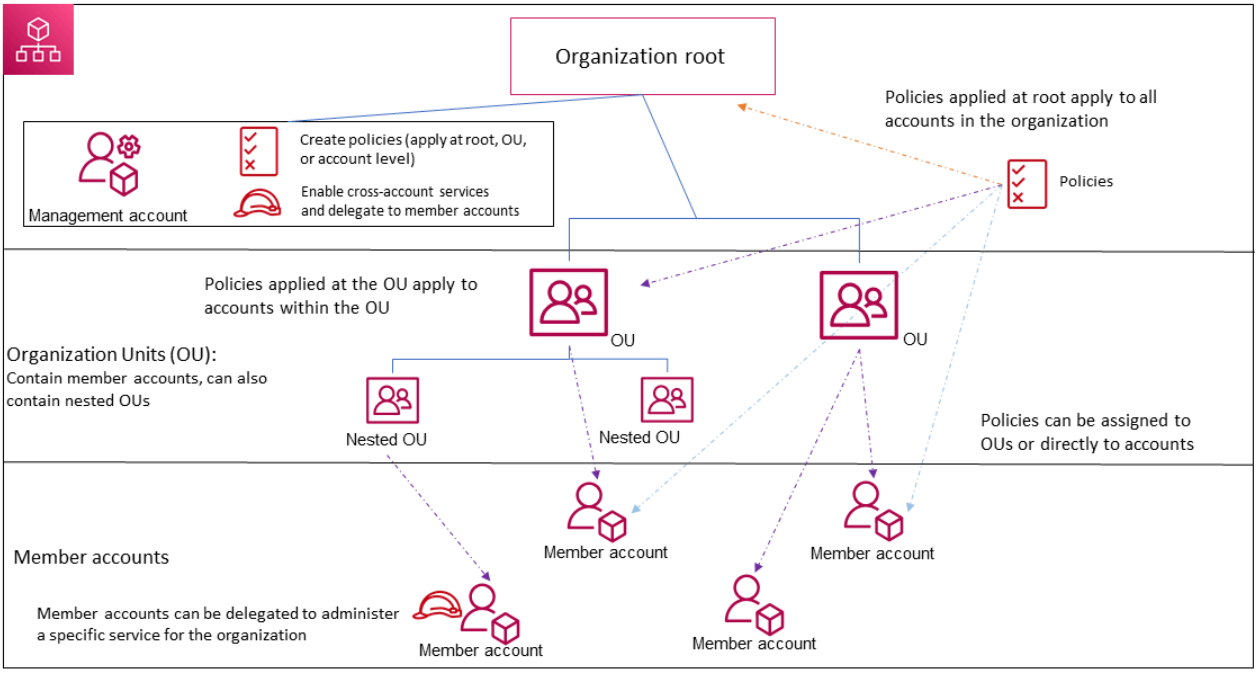
Condividi il tuo AWS Directory Service for Microsoft Active Directorycome archivio di identità centralizzato per le tue applicazioni. Utilizzalo AWS Service Catalogper condividere i servizi IT in account designati in modo che gli utenti possano scoprire e implementare rapidamente i servizi approvati. Assicurati che le risorse applicative vengano create nelle sottoreti Amazon Virtual Private Cloud (Amazon VPC) definendole centralmente una sola volta e condividendole all'interno dell'organizzazione utilizzando ().AWS Resource Access ManagerAWS RAM

Terminologia e concetti per AWS Organizations

Questo argomento spiega alcuni dei concetti chiave per AWS Organizations.

Il diagramma seguente mostra un'organizzazione composta da cinque account organizzati in quattro unità organizzative (OUs) sotto la radice. L'organizzazione dispone inoltre di diverse politiche collegate ad alcuni account OUs o direttamente agli account.

Per una descrizione di ciascuna di queste voci, fare riferimento alle definizioni in questo argomento.



Argomenti

- Set di caratteristiche disponibili
- Struttura dell'organizzazione
- Inviti e strette di mano
- Politiche organizzative

Set di caratteristiche disponibili

Tutte le funzionalità (consigliate)

Tutte le funzionalità è il set di funzionalità predefinito disponibile per AWS Organizations. È possibile impostare politiche e requisiti di configurazione centrali per un'intera organizzazione, creare autorizzazioni o funzionalità personalizzate all'interno dell'organizzazione, gestire e

organizzare gli account in un'unica fattura e delegare le responsabilità ad altri account per conto dell'organizzazione. È inoltre possibile utilizzare le integrazioni con altri Servizi AWS per definire configurazioni centrali, meccanismi di sicurezza, requisiti di controllo e condivisione delle risorse tra tutti gli account dei membri dell'organizzazione. Per ulteriori informazioni, consulta Utilizzo AWS Organizations con altri Servizi AWS.

La modalità Tutte le funzionalità offre tutte le funzionalità della fatturazione consolidata insieme alle funzionalità amministrative.

Fatturazione consolidata

La fatturazione consolidata è il set di funzionalità che fornisce funzionalità di fatturazione condivise, ma non include le funzionalità più avanzate di. AWS Organizations Ad esempio, non è possibile consentire l'integrazione di altri AWS servizi con l'organizzazione in modo che funzionino su tutti gli account dell'organizzazione o utilizzare policy per limitare le operazioni consentite a utenti e ruoli in account diversi.

Puoi abilitare tutte le funzionalità per un'organizzazione che originariamente supportava solo le funzionalità 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. Per ulteriori informazioni, consulta Abilitazione di tutte le funzionalità per un'organizzazione con AWS Organizations.

Struttura dell'organizzazione

Organizzazione

Un'organizzazione è un insieme di elementi Account AWSche è possibile gestire centralmente e organizzare in una struttura gerarchica ad albero con una radice nella parte superiore e unità organizzative annidate sotto la radice. Ogni account può trovarsi direttamente nella directory principale o collocato in uno dei punti della gerarchia. OUs

Ogni organizzazione è composta da:

- Un account di gestione
- Zero o più account membri
- Zero o più unità organizzative (OUs)
- Zero o più politiche.

Un'organizzazione ha la funzionalità determinata dall'insieme di caratteristiche che si abilita.

Root

Una radice amministrativa (root) è contenuta nell'account di gestione ed è il punto di partenza per l'organizzazione di Account AWS. La radice è il contenitore più in alto nella gerarchia dell'organizzazione. In base a questa radice, puoi creare unità organizzative (OUs) per raggruppare logicamente i tuoi account e organizzarli OUs in una gerarchia che meglio si adatti alle tue esigenze.

Se applichi una politica di gestione alla radice, questa si applica a tutte le unità organizzative (OUs) e agli account, incluso l'account di gestione dell'organizzazione.

Se si applica una politica di autorizzazione (ad esempio, una politica di controllo del servizio (SCP)), alla radice, questa si applica a tutte le unità organizzative (OUs) e agli account membri dell'organizzazione. Non si applica all'account di gestione dell'organizzazione.

> **Note**
>
> Puoi avere una sola radice. AWS Organizations crea automaticamente la radice per te quando crei un'organizzazione.

Unità organizzativa (UO)

Un'unità organizzativa (OU) è un gruppo Account AWSall'interno di un'organizzazione. Un'unità organizzativa può anche contenere altre unità che OUs consentono di creare una gerarchia. Ad esempio, è possibile raggruppare tutti gli account che appartengono allo stesso reparto in un'unità organizzativa dipartimentale. Allo stesso modo, è possibile raggruppare tutti gli account che eseguono servizi di sicurezza in un'unità organizzativa di sicurezza.

OUs sono utili quando è necessario applicare gli stessi controlli a un sottoinsieme di account dell'organizzazione. Il nesting OUs consente unità di gestione più piccole. Ad esempio, puoi creare OUs per ogni carico di lavoro, quindi crearne due annidate OUs in ogni unità organizzativa di carico di lavoro per dividere i carichi di lavoro di produzione da quelli di pre-produzione. Queste OUs ereditano le policy dall'unità organizzativa principale oltre a tutti i controlli assegnati direttamente all'unità organizzativa a livello di team. Includendo la radice e quella Account AWS creata nella parte inferiore OUs, la gerarchia può avere una profondità di cinque livelli.

Account AWS

An Account AWSè un contenitore per le tue AWS risorse. Crei e gestisci AWS le tue risorse in un unico Account AWS ambiente e Account AWS fornisce funzionalità amministrative per l'accesso e la fatturazione.

L'uso di più risorse Account AWS è una best practice per scalare l'ambiente, in quanto fornisce un limite di fatturazione per i costi, isola le risorse per motivi di sicurezza, offre flessibilità ai singoli utenti e ai team, oltre ad essere adattabile ai nuovi processi.

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

Esistono due tipi di account in un'organizzazione: un account singolo designato come account di gestione e uno o più account membro.

Gestione dell'account

Un account di gestione è l'account Account AWS che usi per creare la tua organizzazione. Dall'account di gestione, puoi effettuare le seguenti operazioni:

- Crea altri account nella tua organizzazione
- Invita e gestisci gli inviti affinché altri account entrino a far parte della tua organizzazione
- Designare account amministrativi delegati
- Rimuovi gli account dalla tua organizzazione
- Allega le politiche a entità quali radici, unità organizzative (OUs) o account all'interno dell'organizzazione
- Abilita l'integrazione con AWS i servizi supportati per fornire funzionalità di servizio a tutti gli account dell'organizzazione.

L'account di gestione è il proprietario finale dell'organizzazione e detiene il controllo finale sulle politiche di sicurezza, infrastruttura e finanza. Questo account ha la funzione di conto di pagamento ed è responsabile del pagamento di tutti gli addebiti maturati dai conti della sua organizzazione.

> **Note**
>
> Non è possibile modificare l'account dell'organizzazione utilizzato come account di gestione.

Account membro

Un account membro è un account Account AWS, diverso dall'account di gestione, che fa parte di un'organizzazione. Se sei un amministratore di un'organizzazione, puoi creare account membro nell'organizzazione e invitare gli account esistenti a unirsi all'organizzazione. Puoi anche applicare politiche agli account dei membri.

> **Note**
>
> Un account membro può appartenere a una sola organizzazione alla volta. È possibile designare gli account membro come account amministratore con delega.

Amministratore delegato

Consigliamo di utilizzare l'account di gestione e i relativi utenti e ruoli solo per le attività che devono essere eseguite 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 Organizations service control policies (SCPs) 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. 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 le organizzazioni: da questi account, è possibile gestire le politiche dell'organizzazione e allegare le politiche alle entità (radici o account) all'interno dell'organizzazione. OUs 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 AWS servizio: da questi account è possibile gestire i AWS servizi 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 Servizi AWS quel lavoro con Organizations

Inviti e strette di mano

Invito

Un invito è una richiesta effettuata dall'account di gestione di un'organizzazione a un altro account. Ad esempio, il processo di richiesta a un account indipendente di entrare a far parte di un'organizzazione è un invito.

Gli inviti vengono implementati come strette di mano. Gli handshake potrebbero non essere visibili quando utilizzi la console AWS Organizations . Ma se usi l' AWS Organizations API AWS CLI or, devi lavorare direttamente con le strette di mano.

Handshake

Una stretta di mano è lo scambio sicuro di informazioni tra due AWS account: un mittente e un destinatario.

Sono supportate le seguenti strette di mano:

- INVITO: invio di una stretta di mano a un account indipendente per consentirne l'ingresso nell'organizzazione del mittente.
- ENABLE_ALL_FEATURES: Handshake inviato agli account dei membri invitati per abilitare tutte le funzionalità per l'organizzazione.
- APPROVE_ALL_FEATURES: Stretta di mano inviata all'account di gestione quando tutti gli account dei membri invitati hanno approvato l'attivazione di tutte le funzionalità.

In genere è necessario interagire direttamente con gli handshake solo se si utilizza l' AWS Organizations API o strumenti da riga di comando come. AWS CLI

Politiche organizzative

Una politica è un «documento» con una o più istruzioni che definiscono i controlli che si desidera applicare a un gruppo di Account AWS. AWS Organizations supporta politiche di autorizzazione e politiche di gestione.

Policy di autorizzazione

Le politiche di autorizzazione consentono di gestire centralmente la sicurezza di Account AWS tutta l'organizzazione.

Policy di controllo dei servizi (SCP)

Una policy di controllo dei servizi è un tipo di policy che offre il controllo centralizzato sulle autorizzazioni massime disponibili per gli utenti IAM e i ruoli IAM in un'organizzazione.

Ciò significa che è SCPs necessario specificare i controlli incentrati sui principali. SCPs crea una barriera per le autorizzazioni o imposta dei limiti alle autorizzazioni massime disponibili per i responsabili nei tuoi account membro. Utilizzate un SCP quando desiderate applicare centralmente controlli di accesso coerenti ai responsabili della vostra organizzazione.

Ciò può includere la specificazione a quali servizi possono accedere gli utenti IAM e i ruoli IAM, a quali risorse possono accedere o le condizioni in base alle quali possono effettuare richieste (ad esempio, da regioni o reti specifiche). Per ulteriori informazioni, consulta SCPs.

Politica di controllo delle risorse (RCP)

Una politica di controllo delle risorse è un tipo di politica che offre il controllo centralizzato sulle autorizzazioni massime disponibili per le risorse in un'organizzazione.

Ciò significa che è RCPs necessario specificare controlli incentrati sulle risorse. RCPs crea una barriera di autorizzazioni, o imposta dei limiti, alle autorizzazioni massime disponibili per le risorse nei tuoi account membro. Utilizza un RCP quando desideri applicare centralmente controlli di accesso coerenti tra le risorse della tua organizzazione.

Ciò può includere la limitazione dell'accesso alle risorse in modo che possano accedervi solo le identità che appartengono all'organizzazione o la specificazione delle condizioni in base alle quali le identità esterne all'organizzazione possono accedere alle risorse. Per ulteriori informazioni, consulta RCPs.

Policy di gestione

Le politiche di gestione consentono di configurare e gestire centralmente Servizi AWS e le relative funzionalità all'interno dell'organizzazione.

Politica dichiarativa

Una politica dichiarativa è un tipo di politica che consente di dichiarare e applicare a livello centrale le configurazioni desiderate per un determinato ambiente su larga scala Servizio AWS all'interno dell'organizzazione. Una volta collegata, la configurazione viene sempre mantenuta quando il servizio aggiunge nuove funzionalità oppure APIs. per ulteriori informazioni, consulta la politica dichiarativa.

Policy di backup

Una policy di backup è un tipo di policy che consente di gestire e applicare centralmente i piani di backup alle AWS risorse degli account di un'organizzazione. Per ulteriori informazioni, consulta la politica di backup.

Policy di tag

Una politica sui tag è un tipo di politica che consente di standardizzare i tag allegati alle AWS risorse negli account di un'organizzazione. Per ulteriori informazioni, consulta la politica dei tag.

Politica sulle applicazioni di chat

Un criterio per le applicazioni di chat è un tipo di criterio che consente di controllare l'accesso agli account di un'organizzazione da applicazioni di chat come Slack e Microsoft Teams. Per ulteriori informazioni, consulta la politica delle applicazioni di chat.

Policy di rifiuto dei servizi di IA

Una politica di disattivazione dei servizi di intelligenza artificiale è un tipo di politica che consente di controllare la raccolta dei dati per i servizi di AWS intelligenza artificiale per tutti gli account di un'organizzazione. Per ulteriori informazioni, consulta la politica di disattivazione dei servizi AI.

Quote e limiti di servizio per AWS Organizations

Questo argomento descrive le quote e i limiti di servizio per 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 (OUs), delle radici e delle politiche:

- I nomi devono essere composti da caratteri Unicode.

- La lunghezza massima della stringa dei nomi varia in base all'oggetto. Per informazioni sul limite effettivo per ogni oggetto, consulta l'AWS Organizations API Reference e trova l'operazione API che crea l'oggetto, quindi guarda i dettagli del `Name` parametro di quell'operazione. Ad esempio: Account name (Nome account) oppure OU name (Nome UO).

Considerazioni

I codici delle quote di servizio potrebbero cambiare nel tempo a causa degli aggiornamenti. Ciò non influisce sui valori o sui nomi delle quote. Per trovare il codice di quota per una quota specifica, utilizza l'ListServiceQuotasoperazione e cerca la `QuotaCode` risposta nell'output relativo alla quota desiderata.

Valori massimi e minimi

Di seguito sono riportati i valori massimi predefiniti per le entità in AWS Organizations.

> **Note**
>
> Considerate le seguenti informazioni sulle AWS Organizations quote:
>
> - È possibile richiedere un aumento di alcuni di questi valori utilizzando il metodo Console Service Quotas.
> - AWS Organizations i limiti si applicano a livello di organizzazione, se non diversamente specificato. Molte quote si applicano solo alle azioni eseguite dall'account di AWS Organizations gestione.
> - AWS 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 a queste quote quando si utilizza la console Service Quotas, AWS CLI il o AWS un SDK.

Descrizione	Limite
Numero massimo predefinito di account	10 — Il numero massimo di default di account consentiti in un'organizzazione. Questa quota è regolabile e può essere aumentata utilizzando la console Service Quotas.

Descrizione	Limite
	Nota: solo l'account di gestione di un'organizzazione può inviare questa richiesta di aumento della quota. È possibile concedere aumenti del limite fino a 10.000 account in base alle qualifiche e ai requisiti del cliente. Gli account e le organizzazioni appena creati potrebbero avere una quota inferiore al valore predefinito di 10 account. 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. Quando un account viene chiuso, non smette di rientrare in questa quota finché non viene chiuso definitivamente. Per ulteriori informazioni su quando un account viene chiuso definitivamente, consulta Periodo successivo alla chiusura nella Guida Gestione dell'account AWS di riferimento. Alcuni servizi hanno limiti di account diversi dal numero massimo di account consentito in un'organizzazione. Per ulteriori informazioni, consulta Limiti per AWS servizio.
Età minima per la rimozione degli account creati	Ogni regione supportata: 7 — Il numero minimo di giorni in cui un account creato deve esistere prima di poterlo rimuovere dall'organizzazione.
Numero di radici in un'organizzazione	1
Numero di membri OUs di un'organizzazione	2000

Descrizione	Limite
Numero di policy di ciascun tipo in un'organizzazione	Politiche di controllo del servizio: 10.000 Politiche di controllo delle risorse: 1000 Politiche dichiarative: 1000 Politiche di Backup: 1000 Politiche per i tag: 1000 Politiche per le applicazioni di chat: 1000 Politiche di disattivazione dei servizi di intelligenza artificiale: 1000 Politiche del Security Hub: 1000
Dimensione massima di un documento di policy	Policy di controllo dei servizi: 5.120 caratteri Politiche di controllo delle risorse: 5120 caratteri Politiche dichiarative: 10.000 caratteri Policy di backup: 10.000 caratteri Politiche per le applicazioni di chat: 10.000 caratteri Policy di rifiuto dei servizi di IA: 2.500 caratteri Policy di tag: 10.000 caratteri Politiche del Security Hub: 10.000 caratteri Nota: se si salva la policy utilizzando lo spazio bianco aggiuntivo (come 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.

Descrizione	Limite
Nidificazione massima UO in una radice	Cinque livelli di OUs profondità 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 che puoi chiudere in un periodo di 30 giorni	10% degli account dei membri di un'organizzazione, con un massimo di 1000. Questa quota non è regolabile. • < 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 Dopo aver raggiunto questa quota, puoi chiudere altri account o attendere che la quota venga ripristinata. Per ulteriori informazioni, consulta Chiudere un AWS 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.

Descrizione	Limite
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

Limiti per AWS servizio

La maggior parte Servizi AWS supporta il numero massimo dichiarato di account che è possibile avere in un'organizzazione. Tuttavia, alcuni servizi hanno limiti di account diversi dal numero massimo di account consentito in un'organizzazione.

La tabella seguente mostra i servizi con limiti di account separati.

AWS servizio	Limite	Può essere aumentata
AWS IAM Identity Center	3000	Sì
AWS Application Migration Service	5000	No
AWS Directory Service	250	Sì

Per ulteriori informazioni, consulta le AWS IAM Identity Center quote nella Guida per l'utente di IAM Identity Center e i limiti delle quote dei servizi AWS MGN nella Guida per l'utente del servizio di migrazione delle applicazioni.

Tempi di scadenza per gli handshake

Di seguito sono riportati i timeout per le strette di mano. AWS Organizations

Descrizione	Limite
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. Tutti i limiti delle politiche sono limiti rigidi.

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 un SCP collegato in ogni momento quando viene abilitata. SCPs	5	5	5

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
	Non è possibile rimuovere l'ultima SCP da un'entità.			
Politica di controllo delle risorse	1 — La `RCPFullAWSAccess` policy viene automaticamente allegata alla directory principale, a tutte le unità organizzative e a tutti gli account dell'organizzazione quando viene abilitata RCPs. Non è possibile scollegare questa policy e viene conteggiata ai fini della quota di 5 policy.	5	5	5
Politica dichiarativa	0	10	10	10
Policy di backup	0	10	10	10
Policy di tag	0	10	10	10
Politica sulle applicazioni di chat	0	5	5	5

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 rifiuto dei servizi di IA	0	5	5	5
Politica Security Hub	0	10	10	10

> **Note**
>
> È possibile avere una sola radice in un'organizzazione.

Limiti di limitazione

Le tabelle seguenti elencano i AWS Organizations APIs dati per categoria di gestione e mostrano i rispettivi tassi di limitazione a livello di account e organizzazione.

AWS Organizations utilizza l'algoritmo token bucket per implementare il throttling delle API. Con questo algoritmo, il tuo account dispone di un bucket che contiene un numero specifico di token. Il numero di token nel bucket rappresenta la tua quota di throttling in un dato secondo.

La frequenza è la velocità fissa con cui i token vengono aggiunti al bucket di token al secondo.

Burst è il numero massimo di token che è possibile aggiungere e il numero massimo di token utilizzabili al secondo.

Ad esempio, l'`DescribeAccount`API è limitata a una singola richiesta Account AWS al secondo come frequenza di base e a 30 richieste al secondo come frequenza di burst. La frequenza di burst di 30 richieste al secondo consente di superare temporaneamente la frequenza di base di 20 richieste al secondo.

È possibile effettuare 20 richieste nel primo secondo, che è la frequenza di base. Nel secondo successivo, puoi effettuare 30 richieste, superando la linea di base ma rimanendo entro la frequenza di burst di 30. Tuttavia, nel terzo secondo, se provi a fare più di 20 richieste, non riuscirai a superare la velocità di base e perché la capacità di burst è stata utilizzata.

La frequenza di burst ti consente di gestire picchi temporanei di traffico senza subire rallentamenti, a condizione che la media delle richieste al secondo rimanga entro il limite di base nel tempo.

Limiti di gestione dell'account

La tabella seguente elenca i dati AWS Organizations APIs per la gestione degli account.

AWS Organizations API	Limite per account (rate, burst)	Limite per organizzazione (rate, burst)
CloseAccount	0,05, 1	
CreateAccount, CreateGov CloudAccount	0,1, 3	
DescribeAccount	20, 30	24, 36
DescribeCreateAccountStatus	2, 2	2, 3
LeaveOrganization	1, 1	
ListCreateAccountStatus	5, 8	6, 10

Limiti di gestione dell'handshake

La tabella seguente elenca l'handshake AWS Organizations APIs per l'account.

AWS Organizations API	Limite per account (rate, burst)	Limite per organizzazione (rate, burst)
AcceptHandshake	1, 2	5, 5
DescribeHandshake	1, 2	6, 10
CancelHandshake	2, 3	
DeclineHandshake	1, 1	5, 5
InviteAccountToOrganization	3, 5	

AWS Organizations API	Limite per account (rate, burst)	Limite per organizzazione (rate, burst)
ListHandshakesForAccount, ListHandshakesForOrganization	5, 8	6, 10

Limiti di gestione dell'organizzazione

La tabella seguente elenca i dati AWS Organizations APIs per la gestione dell'organizzazione.

AWS Organizations API	Limite per account (rate, burst)	Limite per organizzazione (rate, burst)
CreateOrganization, DeleteOrganization, EnableFullControl	1, 1	
CreateOrganizationalUnit, DescribeOrganization	1, 2	
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

AWS Organizations API	Limite per account (rate, burst)	Limite per organizzazione (rate, burst)
RemoveAccountFromOrganization	2, 2	
TagResource, UntagResource	4, 6	

Limiti di gestione delle politiche

La tabella seguente elenca i dati AWS Organizations APIs per la gestione delle politiche.

AWS Organizations API	Limite per account (rate, burst)	Limite per organizzazione (rate, burst)
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	

Limiti di gestione del servizio

La tabella seguente elenca i dati AWS Organizations APIs per la gestione dei servizi.

AWS Organizations API	Limite per account (rate, burst)	Limite per organizzazione (rate, burst)
Abilita AWSService l'accesso , disabilita AWSService l'accesso	1, 2	
Elenco AWSServiceAccessFo rOrganization, ListDeleg atedServicesForAccount	1, 3	1, 4
ListDelegatedAdministrators	5, 8	6, 10
RegisterDelegatedAdministra tor, DeregisterDelegate dAdministrator	1, 2	

Supporto regionale per AWS Organizations

AWS Organizations è disponibile in tutte le regioni AWS commerciali e in tutte le regioni della Cina. AWS GovCloud (US) Regions

Per un elenco delle differenze di funzionalità in AWS GovCloud (US) Regions, vedere AWS Organizations in AWS GovCloud (US).

Per un elenco delle differenze di funzionalità nelle regioni della Cina, vedi AWS Organizations in Cina.

Gli endpoint del servizio per Organizations si trovano:

- Negli Stati Uniti orientali (Virginia settentrionale) per le organizzazioni commerciali
- In AWS GovCloud (Stati Uniti occidentali) per le organizzazioni AWS GovCloud (US)
- In Cina (Ningxia) per le organizzazioni cinesi, gestite da Ningxia Western Cloud Data Technology Co. Ltd (NWCD).

Tutte le entità organizzative sono accessibili a livello globale, ad eccezione delle organizzazioni gestite in Cina, in modo simile a come funziona oggi AWS Identity and Access Management (IAM).

Non è necessario specificare un Regione AWS quando si crea e si gestisce l'organizzazione, ma è necessario creare un'organizzazione separata per gli account utilizzati in Cina. Gli utenti del tuo paese Account AWS possono utilizzare il servizio Servizi AWS in qualsiasi area geografica in cui tale servizio è disponibile.

> **Note**
>
> Le politiche relative ai tag sono supportate solo in un sottoinsieme di regioni
> Le policy di tag sono un tipo di policy che può semplificare la standardizzazione dei tag tra le risorse degli account dell'organizzazione. Le politiche relative ai tag sono supportate solo in un sottogruppo di Regioni in cui è supportato Organizations. Per un elenco delle regioni in cui sono supportate le politiche sui tag, consulta Politiche sui tag | Regioni di supporto.

Elenco delle opzioni disponibili Regioni AWS

La tabella seguente elenca tutte le opzioni disponibili Regioni AWS.

Nome della regione	Regione	Endpoint	Protocollo	
US East (Ohio)	us-east-2	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
US East (N. Virginia)	us-east-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
Stati Uniti occidentali (California settentrionale)	us-west-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	

Nome della regione	Regione	Endpoint	Protocollo	
US West (Oregon)	us-west-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Africa (Cape Town)	af-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Asia Pacifico (Hong Kong)	ap-east-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Asia Pacific (Hyderabad)	ap-south-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Asia Pacifico (Giacarta)	ap-southeast-3	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Asia Pacifico (Malesia)	ap-southeast-5	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Asia Pacifico (Melbourne)	ap-southeast-4	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Asia Pacifico (Mumbai)	ap-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	

Nome della regione	Regione	Endpoint	Protocollo	
Asia Pacifico (Osaka-Locale)	ap-northeast-3	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Asia Pacifico (Seoul)	ap-northeast-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Asia Pacifico (Singapore)	ap-southeast-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Asia Pacifico (Sydney)	ap-southeast-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Asia Pacifico (Taipei)	ap-east-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Asia Pacifico (Thailandia)	ap-southeast-7	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Asia Pacifico (Tokyo)	ap-northeast-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Canada (Centrale)	ca-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	

Nome della regione	Regione	Endpoint	Protocollo	
Canada occidentale (Calgary)	ca-west-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Europa (Francoforte)	eu-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Europa (Irlanda)	eu-west-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Europa (Londra)	eu-west-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Europa (Milano)	eu-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Europa (Parigi)	eu-west-3	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Europa (Spagna)	eu-south-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Europa (Stoccolma)	eu-north-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Europa (Zurigo)	eu-central-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	

Nome della regione	Regione	Endpoint	Protocollo	
Israele (Tel Aviv)	il-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Messico (centrale)	mx-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Medio Oriente (Bahrein)	me-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Medio Oriente (Emirati Arabi Uniti)	me-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Sud America (São Paulo)	sa-east-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	organizations.us-gov-west-1.amazonaws.com	HTTPS	
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	organizations.us-gov-west-1.amazonaws.com	HTTPS	

Fatturazione e prezzi per AWS Organizations

AWS Organizations è offerto senza costi aggiuntivi. Ti vengono addebitati solo i costi AWS delle risorse utilizzate dagli utenti e dai ruoli dei tuoi account membro. Ad esempio, ti vengono addebitate le tariffe standard per EC2 le istanze Amazon utilizzate dagli utenti o dai ruoli nei tuoi account membro. Per informazioni sui prezzi di altri AWS servizi, consulta la pagina AWS Prezzi.

Chi paga per l'utilizzo sostenuto dagli utenti con un account AWS membro nella mia organizzazione?

Il proprietario dell'account di gestione è responsabile del pagamento di tutti gli utilizzi, i dati e le risorse utilizzati dagli account dell'organizzazione.

La mia fattura rifletterà la struttura delle unità organizzative che ho creato nella mia organizzazione?

La fattura non rifletterà la struttura definita nell'organizzazione. È possibile utilizzare i tag di allocazione dei costi Account AWS singolarmente per classificare e tenere traccia AWS dei costi e tale allocazione sarà visibile nella fattura consolidata dell'organizzazione.

Support 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 AWS supporto, consulta l'Aiuto dei forum.

Altre AWS risorse

- AWS Formazione e corsi: collegamenti a corsi specializzati e basati su ruoli, nonché a laboratori di autoapprendimento per aiutarti ad affinare le tue abilità e acquisire esperienza pratica. AWS
- 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.
- Supporto AWS Center: l'hub per la creazione e la gestione dei casi di AWS Support. Include anche collegamenti ad altre risorse utili, come forum, informazioni tecniche FAQs, stato di integrità del servizio e AWS Trusted Advisor.

- AWS Supporto: la pagina Web principale per informazioni su AWS Support one-on-one, un canale di supporto a risposta rapida per aiutarti a creare ed eseguire applicazioni nel cloud.
- Contattaci: un punto di contatto centrale per domande relative a AWS fatturazione, account, eventi, abusi e altre questioni.
- AWS Termini del sito: informazioni dettagliate sul nostro copyright e marchio, sull'account, sulla licenza e sull'accesso al sito dell'utente e su altri argomenti.

Le migliori pratiche per un ambiente con più account

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

Argomenti

Account e credenziali

Abilita la gestione degli accessi root per semplificare la gestione delle credenziali degli utenti root per gli account dei membri

Ti consigliamo di abilitare la gestione dell'accesso root per aiutarti a monitorare e rimuovere le credenziali degli utenti root per gli account dei membri. La gestione degli accessi root impedisce il recupero delle credenziali degli utenti root, migliorando la sicurezza degli account nell'organizzazione.

- Rimuovi le credenziali dell'utente root per gli account dei membri per impedire l'accesso all'utente root. Ciò impedisce inoltre il ripristino degli account membro dell'utente root.
- Si supponga di disporre di una sessione privilegiata per eseguire le seguenti attività sugli account dei membri:
  - Rimuovi una policy del bucket configurata non correttamente che impedisce a tutti i principali di accedere al bucket Amazon S3.
  - Elimina una policy basata sulle risorse Amazon Simple Queue Service che nega a tutti i principali l'accesso a una coda Amazon SQS.
  - Consenti a un account membro di recuperare le credenziali dell'utente root. La persona con accesso alla casella di posta elettronica dell'utente root di per l'account membro può reimpostare la password dell'utente root e accedere come utente root dell'account membro.

Dopo aver abilitato la gestione dell'accesso root, gli account membro appena creati non secure-by-default dispongono di credenziali utente root, il che elimina la necessità di ulteriori misure di sicurezza, come l'MFA dopo il provisioning.

Per ulteriori informazioni, consulta Centralizzare le credenziali utente root per gli account dei membri nella Guida per l'utente.AWS Identity and Access Management

Mantieni aggiornato il numero di telefono di contatto

Per ripristinare l'accesso al proprio Account AWS, è fondamentale disporre di un numero di telefono di contatto valido e attivo che consenta di ricevere messaggi di testo o chiamate. Ti 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 del tuo account tramite la AWS Management Console pagina o Gestione account APIs.

Esistono vari modi per ottenere un numero di telefono dedicato che ti consenta di AWS 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 delle informazioni di AWS contatto e condividi i dettagli con i team specifici che devono esserne a conoscenza all'interno dell'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 sia AWS necessario 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.

Struttura organizzativa e carichi di lavoro

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.

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

Ti consigliamo di isolare gli ambienti e i dati dei carichi di lavoro di produzione in base ai carichi di lavoro di primo livello orientati ai carichi di lavoro. OUs OUs Dovreste basarvi su un insieme comune di controlli anziché rispecchiare la struttura di rendicontazione della vostra azienda. Oltre alla produzione OUs, ti consigliamo di definire uno o più ambienti non di produzione OUs che contengano account e ambienti di carico di lavoro utilizzati per sviluppare e testare i carichi di lavoro. Per ulteriori indicazioni, vedi Organizzazione orientata al carico di lavoro. OUs

Utilizzo di più account per organizzare i carichi di lavoro

An Account AWS fornisce sicurezza naturale, accesso e limiti di fatturazione per le tue 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.

Gestione dei servizi e dei costi

Abilita AWS i servizi a livello organizzativo utilizzando la console di servizio o le operazioni API/CLI

Come best practice, ti consigliamo di abilitare o disabilitare tutti i servizi con cui desideri integrarti AWS Organizations utilizzando la console di quel servizio o gli equivalenti delle operazioni API/

comandi CLI. Utilizzando questo metodo, il AWS servizio può eseguire tutte le fasi di inizializzazione necessarie per l'organizzazione, come la creazione di tutte le risorse necessarie e la pulizia delle risorse quando si disabilita il servizio. Gestione dell'account AWS è l'unico servizio che richiede l'uso o APIs l'attivazione della AWS Organizations console. Per visualizzare l'elenco dei servizi integrati con AWS Organizations, vedereServizi AWS che puoi usare 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 denominazione dei tag, segui le indicazioni riportate in Etichettare le tue risorse. AWS Oltre alle risorse, puoi creare tag nella cartella principale, negli account e nelle politiche dell'organizzazione. OUs Per ulteriori informazioni, consulta Building your tagging strategy.

Guida introduttiva con AWS Organizations

I seguenti argomenti forniscono informazioni utili per iniziare a utilizzare AWS Organizations. È inoltre possibile utilizzare i seguenti tutorial per iniziare a eseguire attività utilizzando. AWS Organizations

Tutorial: creazione e configurazione di un'organizzazione

Inizia subito con step-by-step le istruzioni per creare la tua organizzazione, invitare i tuoi primi account membro, creare una gerarchia di unità organizzative che contenga i tuoi account e applicare alcune politiche di controllo del servizio (). SCPs

Tutorial: monitora le modifiche importanti alla tua organizzazione con Amazon EventBridge

Monitora i cambiamenti chiave nella tua organizzazione configurando Amazon EventBridge per attivare un allarme sotto forma di e-mail, SMS o registrazione del registro quando si verificano azioni da te designate nella tua organizzazione. Ad esempio, molte organizzazioni vogliono sapere quando viene creato un nuovo account o quando un account tenta di lasciare l'organizzazione.

Argomenti

Iscrizione a AWS

Argomenti

Iscriviti per un Account AWS

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

Per iscriverti a un Account AWS

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

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

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

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

Crea un utente con accesso amministrativo

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

Proteggi i tuoi Utente root dell'account AWS

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

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

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

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

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

2. In IAM Identity Center, assegna l'accesso amministrativo a un utente.

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

Accesso come utente amministratore

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

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

Assegna l'accesso a ulteriori utenti

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

   Segui le istruzioni riportate nella pagina Creazione di un set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

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

Accedendo AWS Organizations

Puoi lavorare con AWS Organizations in uno dei seguenti modi:

AWS Management Console

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

AWS Strumenti da riga di comando

Con gli strumenti da riga di AWS comando, è possibile impartire comandi sulla riga di comando del sistema per eseguire AWS operazioni AWS Organizations e operazioni. 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 fornisce due set di strumenti da riga di comando:

- AWS Command Line Interface

  Il AWS Command Line Interface (AWS CLI) è uno strumento unificato per gestire i tuoi Servizi AWS. Con un solo strumento da scaricare e configurare, puoi controllarne più di uno Servizi AWS dalla riga di comando e automatizzarli tramite script.

  Per informazioni sull'installazione e l'utilizzo di AWS CLI, consulta la Guida per l'AWS Command Line Interface utente.

- AWS Tools for Windows PowerShell

  Gli strumenti per Windows PowerShell consentono a sviluppatori e amministratori di gestire le proprie Servizi AWS risorse nell'ambiente di PowerShell scripting. Puoi gestire AWS le tue risorse con gli stessi PowerShell strumenti che usi per gestire gli ambienti Windows, Linux e macOS.

  Per informazioni sull'installazione e l'utilizzo degli strumenti per Windows PowerShell, consulta la Guida per l'AWS Strumenti per PowerShell utente.

AWS SDKs

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

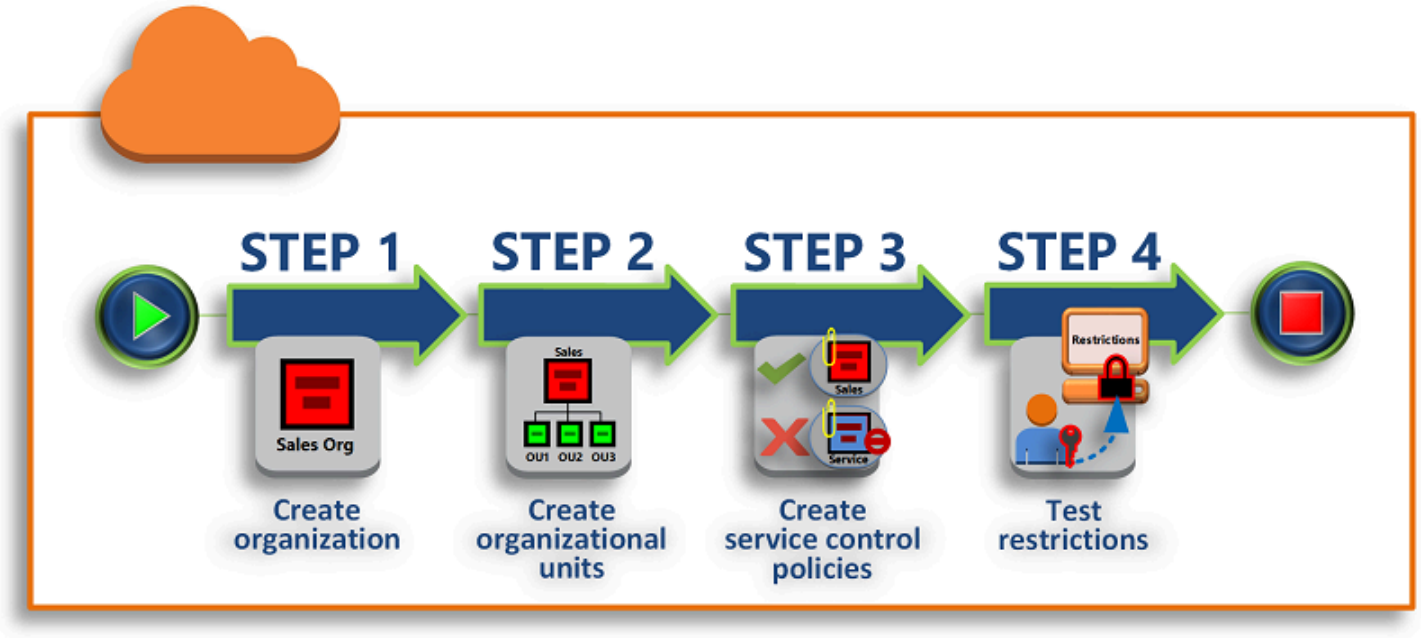
AWS Organizations API di interrogazione HTTPS

L'API AWS Organizations HTTPS Query offre accesso programmatico a 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.

Tutorial: creazione e configurazione di un'organizzazione

In questo tutorial, crei la tua organizzazione e la configuri con due account AWS membri. 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. Ciò consente agli amministratori di convalidare qualsiasi nuovo servizio AWS introdotto prima di consentirne l'utilizzo da parte di chiunque altro membro dell'azienda. In questo modo, se si AWS introduce un nuovo servizio, questo rimane proibito finché un amministratore non aggiunge il servizio all'elenco consentito nella politica appropriata. Il tutorial mostra anche come utilizzare un elenco di utenti non autorizzati per garantire che nessun utente di un account membro possa modificare la configurazione dei registri di controllo creati. AWS CloudTrail

La figura seguente mostra le fasi principali del tutorial.



Fase 1: creazione dell'organizzazione

In questo passaggio, crei un'organizzazione con il tuo attuale account Account AWS di gestione. Inoltre, ne inviti una persona Account AWS a entrare a far parte della tua organizzazione e crei un secondo account come account membro.

[Fase 2: creazione delle unità organizzative (UO)]

Successivamente, crei due unità organizzative (OUs) nella nuova organizzazione e inserisci gli account dei membri in esse OUs.

[Fase 3: creazione delle policy di controllo dei servizi]

È possibile applicare restrizioni alle azioni che possono essere delegate agli utenti e ai ruoli negli account dei membri utilizzando le politiche di controllo del servizio (SCPs). In questo passaggio, ne crei due SCPs e li alleghi OUs all'interno dell'organizzazione.

[Fase 4: Test delle policy dell'organizzazione]

Potete accedere come utenti da ciascuno degli account di prova e vedere gli effetti che SCPs hanno sugli account.

Nessuno dei passaggi di questo tutorial comporta costi in AWS bolletta. AWS Organizations è un servizio gratuito.

Prerequisiti

Questo tutorial presuppone che tu abbia accesso a due esistenti Account AWS (ne crei un terzo come parte di questo tutorial) e che tu possa accedere a ciascuno come amministratore.

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 AWS come amministratore dell'account 1111 e apri la AWS Organizations console.
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 Account AWSpagina. 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 con AWS Organizations.

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 una Account AWS pagina, scegli Invita un esistente Account AWS.
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 Account AWS ID, puoi inserirlo al suo posto.
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 Invia invito. AWS Organizations invia 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 AWS inviata dall'account di gestione e scegli 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

Nei passaggi di questa sezione, crei un utente Account AWS che diventa automaticamente membro dell'organizzazione. Nel tutorial ci si riferisce a questo account come 333333333333..

AWS Management Console

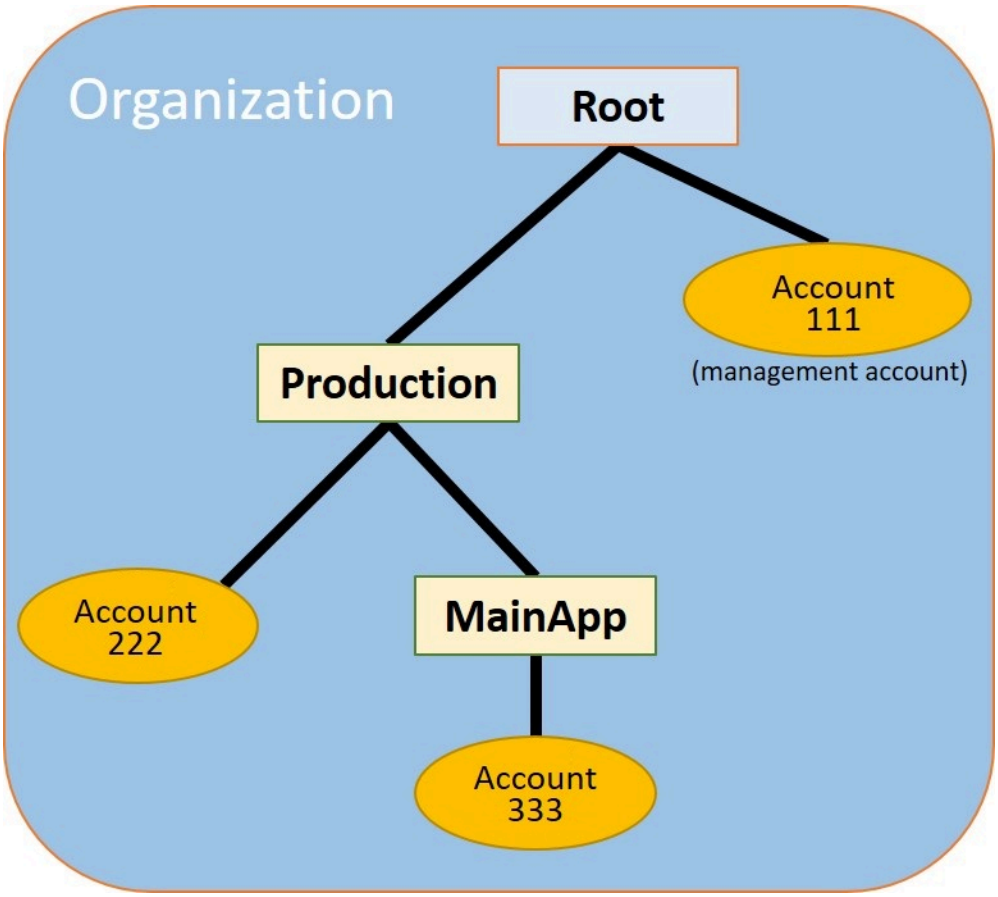
Per creare un account membro

1. Nella AWS Organizations console, nella Account AWSpagina, scegli 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 Account AWS (Crea). 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)

Nei passaggi di questa sezione, creerai unità organizzative (OUs) e inserirai i tuoi account membro al loro interno. Al termine, la gerarchia si presenterà come illustrato di seguito. L'account di gestione rimane nel root. Un account membro viene spostato nell'unità organizzativa di produzione e l'altro account membro viene spostato nell' MainApp unità organizzativa, che è figlia di Production.



AWS Management Console

Per creare e compilare il OUs

> **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. Scegli il menu a discesa Azioni, quindi in Unità organizzativa, scegli Crea nuovo.
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 i tuoi account membro in questi OUs.
8. Torna alla pagina Account AWS ed espandi la struttura sotto l'UO Production (Produzione) scegliendo il triangolo
   
   accanto ad essa. In questo modo l'MainAppunità organizzativa viene visualizzata 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 '3333', scegli il triangolo accanto a Production per espanderlo. Quindi MainApp, scegli il pulsante di opzione 
    (non il suo 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 Move Account AWS '222222222222', accanto a Production, scegli il pulsante di opzione (non il nome), quindi scegli Sposta. Account AWS

Fase 3: creazione delle policy di controllo dei servizi

Nei passaggi di questa sezione, crei tre criteri di controllo del servizio (SCPs) e li alleghi alla radice e al fine di limitare ciò che gli utenti degli account dell'organizzazione possono fare. OUs Il primo SCP impedisce a chiunque faccia parte degli account membri di creare o modificare AWS CloudTrail i log configurati. L'account di gestione non è interessato da alcun SCP, quindi dopo aver applicato l' CloudTrail SCP, è necessario creare eventuali registri 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

Da abilitare per la tua organizzazione SCPs

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 SCPs nella tua organizzazione.

Crea il tuo SCPs

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 il primo SCP che blocchi le CloudTrail azioni di configurazione

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 Politica, nell'elenco dei servizi sulla destra, seleziona CloudTrail il servizio. Quindi scegli le seguenti azioni: AddTagsCreateTrail, DeleteTrail, RemoveTags, StartLogging, StopLogging, e UpdateTrail.
5. Sempre nel riquadro di destra, scegli Aggiungi risorsa e specifica CloudTraile Tutte le risorse. Scegliere Add resource (Aggiungi risorsa).

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

   JSON

```
{
    "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. Scegliere Create Policy (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.

   JSON

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

```
}
```

4. Scegliere Create Policy (Crea policy).

La policy finale fornisce un elenco di servizi di cui è bloccato l'uso nell' MainApp unità organizzativa. In questo tutorial, blocchi l'accesso ad Amazon DynamoDB in tutti gli account presenti nell'unità organizzativa. MainApp

AWS Management Console

Per creare la terza politica che neghi l'accesso ai servizi che non possono essere utilizzati nell'unità organizzativa 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.

   JSON

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

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

Allegalo SCPs al tuo OUs

Ora che SCPs esistono e sono abilitati per la tua root, puoi collegarli alla radice e OUs.

AWS Management Console

Per collegare le politiche alla radice e alla OUs

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, lo colleghi alla radice in modo che influisca su tutti gli account membri per evitare che qualcuno alteri il modo in cui hai configurato CloudTrail.

   La pagina dei dettagli di Root, scheda Policies, ora mostra che due SCPs sono collegati alla radice: quello che hai appena collegato e l'`FullAWSAccess`SCP predefinito.
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. Scegli nuovamente la scheda Politiche per vedere che due SCPs sono collegate all'unità organizzativa: quella appena collegata e l'`FullAWSAccess`SCP predefinito. 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 politica predefinita dall'unità organizzativa di produzione, fate clic sul pulsante di opzione Completo AWSAccess, scegliete Scollega, quindi nella finestra di dialogo di conferma, scegliete Scollega politica.

    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 puoi allegare il nome SCP `Deny List for MainApp Prohibited services` per impedire a chiunque negli account dell' MainApp unità organizzativa di utilizzare uno qualsiasi dei servizi con restrizioni.

    A tale scopo, accedi alla Account AWSpagina, scegli l'icona a forma di triangolo per espandere il ramo dell'unità di produzione, quindi scegli l'MainAppunità organizzativa (è il nome, non il pulsante di opzione) per accedere al suo contenuto.

12. Nella pagina dei MainAppdettagli, scegli la scheda Politiche.

13. In Criteri di controllo del servizio, scegli Allega, quindi nell'elenco dei criteri disponibili, scegli il pulsante di opzione accanto a Deny List for MainApp Prohibited Services, quindi scegli Allega 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. SCPs Non influiscono su alcun utente o ruolo dell'account di gestione, indipendentemente dalla radice o dall'unità organizzativa in cui si trova l'account.
- Se accedi come utente nell'account 222222222222, puoi eseguire tutte le azioni consentite dall'elenco degli utenti consentiti. AWS Organizations nega qualsiasi tentativo di eseguire un'azione in qualsiasi servizio che non è nell'elenco consentito. Inoltre, AWS Organizations nega qualsiasi tentativo di eseguire una delle CloudTrail azioni di configurazione.

- 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 nega qualsiasi tentativo di eseguire una delle CloudTrail azioni di configurazione.

Tutorial: monitora le modifiche importanti alla tua organizzazione con Amazon EventBridge

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

La figura seguente mostra le fasi principali del tutorial.

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

Crea un registro, chiamato trail, in. AWS CloudTrail e configuralo in modo da acquisire tutte le chiamate API.

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

Crea una AWS Lambda funzione che registri 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: Creare una EventBridge regola Amazon

Crea una regola che indichi EventBridge ad Amazon di trasmettere i dettagli di chiamate API specificate alla funzione Lambda e agli abbonati all'argomento SNS.

Passaggio 5: verifica la tua EventBridge regola Amazon

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 AWS CloudTrail e su Amazon EventBridge con AWS Organizations, consultaRegistrazione e monitoraggio AWS Organizations.

Prerequisiti

Questo tutorial presuppone quanto segue:

- Puoi accedere AWS Management Console come utente IAM dall'account di gestione della tua organizzazione. L'utente IAM deve disporre delle autorizzazioni per creare e configurare un accesso 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 bucket Amazon Simple Storage Service (Amazon S3) esistente (oppure disponi delle autorizzazioni per creare un bucket) per ricevere CloudTrail il log configurato nella fase 1.

> **Important**
>
> Attualmente, AWS Organizations è ospitato solo nella regione Stati Uniti orientali (Virginia settentrionale) (anche se è disponibile a livello globale). Per eseguire i passaggi di questo tutorial, è necessario configurare l'utilizzo AWS Management Console di quella 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. Puoi anche configurare un selettore di eventi durante il percorso per acquisire tutte le chiamate API di lettura/scrittura in modo che Amazon EventBridge abbia chiamate da attivare.

Per creare un trail

1. Accedi AWS come amministratore dell'account di gestione dell'organizzazione, quindi apri la console all' CloudTrail indirizzo. 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 diversa, AWS Organizations non appare come opzione nelle impostazioni di EventBridge configurazione di Amazon e CloudTrail non acquisisce informazioni su 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. Esegui una delle seguenti opzioni per specificare dove CloudTrail inviare i log:

   - 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. Scegli Next (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. Scegli Next (Successivo).
10. Rivedi le selezioni effettuate, quindi scegli Create trail (Crea trail).

Amazon ti EventBridge consente di scegliere tra diversi modi per inviare avvisi quando una regola di allarme 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 questo passaggio, crei una funzione Lambda che registra l'attività dell'API che le viene inviata dalla EventBridge regola Amazon che configurerai in seguito.

Per creare una funzione Lambda che registri gli eventi Amazon EventBridge

1. Apri la AWS Lambda console 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. Scegli 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 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. Fai di questo argomento un obiettivo della EventBridge regola Amazon che creerai in seguito.

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. Scegli Crea sottoscrizione.
   a. Nella pagina Create subscription (Crea sottoscrizione) scegli Email (E-mail) in Protocol (Protocollo).
   b. Per Endpoint, immettere il proprio indirizzo e-mail.

c. Scegli Crea abbonamento. AWS invia un'e-mail all'indirizzo e-mail specificato nel passaggio 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: Creare una EventBridge regola Amazon

Ora che la funzione Lambda richiesta è presente nel tuo account, crei una EventBridge regola Amazon che la richiama quando vengono soddisfatti i criteri della regola.

Per creare una regola EventBridge

1. Apri la EventBridge console Amazon all'indirizzohttps://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 istruzioni sulla creazione di regole, consulta Rules in Amazon EventBridge nella guida per EventBridge l'utente di Amazon.

Passaggio 5: verifica la tua EventBridge regola Amazon

In questa fase, crei un'unità organizzativa (OU) e osservi la EventBridge regola di Amazon, generi una voce di registro e ti invii un'e-mail con i dettagli sull'evento.

AWS Management Console

Per creare un'unità organizzativa

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

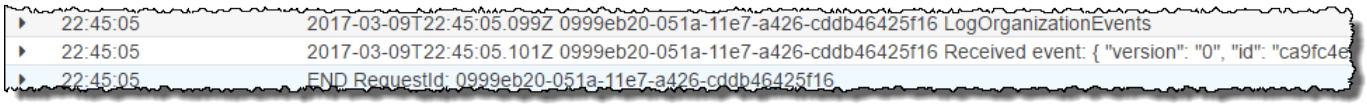
   ☑

   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).

Per visualizzare la voce del EventBridge registro

1. Apri la CloudWatch console all'indirizzohttps://console.aws.amazon.com/cloudwatch/.
2. Nella pagina di navigazione scegli Log.
3. In Gruppi di log, scegli il gruppo associato alla tua 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 se nel tuo account e-mail è presente un messaggio proveniente da CWEvntOrg (il nome visualizzato del tuo 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 evitare di incorrere in addebiti, dovresti eliminare tutte AWS le risorse che hai creato come parte di questo tutorial che non desideri conservare.

Per ripulire l'ambiente AWS

1. Usa la CloudTrail console per eliminare il percorso denominato **`My-Test-Trail`** che hai creato nel passaggio 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. Usa la CloudWatch console per eliminare la EventBridge regola denominata **`OrgsMonitorRule`** che hai creato nel passaggio 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, ti sei configurato EventBridge per monitorare le modifiche apportate alla tua organizzazione. 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.

Utilizzo AWS Organizations con un SDK AWS

AWS i kit di sviluppo software (SDKs) sono disponibili per molti linguaggi di programmazione più diffusi. Ogni SDK fornisce un'API, esempi di codice, e documentazione che facilitano agli sviluppatori la creazione di applicazioni nel loro linguaggio preferito.

Documentazione sugli SDK	Esempi di codice
AWS SDK per C++	AWS SDK per C++ esempi di codice
AWS CLI	AWS CLI esempi di codice
AWS SDK per Go	AWS SDK per Go esempi di codice
AWS SDK per Java	AWS SDK per Java esempi di codice
AWS SDK per JavaScript	AWS SDK per JavaScript esempi di codice
AWS SDK per Kotlin	AWS SDK per Kotlin esempi di codice
AWS SDK per .NET	AWS SDK per .NET esempi di codice
AWS SDK per PHP	AWS SDK per PHP esempi di codice
AWS Strumenti per PowerShell	AWS Strumenti per PowerShell esempi di codice
AWS SDK per Python (Boto3)	AWS SDK per Python (Boto3) esempi di codice
AWS SDK per Ruby	AWS SDK per Ruby esempi di codice

Documentazione sugli SDK	Esempi di codice
AWS SDK for Rust	AWS SDK for Rust esempi di codice
SDK AWS per SAP ABAP	SDK AWS per SAP ABAP esempi di codice
SDK AWS per Swift	SDK AWS per Swift esempi di codice

Esempio di disponibilità

Non riesci a trovare quello che ti serve? Richiedi un esempio di codice utilizzando il link Provide feedback (Fornisci un feedback) nella parte inferiore di questa pagina.

Gestire un'organizzazione con AWS Organizations

Un'organizzazione è un insieme di elementi Account AWS che è possibile gestire centralmente e organizzare in una struttura gerarchica ad albero con una radice nella parte superiore e unità organizzative annidate sotto la radice. Ogni account può trovarsi direttamente nella directory principale o collocato in uno dei punti della gerarchia. OUs

Ogni organizzazione è composta da:

- Un account di gestione
- Zero o più account membri
- Zero o più unità organizzative (OUs)
- Zero o più politiche.

Un'organizzazione ha la funzionalità determinata dall'insieme di caratteristiche che si abilita.

Argomenti

- Creare un'organizzazione con AWS Organizations
- Verifica dell'indirizzo e-mail con AWS Organizations
- Invia nuovamente l'email di verifica con AWS Organizations
- Modifica dell'indirizzo e-mail di un'organizzazione con AWS Organizations
- Abilitazione di tutte le funzionalità per un'organizzazione con AWS Organizations
- Visualizzazione dei dettagli di un'organizzazione dall'account di gestione
- Eliminazione di un'organizzazione con AWS Organizations

Creare un'organizzazione con AWS Organizations

Puoi creare un'organizzazione con Account AWS il tuo account di gestione. Quando crei un'organizzazione, puoi scegliere se l'organizzazione supporta tutte le funzionalità (scelta consigliata) o solo la fatturazione consolidata. Per impostazione predefinita, un'organizzazione creata supporta tutte le funzionalità.

Creazione di un'organizzazione

È possibile creare un'organizzazione utilizzando AWS Management Console o utilizzando un comando dall'SDK AWS CLI o da uno degli SDK APIs.

> **Autorizzazioni minime**
>
> Per creare un'organizzazione con la tua attuale organizzazione Account AWS, devi disporre delle seguenti autorizzazioni:
>
> - `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, consulta Verifica dell'indirizzo e-mail con AWS Organizations. 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

Gli esempi di codice seguenti mostrano come utilizzare `CreateOrganization`.

.NET

SDK per .NET

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates an organization in AWS Organizations.
/// </summary>
```

```
   public class CreateOrganization
   {
       /// <summary>
       /// Creates an Organizations client object and then uses it to create
       /// a new organization with the default user as the administrator, and
       /// then displays information about the new organization.
       /// </summary>
       public static async Task Main()
       {
           IAmazonOrganizations client = new AmazonOrganizationsClient();

           var response = await client.CreateOrganizationAsync(new
CreateOrganizationRequest
           {
               FeatureSet = "ALL",
           });

           Organization newOrg = response.Organization;

           Console.WriteLine($"Organization: {newOrg.Id} Main Accoount:
{newOrg.MasterAccountId}");
       }
   }
```

- Per i dettagli sull'API, consulta la CreateOrganizationsezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Esempio 1: creare una nuova organizzazione

Bill desidera creare un'organizzazione utilizzando le credenziali dell'account 1111. L'esempio seguente mostra che l'account diventa l'account principale nella nuova organizzazione. Poiché non specifica un set di funzionalità, per impostazione predefinita la nuova organizzazione prevede che tutte le funzionalità siano abilitate e le politiche di controllo del servizio sono abilitate nella directory principale.

```
aws organizations create-organization
```

L'output include un oggetto dell'organizzazione con dettagli sulla nuova organizzazione:

```
{
        "Organization": {
                "AvailablePolicyTypes": [
                        {
                                "Status": "ENABLED",
                                "Type": "SERVICE_CONTROL_POLICY"
                        }
                ],
                "MasterAccountId": "111111111111",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "FeatureSet": "ALL",
                "Id": "o-exampleorgid",
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid"
        }
}
```

Esempio 2: creare una nuova organizzazione con solo le funzionalità di fatturazione consolidate abilitate

L'esempio seguente crea un'organizzazione che supporta solo le funzionalità di fatturazione consolidata:

```
aws organizations create-organization --feature-set CONSOLIDATED_BILLING
```

L'output include un oggetto dell'organizzazione con dettagli sulla nuova organizzazione:

```
{
        "Organization": {
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
                "AvailablePolicyTypes": [],
                "Id": "o-exampleorgid",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
```

```
                "MasterAccountEmail": "bill@example.com",
                "MasterAccountId": "111111111111",
                "FeatureSet": "CONSOLIDATED_BILLING"
        }
}
```

Per ulteriori informazioni, vedere Creating an Organization nella AWS Organizations Users Guide.

- Per i dettagli sull'API, consulta CreateOrganization AWS CLICommand Reference.

Dopo aver creato un'organizzazione, puoi aggiungere account all'organizzazione in questi modi dall'account di gestione:

- Creando altri Account AWS che vengono aggiunti automaticamente alla tua organizzazione come account membri
- Dopo aver verificato il tuo indirizzo e-mail, invita gli utenti esistenti Account AWS a entrare a far parte della tua organizzazione come account membri.

Verifica dell'indirizzo e-mail con AWS Organizations

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 crei un'organizzazione, se l'account di gestione non è stato verificato in precedenza, invia AWS automaticamente un'email di verifica all'indirizzo e-mail specificato. Potrebbe verificarsi un ritardo prima di ricevere l'e-mail di verifica.

Verifica del tuo indirizzo e-mail

Entro 24 ore, segui le istruzioni contenute nell'e-mail per verificare il tuo indirizzo e-mail. Se sono trascorse più di 24 ore, vedi Reinvio dell'email di verifica.

Invia nuovamente l'email di verifica con AWS Organizations

Se non verifichi il tuo indirizzo email entro 24 ore, puoi inviare nuovamente la richiesta di verifica. Dopo aver verificato il tuo indirizzo email, puoi invitare altre persone Account AWS a far parte della tua 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, consulta Gestione degli inviti all'account con AWS Organizations.

Modifica dell'indirizzo e-mail di un'organizzazione con AWS Organizations

Per modificare l'indirizzo e-mail associato al tuo account di gestione, consulta Aggiornare il Account AWS nome, l'indirizzo e-mail o la password dell'utente root nella Guida Gestione dell'account AWS di riferimento.

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 degli account a entrare a far parte della tua organizzazione prima di aver modificato l'indirizzo e-mail dell'account di gestione e tali inviti non sono ancora stati accettati, non possono essere accettati finché non verifichi il nuovo indirizzo e-mail dell'account di

gestione. Devi prima inviare nuovamente la richiesta di verifica. Dopo aver completato la procedura rispondendo all'e-mail, gli account che hai invitato possono accettare gli inviti.

Abilitazione di tutte le funzionalità per un'organizzazione con AWS Organizations

AWS Organizations dispone di due set di funzionalità disponibili:

- Tutte le funzionalità: questo set di funzionalità è il modo preferito e predefinito di utilizzo AWS Organizations e include tutte le funzionalità di consolidamento della fatturazione. Quando si crea un'organizzazione, l'abilitazione di tutte le caratteristiche è l'impostazione predefinita. Con tutte le funzionalità abilitate, puoi utilizzare le funzionalità avanzate di gestione degli account disponibili in Organizations, come l'integrazione con AWS i servizi supportati e le politiche organizzative.
- Funzionalità di fatturazione consolidate: questo set di funzionalità si limita alla generazione di un'unica fattura all'interno di un'organizzazione. Non sono disponibili altre funzionalità di gestione con la fatturazione consolidata.

Se crei un'organizzazione con il set di funzionalità di fatturazione consolidata, puoi abilitare tutte le funzionalità in un secondo momento. Tuttavia, non è possibile migrare da tutte le funzionalità alla fatturazione consolidata dopo aver abilitato tutte le funzionalità.

Migrazione standard e migrazione assistita

I due approcci per la migrazione a tutte le funzionalità sono la migrazione standard e la migrazione assistita.

La migrazione standard è il processo self-service disponibile per tutti i AWS Organizations clienti per abilitare la modalità con tutte le funzionalità.

La migrazione assistita è un processo disponibile per i clienti del piano Enterprise Support per richiedere la AWS migrazione della propria organizzazione alla modalità con tutte le funzionalità per conto dell'utente.

> **Note**
>
> Processi unidirezionali e processi di rollback

- 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.
- Dopo aver iniziato il processo di migrazione assistita, non è possibile ripristinarlo. Dovrai attendere 90 giorni fino alla scadenza del processo se desideri invece passare alla procedura standard.

Argomenti

Considerazioni

Prima di passare da un'organizzazione che supporta solo le funzionalità di fatturazione consolidate a un'organizzazione che supporta tutte le funzionalità, considera quanto segue:

Gli account invitati devono approvare la migrazione

Quando avvii la procedura per abilitare tutte le funzionalità, AWS Organizations invia una richiesta a tutti gli account membri che hai invitato a far parte della 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.

Agli account invitati viene notificato quale set di funzionalità è attualmente abilitato

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. Puoi continuare a invitare gli account a fa parte dell'organizzazione abilitando tutte le caratteristiche.

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.

Il processo di creazione degli account in un'organizzazione non è influenzato dalla migrazione

È possibile continuare a creare account nell'organizzazione. Questo processo non è influenzato da questa modifica.

Il ruolo **`AWSServiceRoleForOrganizations`** collegato al servizio è obbligatorio

AWS Organizations verifica che a ogni account membro sia associato un ruolo collegato al servizio 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 creato utilizzando AWS Organizations, quell'account riceve un invito specifico a ricreare quel ruolo. Tutti questi inviti devono essere accettati affinché l'organizzazione possa completare il processo di abilitazione di tutte le caratteristiche.

Processo di migrazione standard per abilitare tutte le funzionalità con Organizations

Questo argomento descrive come abilitare tutte le funzionalità con il processo di migrazione standard.

Fase 1: Richiedere agli account invitati di approvare la migrazione (account di gestione)

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. 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 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 tutti gli account invitati (non creati) dell'organizzazione chiedendo l'approvazione per abilitare tutte le funzionalità dell'organizzazione. Se disponi di account creati utilizzando AWS Organizations e l'amministratore dell'account membro ha eliminato il ruolo collegato al servizio denominato`AWSServiceRoleForOrganizations`, AWS Organizations invia all'account 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.

- AWS SDKs: 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 Passaggio 3: finalizza il processo di migrazione per abilitare tutte le funzionalità (account di gestione).

Passaggio 2: approva la richiesta per abilitare tutte le funzionalità o per ricreare il ruolo collegato al servizio (account invitato)

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 il tuo account è stato invece creato utilizzando AWS Organizations e hai eliminato il ruolo `AWSServiceRoleForOrganizations` collegato al servizio, riceverai solo un invito a 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 funzionalità del tuo account membro, l'account membro deve disporre delle seguenti autorizzazioni:

- `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 da AWS Organizations console.AWS Organizations 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"
            }
        ]
    }
}
```

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

Passaggio 3: finalizza il processo di migrazione per abilitare tutte le funzionalità (account di gestione)

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. 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 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"
            }
        ]
    }
}
```

- AWS SDKs:
  - ListHandshakesForOrganization
  - AcceptHandshake

Processo di migrazione assistita per abilitare tutte le funzionalità con Organizations

Se sei un cliente Enterprise, può essere difficile completare il processo di migrazione standard a causa dell'elevato numero di account che potresti gestire. Ad esempio, potresti avere difficoltà

a ottenere l'approvazione per la migrazione di tutti gli account invitati in organizzazioni di grandi dimensioni.

La migrazione assistita aiuta in questo processo consentendo ai clienti con un piano Enterprise Support di richiedere la AWS migrazione della propria organizzazione a tutte le funzionalità per conto dell'utente. Questo processo richiede la firma di un contratto che attesti la proprietà di tutti gli account, seguito da un periodo di attesa di 14 giorni. Questo periodo di attesa consente agli account di lasciare l'organizzazione, se lo desiderano, prima che la migrazione a tutte le funzionalità abbia effetto.

AWS Management Console

Per migrare a tutte le funzionalità con la migrazione assistita

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 Impostazioni scegli Abilita tutte le funzionalità, quindi seleziona Migrazione assistita.
3. Leggi i termini e le condizioni del contratto, scegli Accetta e scegli Inizia processo per abilitare tutte le funzionalità per avviare la migrazione.

> **Note**
>
> L'avvio del processo di migrazione assistita ha la precedenza sul processo di migrazione standard
> Se attualmente state abilitando tutte le funzionalità utilizzando la procedura di migrazione standard, questa verrà annullata e verrà avviato il processo di migrazione assistita.
> Il processo di migrazione assistita è unidirezionale e non può essere ripristinato
> Dopo aver iniziato il processo di migrazione assistita, non è possibile ripristinarlo. Dovrai attendere 90 giorni fino alla scadenza del processo se desideri invece passare alla procedura standard.

Se utilizzi la migrazione assistita, non devi preoccuparti di accedere al tuo account invitato come utente root per accettare la migrazione a tutte le funzionalità.

Puoi contattare il tuo Technical Account Manager (TAM) per i dettagli esatti, lo stato di avanzamento e le tempistiche della migrazione assistita.

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. 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). 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.

- AWS SDKs: DescribeOrganization

Eliminazione di un'organizzazione con AWS Organizations

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 autonomo e non Account AWS è più gestito da. AWS Organizations Sono quindi disponibili tre opzioni:

- Puoi continuare a usarlo come account autonomo
- Puoi usarlo per creare un'organizzazione diversa
- Puoi accettare un invito da un'altra organizzazione per aggiungere l'account a quell'organizzazione come account membro.

Argomenti

- Considerazioni

- Eliminazione di un'organizzazione

Considerazioni

Le organizzazioni eliminate non possono essere recuperate

Se elimini un'organizzazione, non puoi ripristinarla. Se hai creato delle policy all'interno dell'organizzazione, anch'esse verranno eliminate e non potrai recuperarle.

Le organizzazioni possono essere eliminate solo dopo che tutti gli account dei membri sono stati rimossi

Puoi eliminare un'organizzazione solo dopo avere rimosso tutti gli account membri. Se hai creato alcuni dei tuoi account membro utilizzando AWS Organizations, ti potrebbe essere impedito di rimuovere tali account. 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 Uscire da un'organizzazione da un account membro con AWS Organizations.

Gli account dei membri in uno stato «sospeso» non possono essere rimossi da un'organizzazione

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.

La rimozione dell'account di gestione da un'organizzazione eliminando l'organizzazione può influire sull'account 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 il funzionamento di un'organizzazione, quindi se rimuovi un account da un'organizzazione che supporta IAM Identity Center, gli utenti di quell'account non possono più utilizzare quel servizio.

L'account di gestione di un'organizzazione non è mai influenzato dalle politiche di controllo del servizio (SCPs), quindi non vi è alcuna modifica nelle autorizzazioni dopo che non SCPs sono più disponibili.

Esegui il backup di tutti i report

Assicurati di esportare o eseguire il backup dei report dall'account di gestione, in particolare dei report di fatturazione. I report e la cronologia a livello organizzativo non vengono archiviati quando elimini un'organizzazione. Tutti i dati sui costi (ad esempio il set di dati Cost Explorer) vengono eliminati. Si consiglia di eseguire un'esportazione completa di tutta la cronologia di fatturazione.

Per ulteriori informazioni, consulta Cost and Usage Reports, Cost Explorer Reports, Savings Plans Reports e utilizzo e copertura delle istanze riservate (RI).

Eliminazione di un'organizzazione

Utilizzare la procedura seguente per eliminare un'organizzazione che ripristina il precedente account di gestione in uno standalone Account AWS 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. 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. Prima di poter eliminare l'organizzazione, occorre innanzitutto rimuovere tutti gli account da essa. Per ulteriori informazioni, consulta Rimuovere un account membro da un'organizzazione con AWS Organizations.
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 in un'organizzazione con AWS Organizations.

AWS CLI & AWS SDKs

Gli esempi di codice seguenti mostrano come utilizzare `DeleteOrganization`.

.NET

SDK per .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing organization using the AWS
/// Organizations Service.
/// </summary>
public class DeleteOrganization
{
    /// <summary>
    /// Initializes the Organizations client and then calls
    /// DeleteOrganizationAsync to delete the organization.
    /// </summary>
    public static async Task Main()
```

```
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var response = await client.DeleteOrganizationAsync(new
DeleteOrganizationRequest());

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine("Successfully deleted organization.");
            }
            else
            {
                Console.WriteLine("Could not delete organization.");
            }
        }
    }
```

- Per i dettagli sull'API, DeleteOrganizationconsulta AWS SDK per .NET API Reference.

CLI

AWS CLI

Per eliminare un'organizzazione

L'esempio seguente mostra come eliminare un'organizzazione. Per eseguire questa operazione, devi essere un amministratore dell'account principale dell'organizzazione. L'esempio presuppone che in precedenza siano stati rimossi tutti gli account dei membri e le politiche dall'organizzazione: OUs

```
aws organizations delete-organization
```

- Per i dettagli sull'API, consulta DeleteOrganization AWS CLICommand Reference.

Gestione degli account in un'organizzazione con AWS Organizations

An Account AWSè un contenitore per AWS le tue risorse. Crei e gestisci AWS le tue risorse in un Account AWS.

Questo argomento descrive come gestire gli account per AWS Organizations.

Argomenti

Gestione dell'account di gestione con AWS Organizations

Un account di gestione è l'account Account AWS che usi per creare la tua organizzazione.

L'account di gestione è il proprietario finale dell'organizzazione e detiene il controllo finale sulle politiche di sicurezza, infrastruttura e finanza. Questo account ha la funzione di conto di pagamento ed è responsabile del pagamento di tutti gli addebiti maturati dai conti della sua organizzazione.

Questo argomento descrive come gestire l'account di gestione con. AWS Organizations

Argomenti

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

L'account di gestione è fondamentale per tutte le attività amministrative menzionate, come la gestione degli account, le politiche, l'integrazione con altri AWS servizi, 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 tue AWS risorse Account AWS in altri membri dell'organizzazione e tienile lontane dall'account di gestione. Un motivo importante per conservare le risorse in altri account è che le politiche di controllo del servizio Organizations (SCPs) 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.

Per un elenco delle attività che devono essere richiamate dall'account di gestione, vedi Operazioni che è possibile chiamare solo dall'account di gestione dell'organizzazione.

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 SCPs 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, è possibile registrare più amministratori delegati per i servizi che supportano questa funzionalità, ad esempio per la condivisione del software all'interno dell'organizzazione o AWS Service Catalog AWS CloudFormation StackSets per la creazione e la distribuzione di stack.

Per ulteriori informazioni, consulta Security Reference Architecture, Organizzazione AWS dell'ambiente utilizzando più account e Servizi AWS che puoi usare con AWS Organizations per suggerimenti sulla registrazione degli account dei membri come amministratore delegato per vari servizi. AWS

Per ulteriori informazioni sulla configurazione degli amministratori delegati, consulta Enabling a delegated admin account for Gestione dell'account AWS e Amministratore delegato per AWS Organizations.

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.

Chiudi l'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'AWS account.

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. Per fare ciò, vai alla AWS Organizations console. Se disponi di un account membro ancora attivo, dovrai seguire le indicazioni fornite Rimuovere un account membro da un'organizzazione prima di poter passare alla fase successiva. Chiusura di un account membro in un'organizzazione con AWS Organizations
3. Nella barra di navigazione nell'angolo in alto a destra, scegli il nome o il numero del tuo account, quindi scegli Account.
4. Nella pagina Account, scegli il pulsante Chiudi account. Leggi e assicurati di aver compreso la guida alla 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 in AWS CLI o da un'operazione API di uno dei AWS SDKs. È possibile eseguire questa operazione solo utilizzando AWS Management Console.

Gestione degli account dei membri con AWS Organizations

Un account membro è un account Account AWS, diverso dall'account di gestione, che fa parte di un'organizzazione.

Questo argomento descrive come gestire gli account dei membri con AWS Organizations.

Argomenti

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

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

Durante la scalabilità, prima di creare nuovi account, assicurati che non esistano già account con esigenze simili, per evitare inutili duplicazioni. Account AWS dovrebbe 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 e limiti di servizio 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, eviterai di incorrere in costi legati all'utilizzo delle risorse e di raggiungere i limiti delle CloseAccount API.

Abilita la gestione degli accessi root per semplificare la gestione delle credenziali degli utenti root per gli account dei membri

Ti consigliamo di abilitare la gestione dell'accesso root per aiutarti a monitorare e rimuovere le credenziali degli utenti root per gli account dei membri. La gestione degli accessi root impedisce il recupero delle credenziali degli utenti root, migliorando la sicurezza degli account nell'organizzazione.

- Rimuovi le credenziali dell'utente root per gli account dei membri per impedire l'accesso all'utente root. Ciò impedisce inoltre il ripristino degli account membro dell'utente root.
- Si supponga di disporre di una sessione privilegiata per eseguire le seguenti attività sugli account dei membri:
  - Rimuovi una policy del bucket configurata non correttamente che impedisce a tutti i principali di accedere al bucket Amazon S3.
  - Elimina una policy basata sulle risorse Amazon Simple Queue Service che nega a tutti i principali l'accesso a una coda Amazon SQS.

- Consenti a un account membro di recuperare le credenziali dell'utente root. La persona con accesso alla casella di posta elettronica dell'utente root di per l'account membro può reimpostare la password dell'utente root e accedere come utente root dell'account membro.

Dopo aver abilitato la gestione dell'accesso root, gli account membro appena creati non secure-by-default dispongono di credenziali utente root, il che elimina la necessità di ulteriori misure di sicurezza, come l'MFA dopo il provisioning.

Per ulteriori informazioni, consulta Centralizzare le credenziali utente root per gli account dei membri nella Guida per l'utente.AWS Identity and Access Management

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, il seguente SCP impedisce all'utente root di qualsiasi account membro di effettuare chiamate API di AWS servizio tranne «Aggiornamento di una policy del bucket S3 non configurata correttamente e nega l'accesso a tutti i principali» (una delle azioni che richiede credenziali root). Per ulteriori informazioni, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

JSON

```
{
 "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 di un account membro in un'organizzazione con AWS Organizations

Questo argomento descrive come creare Account AWS all'interno dell'organizzazione in AWS Organizations. Per informazioni sulla creazione di un singolo Account AWS, consulta il Getting Started Resource Center.

Considerazioni prima di creare un account membro

Organizations crea automaticamente il ruolo IAM **`OrganizationAccountAccessRole`** per l'account membro

Quando crei un account membro nella tua organizzazione, Organizations crea automaticamente il ruolo IAM `OrganizationAccountAccessRole` nell'account membro che consente agli utenti e ai ruoli dell'account di gestione di esercitare il pieno controllo amministrativo sull'account membro. Tutti gli account aggiuntivi collegati alla stessa policy gestita verranno aggiornati automaticamente

ogni volta che la policy viene aggiornata. Questo ruolo è soggetto a qualsiasi politica di controllo del servizio (SCPs) che si applica all'account membro.

Organizations crea automaticamente il ruolo collegato al servizio **`AWSServiceRoleForOrganizations`** per l'account membro

Quando crei un account membro nella tua organizzazione, Organizations crea automaticamente un ruolo collegato al servizio `AWSServiceRoleForOrganizations` nell'account membro che consente l'integrazione con servizi selezionati AWS . È necessario configurare gli altri servizi per consentire l'integrazione. Per ulteriori informazioni, consulta AWS Organizations e ruoli collegati ai servizi.

Gli account dei membri possono essere creati solo nella directory principale di un'organizzazione

Gli account dei membri di un'organizzazione possono essere creati solo nella radice di un'organizzazione. Dopo aver creato un account membro principale di un'organizzazione, puoi spostarlo da un account all'altro OUs. Per ulteriori informazioni, consulta Spostamento degli account in un'unità organizzativa (OU) o tra la radice e OUs con AWS Organizations.

Le politiche allegate alla radice vengono applicate immediatamente

Se hai delle politiche collegate alla directory principale, tali politiche si applicano immediatamente a tutti gli utenti e i ruoli dell'account creato.

Se hai abilitato il service trust per un altro AWS servizio per la tua organizzazione, quel servizio affidabile può creare ruoli collegati al servizio o eseguire azioni in qualsiasi account membro dell'organizzazione, incluso l'account creato.

Gli account dei membri devono attivare la ricezione di e-mail di marketing

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

Gli account dei membri per le organizzazioni gestite da AWS Control Tower devono essere creati in AWS Control Tower

Se la tua organizzazione è gestita da AWS Control Tower, ti consigliamo di creare i tuoi account membro utilizzando AWS Control Tower Account Factory nella AWS Control Tower console o utilizzando il AWS Control Tower APIs.

Se crei un account membro in Organizations quando l'organizzazione è gestita da AWS Control Tower, l'account non verrà registrato con AWS Control Tower. Per ulteriori informazioni, consulta Riferimento alle risorse esterne a AWS Control Tower nella Guida per l'utente di AWS Control Tower .

Creazione di un account membro

Dopo aver effettuato l'accesso all'account di gestione dell'organizzazione, puoi creare account membro che fanno parte della tua organizzazione.

Quando crei un account utilizzando la procedura seguente, copia AWS Organizations automaticamente le seguenti informazioni di contatto principale dall'account di gestione all'account del nuovo membro:

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

Organizations copia anche il linguaggio di comunicazione e le informazioni di Marketplace (in alcuni casi il fornitore dell'account Regioni AWS) dall'account di gestione.

> **Autorizzazioni minime**
>
> Per creare un account membro nell'organizzazione, è necessario disporre delle seguenti autorizzazioni:
>
> - `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations
> - `organizations:CreateAccount`
> - `iam:CreateServiceLinkedRole`

AWS Management Console

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

1. Accedi alla AWS Organizations console . 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 nome Account 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 si specifica un nome, AWS Organizations assegna 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 Account AWS (Crea).

   - 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.
- Puoi anche controllare il AWS CloudTrail registro per verificare se la creazione dell'account è avvenuta con successo. Per ulteriori informazioni, consulta Registrazione e monitoraggio AWS Organizations.
- Se l'errore persiste, contatta Supporto AWS.

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 dei membri in un'organizzazione con AWS Organizations.

AWS CLI & AWS SDKs

Gli esempi di codice seguenti mostrano come utilizzare `CreateAccount`.

.NET

SDK per .NET

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new AWS Organizations account.
/// </summary>
public class CreateAccount
{
    /// <summary>
    /// Initializes an Organizations client object and uses it to create
```

```
        /// the new account with the name specified in accountName.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var accountName = "ExampleAccount";
            var email = "someone@example.com";

            var request = new CreateAccountRequest
            {
                AccountName = accountName,
                Email = email,
            };

            var response = await client.CreateAccountAsync(request);
            var status = response.CreateAccountStatus;

            Console.WriteLine($"The staus of {status.AccountName} is
{status.State}.");
        }
    }
```

- Per i dettagli sull'API, consulta la CreateAccountsezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Per creare un account membro che faccia automaticamente parte dell'organizzazione

L'esempio seguente mostra come creare un account membro in un'organizzazione. L'account membro è configurato con il nome Account di produzione e l'indirizzo e-mail susan@example.com. Organizations crea automaticamente un ruolo IAM utilizzando il nome predefinito di OrganizationAccountAccessRole perché il parametro RoleName non è specificato. Inoltre, l'impostazione che consente agli utenti o ai ruoli IAM con autorizzazioni sufficienti di accedere ai dati di fatturazione dell'account viene impostata sul valore predefinito di ALLOW perché il IamUserAccessToBilling parametro non è specificato. Organizations invia automaticamente a Susan un'e-mail di «Benvenuto a AWS»:

```
aws organizations create-account --email susan@example.com --account-
name "Production Account"
```

L'output include un oggetto di richiesta che mostra che lo stato è ora`IN_PROGRESS`:

```
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

Successivamente è possibile interrogare lo stato corrente della richiesta fornendo il valore di risposta Id al describe-create-account-status comando come valore per il create-account-request-id parametro.

Per ulteriori informazioni, consulta Creare un AWS account nella tua organizzazione nella AWS Organizations Users Guide.

- Per i dettagli sull'API, consulta CreateAccount AWS CLICommand Reference.

Accesso agli account dei membri in un'organizzazione con AWS Organizations

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 assegnarlo in modo uniforme in tutti gli account. AWS Organizations non crea altri utenti o ruoli.

Per accedere all'account nell'organizzazione, è necessario utilizzare uno dei seguenti metodi:

> **Autorizzazioni minime**
>
> Per accedere a un account Account AWS da qualsiasi altro account della tua organizzazione, devi disporre delle seguenti autorizzazioni:

- `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

Using the root user (Not recommended for everyday tasks)

Quando crei un nuovo account membro nella tua organizzazione, per impostazione predefinita l'account non ha credenziali utente root. Gli account membri non possono accedere al proprio utente root o eseguirne il recupero della password a meno che non sia abilitato il recupero dell'account.

È possibile centralizzare l'accesso root per gli account dei membri per rimuovere le credenziali dell'utente root per gli account membro esistenti nell'organizzazione. L'eliminazione delle credenziali dell'utente root rimuove la password dell'utente root, le chiavi di accesso, i certificati di firma e disattiva l'autenticazione a più fattori (MFA). Questi account membri non dispongono di credenziali dell'utente root, non possono accedere come utente root e non possono recuperare la password dell'utente root. Per impostazione predefinita, i nuovi account creati in Organizations non hanno credenziali dell'utente root.

Rivolgiti all'amministratore se devi eseguire un'operazione che richiede le credenziali dell'utente root su un account membro in cui non sono presenti le credenziali dell'utente root.

Per accedere al proprio account membro come utente root, è necessario eseguire la procedura 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.

Se devi accedere a un account membro utilizzando l'utente root, segui queste best practice:

- Non utilizzare l'utente root per accedere al tuo account se non per creare altri utenti e ruoli con autorizzazioni più limitate. Quindi accedi come uno di questi utenti o questi ruoli.
- Abilita l'autenticazione a più fattori (MFA) sull'utente root. Reimposta la password e assegna un dispositivo MFA all'utente root.

Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM. Per ulteriori consigli sulla sicurezza degli utenti root, consulta le migliori pratiche per l'utente root Account AWS nella IAM User Guide.

Using trusted access for IAM Identity Center

Utilizza AWS IAM Identity Centere abilita l'accesso affidabile per IAM Identity Center con AWS Organizations. Ciò consente agli utenti di accedere al portale di AWS accesso con le proprie credenziali aziendali e accedere alle risorse nell'account di gestione assegnato o negli account membro.

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.

Using the IAM role OrganizationAccountAccessRole

Se si crea un account utilizzando gli strumenti forniti come parte di AWS Organizations, è possibile accedere all'account utilizzando il ruolo preconfigurato denominato `OrganizationAccountAccessRole` che esiste in tutti i nuovi account creati in questo modo. Per ulteriori informazioni, consulta Accedere a un account membro che ha OrganizationAccountAccessRole con AWS Organizations.

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 OrganizationAccountAccessRole di un account invitato con AWS Organizations.

Una volta creato il ruolo, è possibile accedervi tramite le fasi in Accedere a un account membro che ha OrganizationAccountAccessRole con AWS Organizations.

Argomenti

Creazione OrganizationAccountAccessRole di un account invitato con AWS Organizations

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 Accedere a un account membro che ha OrganizationAccountAccessRole con AWS Organizations.

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 di AWS Organizations amministratore 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. Scegli Next (Successivo).
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, quindi seleziona Crea policy.
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 ARNs.
14. Inserisci il numero ID dell'account AWS membro, quindi inserisci il nome del ruolo creato in precedenza nei passaggi da 1 a 8. Scegli Aggiungi ARNs.
15. Se si concede l'autorizzazione per assumere il ruolo in più account membri, ripetere le fasi 14 e 15 per ogni account.
16. Scegli Next (Successivo).
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 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 URLs quello acquisito nel passaggio 9 per accedere al ruolo di ciascun 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 Accedere a un account membro che ha OrganizationAccountAccessRole con AWS Organizations.

Accedere a un account membro che ha OrganizationAccountAccessRole con AWS Organizations

Quando crei un account membro utilizzando la AWS Organizations console, crea AWS Organizations 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 OrganizationAccountAccessRole di un account invitato con AWS Organizations.

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 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 Visual editor, scegli Scegli un servizio, inserisci **`STS`** nella casella di ricerca per filtrare l'elenco, quindi scegli l'opzione STS.
4. Nella sezione Azioni, inserisci **`assume`** nella casella di ricerca per filtrare l'elenco, quindi scegli l'AssumeRoleopzione.
5. Nella sezione Risorse, scegli Specifico, scegli Aggiungi ARNs
6. Nella sezione Specificare ARN, scegli Altro account per la risorsa in.
7. Inserisci l'ID dell'account membro che hai appena creato

8. Per Nome ruolo di risorsa con percorso, inserisci il nome del ruolo che hai creato nella sezione precedente (ti consigliamo di assegnargli un nome`OrganizationAccountAccessRole`).
9. Scegliete Aggiungi ARNs quando nella finestra di dialogo viene visualizzato l'ARN corretto.
10. (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.
11. Scegli Next (Successivo).
12. Nella pagina Rivedi e crea, inserisci un nome per la nuova politica. Ad esempio: **`GrantAccessToOrganizationAccountAccessRole`**. Puoi anche aggiungere una descrizione opzionale.
13. Selezionare Crea policy per salvare la nuova policy gestita.
14. 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.
15. Nella scheda Permissions (Autorizzazioni), scegli Add permissions (Aggiungi autorizzazioni), quindi Attach policies (Collega policy).
16. (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 13. Puoi anche filtrare tutte le politiche AWS gestite scegliendo Tutti i tipi e quindi scegliendo Gestito dal cliente.
17. 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 AWS Organizations console utilizzando la seguente procedura.

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 AWS Organizations console, scegli il link che contiene il nome di accesso corrente, quindi scegli 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`***

Chiusura di un account membro in un'organizzazione con AWS Organizations

Se non hai più bisogno di un account membro nella tua organizzazione, puoi chiuderlo dalla AWS Organizations console seguendo le istruzioni riportate in questo argomento. 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 gestione AWS dell'account.

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

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 AWS Organizations console . Devi accedere come utente IAM o accedere come utente root (scelta non consigliata) nell'account di gestione dell'organizzazione.
2. Nella pagina Account AWS, individua e seleziona il nome dell'account membro che desideri chiudere. È possibile spostarsi nella gerarchia delle unità organizzative o visualizzare un elenco dei soli account senza la struttura dell'unità organizzativa.
3. Scegli Close (Chiudi) accanto al nome dell'account nella parte superiore della pagina. Questa opzione è disponibile solo quando un' AWS organizzazione è in modalità Tutte le funzionalità.

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

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

> **Note**
>
> Qualsiasi account membro che chiudi mostrerà un'`SUSPENDED`etichetta accanto al nome dell'account nella AWS Organizations console per un massimo di 90 giorni dopo la data di chiusura originale. Dopo 90 giorni, l'account del membro non verrà più visualizzato nel AWS Organizations.

Per chiudere un account membro dalla pagina Account

Facoltativamente, puoi chiudere un account AWS membro direttamente dalla pagina Account di. AWS Management Console Per ulteriori step-by-step informazioni, segui le istruzioni riportate in Chiudi e Account AWS nella Guida alla gestione AWS 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 SDKs: CloseAccount

Proteggere gli account dei membri dalla chiusura con AWS Organizations

Per proteggere gli account dei membri dalla chiusura accidentale, crea una policy IAM che specifichi quali account sono esenti. Questa politica impedisce la chiusura degli account dei membri protetti.

Crea una policy IAM per negare la chiusura dell'account utilizzando uno di questi metodi:

- Elenca esplicitamente gli account protetti nell'`Resource`elemento della policy utilizzando il loro. ARNs
- Etichetta i singoli account e utilizza la chiave di condizione `aws:ResourceTag` globale per impedire la chiusura degli account taggati.

> **Le politiche di controllo del servizio non possono proteggere gli account dei membri**
>
> Le politiche di controllo dei servizi (SCPs) non possono proteggere gli account dei membri perché SCPs non influiscono sui principi IAM nell'account di gestione.

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

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

Prevent member accounts with tags from getting closed

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"}
            }
        }
    ]
}
```

Prevent member accounts listed in this policy from getting closed

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"
            ]
        }
    ]
}
```

Rimuovere un account membro da un'organizzazione con AWS Organizations

La rimozione di un account membro non chiude l'account, ma lo rimuove dall'organizzazione. L'account precedente diventa un account autonomo Account AWS 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.

Considerazioni

I ruoli di accesso IAM creati dall'account di gestione non vengono eliminati automaticamente

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.

Puoi rimuovere un account dalla tua organizzazione solo se l'account dispone delle informazioni necessarie per funzionare come account autonomo

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 AWS Organizations console, l'API o AWS CLI i comandi, tutte le informazioni richieste per gli account autonomi non vengono raccolte automaticamente.

Per ogni account che desideri rendere indipendente, devi 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 qualsiasi AWS attività fatturabile (non del piano AWS gratuito) che si verifica quando l'account non è collegato a un'organizzazione. Per rimuovere un account che non dispone ancora di queste informazioni, completa le operazioni riportate in Uscire da un'organizzazione da un account membro con AWS Organizations.

Devi attendere almeno sette giorni dopo la creazione dell'account

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.

Il proprietario dell'account che esce diventa responsabile di tutti i nuovi costi maturati

Nel momento in cui l'account lascia con successo l'organizzazione, il proprietario dell'account Account AWS diventa responsabile di tutti i nuovi AWS costi maturati e viene utilizzato il metodo di pagamento dell'account. L'account di gestione dell'organizzazione non è più responsabile.

L'account non può essere un account amministratore delegato per alcun AWS servizio abilitato per l'organizzazione

L'account che desideri rimuovere non deve essere un account amministratore delegato per alcun AWS servizio 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 di amministratore delegato per un AWS servizio, consulta la documentazione relativa al servizio.

L'account non ha più accesso ai dati sui costi e sull'utilizzo

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.

I tag allegati all'account vengono eliminati

Quando un account membro lascia un'organizzazione, tutti i tag associati all'account vengono eliminati.

I responsabili dell'account non sono più influenzati dalle politiche dell'organizzazione

I principali nell'account non sono più interessati da alcuna policy applicata nell'organizzazione. Ciò significa che le restrizioni imposte da SCPs sono scomparse e gli utenti e i ruoli dell'account

potrebbero avere più autorizzazioni rispetto a prima. Altri tipi di policy dell'organizzazione non possono più essere applicati o elaborati.

L'account non è più coperto da accordi organizzativi

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. Un elenco degli accordi organizzativi attivi può essere visualizzato nella AWS Artifact console nella pagina AWS Artifact Organization Agreements.

L'integrazione con altri servizi potrebbe essere disabilitata

L'integrazione con altri servizi potrebbe essere disabilitata. Se rimuovi un account da un'organizzazione in cui è abilitata l'integrazione con un AWS servizio, gli utenti di quell'account non possono più utilizzare quel servizio.

Rimuovere un account membro da un'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.

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. 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 seleziona la casella di controllo
   ☑
   accanto all'account membro che desideri rimuovere dall'organizzazione. È possibile navigare nella gerarchia delle unità organizzative o abilitare Visualizza Account AWS solo per visualizzare un elenco semplice di account senza la struttura delle unità organizzative. 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 OUs (scegliere il▶)
   per trovare l'account desiderato.
3. Scegli Actions (Operazioni), quindi in Account AWS scegli Remove from organization (Rimuovi dall'organizzazione).
4. Nella sezione Rimuovere l'account 'nome-account' (# account-id-num) dall'organizzazione? nella finestra di dialogo, scegli Rimuovi account.

5. Se AWS Organizations non riesci a rimuovere uno o più account, in genere è perché non hai fornito tutte le informazioni necessarie affinché l'account funzioni come account autonomo. 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 vedi il link Copia, usa questo link per andare alla AWS pagina di registrazione e completare i passaggi di registrazione mancanti. 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. Dopo aver completato l'ultima fase di registrazione, reindirizza AWS automaticamente il browser alla AWS Organizations console dell'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.

- AWS SDKs: 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 Uscire da un'organizzazione da un account membro con AWS Organizations.

Uscire da un'organizzazione da un account membro con AWS Organizations

Quando accedi a un account membro, puoi lasciare un'organizzazione. 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.

Considerazioni

Lo stato di un account presso un'organizzazione influisce sui dati visibili su costi e utilizzo

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.

L'account non è più coperto dagli accordi organizzativi che sono stati accettati per suo conto

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 organizzativi nella AWS Artifact console nella pagina AWS Artifact Organization Agreements. 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.

Abbandona un'organizzazione da un account membro

Per lasciare un'organizzazione, completare la procedura seguente.

> **Autorizzazioni minime**
>
> Per lasciare un'organizzazione , 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 AWS Organizations console 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 hai accesso alla password dell'utente root in un account membro creato utilizzando AWS Organizations. Se necessario, recupera la password dell'utente root seguendo la procedura descritta in Utilizzo dell'utente root (opzione non consigliata per le attività quotidiane) inAccesso agli account dei membri in un'organizzazione con AWS Organizations.
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. Dopo aver confermato, verrai reindirizzato alla pagina Getting Started della AWS Organizations console, dove potrai visualizzare tutti gli inviti in sospeso relativi al tuo account a entrare 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.

   Se non vedi il link Completa la procedura di registrazione dell'account, utilizza questo link per accedere alla AWS pagina di registrazione e completa i passaggi di registrazione mancanti.

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. Verrai reindirizzato alla pagina Guida introduttiva della AWS Organizations console, dove puoi visualizzare tutti gli inviti in sospeso relativi al tuo account a entrare a 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.
- AWS SDKs: 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 dei membri possono anche essere rimossi da un utente nell'account di gestione con instead. remove-account-from-organization Per ulteriori informazioni, consulta Rimuovere un account membro da un'organizzazione.

Aggiornamento del nome dell'account di un account membro con AWS Organizations

Quando accedi all'account di gestione della tua organizzazione, puoi aggiornare il nome dell'account di un account membro. Per informazioni su come aggiornare il nome dell'account di un membro, segui la procedura riportata in Aggiornare il nome dell'account per qualsiasi Account AWS membro dell'organizzazione nella Guida Gestione dell'account AWS di riferimento.

Aggiornamento dell'indirizzo e-mail dell'utente root (indirizzo per un account membro con AWS Organizations

Per una maggiore sicurezza e resilienza amministrativa, i responsabili IAM dell'account di gestione (che dispongono delle autorizzazioni IAM necessarie) possono aggiornare centralmente l'indirizzo e-mail di un utente root () (noto anche come indirizzo e-mail principale) per qualsiasi account membro senza dover accedere a ciascun account singolarmente. Ciò offre agli amministratori dell'account di gestione (o di un account amministratore delegato) un maggiore controllo sugli account dei membri. Garantisce inoltre che gli indirizzi e-mail degli utenti root Gli di qualsiasi account membro del tuo account AWS Organizations possano essere mantenuti aggiornati, anche quando potresti aver perso l'accesso all'indirizzo e-mail dell'utente root originale, all'indirizzo e-mail o alle credenziali amministrative.

Quando l'indirizzo e-mail dell'utente root L'indirizzo viene modificato centralmente dall'amministratore dell'account di gestione, sia la password che la configurazione MFA rimarranno le stesse di prima della modifica. Tieni presente che l'autenticazione a più fattori può essere aggirata da un utente che controlla l'indirizzo e-mail dell'utente root di un account, l'indirizzo e-mail di contatto principale.

Per aggiornare l'indirizzo e-mail dell'utente root (indirizzo) di un account membro dell'organizzazione, l'organizzazione deve aver precedentemente abilitato la modalità tutte le funzionalità. AWS Organizations in modalità di fatturazione consolidata o in account che non fanno parte di un'organizzazione, non possono aggiornare centralmente l'indirizzo e-mail dell'utente root (indirizzo e-mail). Gli utenti che desiderano modificare l'indirizzo e-mail dell'utente root (indirizzo per gli account non supportati dall'API) devono continuare a utilizzare la Console di fatturazione per gestire l'indirizzo e-mail dell'utente root (indirizzo e-mail).

Per step-by-step istruzioni su come aggiornare l'indirizzo e-mail dell'utente root dell'account membro (indirizzo e-mail e-mail dell'utente root per qualsiasi Account AWS utente dell'organizzazione nella Guida Gestione dell'account AWS di riferimento.

Gestione degli inviti all'account con AWS Organizations

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. Utilizza la AWS Organizations console per avviare e gestire gli inviti da inviare ad altri account. Puoi inviare un invito ad altri account solo dall'account di gestione della tua organizzazione.

Quando inviti un account, AWS Organizations invia un invito al proprietario dell'account, che può decidere di accettare o rifiutare l'invito.

Se sei l'amministratore di un Account AWS, puoi anche accettare o rifiutare un invito da un'organizzazione. Se accetti, l'account diventa un membro di tale organizzazione.

Per creare un account che fa automaticamente parte di un'organizzazione, consultaCreazione di un account membro in un'organizzazione con AWS Organizations.

> **Important**
>
> 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 trovarsi in un'organizzazione con account della partizione Regioni Cina o account nella partizione AWS GovCloud (US) Regioni.

Argomenti

Considerazioni

Limitazioni al numero di inviti che puoi inviare al giorno

Per le limitazioni sul numero di inviti che puoi inviare ogni giorno, consultaValori 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 azzerato se l'account invitato rifiuta, l'account di gestione annulla l'invito o l'invito scade.

Un account può entrare a far parte di una sola organizzazione

Un account può entrare a far parte di una sola organizzazione. Se ricevi più inviti, puoi accettarne solo uno.

La cronologia e i report di fatturazione rimangono nell'account di gestione

La cronologia di fatturazione e i report per tutti gli account rimangono nell'account di gestione di un'organizzazione. Prima di trasferire l'account in una nuova organizzazione, esporta o esegui il backup delle cronologie di fatturazione e dei report per tutti gli account membro che desideri conservare. Ciò potrebbe includere report sui costi e sull'utilizzo, report Cost Explorer, report Savings Plans e utilizzo e copertura delle istanze riservate (RI).

L'account di gestione è responsabile di tutti gli addebiti maturati dagli account dei membri

Dopo che un account ha accettato l'invito a entrare a far parte di un'organizzazione, l'account di gestione dell'organizzazione diventa responsabile di tutti gli addebiti maturati 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.

Organizations crea automaticamente il ruolo collegato al servizio **`AWSServiceRoleForOrganizations`**

AWS Organizations crea un ruolo collegato al servizio chiamato `AWSServiceRoleForOrganizations` a supportare le integrazioni tra e altri servizi. AWS Organizations AWS Per ulteriori informazioni, consulta AWS Organizations e ruoli collegati ai servizi. L'account invitato deve avere questo ruolo se l'organizzazione supporta tutte le funzionalità. Puoi eliminare questo ruolo se l'organizzazione supporta solo il set di funzionalità di fatturazione consolidata. Se elimini questo ruolo e successivamente abiliti tutte le funzionalità dell'organizzazione, AWS Organizations ricrea questo ruolo per l'account.

Organizations non crea automaticamente il ruolo IAM **`OrganizationAccountAccessRole`**

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 OrganizationAccountAccessRole di un account invitato con AWS Organizations.

> **Note**
>
> Quando crei un account nella tua organizzazione invece di invitare un account esistente a iscriversi, crea AWS Organizations automaticamente il ruolo IAM `OrganizationAccountAccessRole` per impostazione predefinita.

Le policy allegate alla root o all'unità organizzativa che contengono l'account vengono applicate immediatamente

Se sono state associate delle politiche alla radice o all'unità organizzativa (OU) che contiene l'account invitato, tali politiche si applicano immediatamente a tutti gli utenti e i ruoli dell'account invitato.

È possibile abilitare l'attendibilità del servizio per un altro AWS servizio 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.

Organizations con solo il set di funzionalità di fatturazione consolidata possono comunque invitare account

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.

Invio di inviti all'account con AWS Organizations

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 con AWS Organizations. 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 unirsi alla 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. 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. 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 Supporto AWS.

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 SDKs: InviteAccountToOrganization

Gestire gli inviti all'account in sospeso con AWS Organizations

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. 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 Invitations (Inviti).

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

   Se non riesci a visualizzare un invito, controlla se l'account invitato è l'account di gestione di un'altra organizzazione. Solo gli account membri e gli account autonomi possono ricevere inviti. Gli account di gestione non possono ricevere inviti.

   Se si desidera invitare un account che è un account di gestione di un'altra organizzazione, si consiglia di rendere tale account un account autonomo.

> **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 accanto 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 l'invito è stato annullato. 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 SDKs: ListHandshakesForOrganization, CancelHandshake

Accettare o rifiutare gli inviti all'account con AWS Organizations

Se ricevi un invito a entrare a far parte di un'organizzazione, puoi accettare o rifiutare l'invito.

Considerazioni

Lo stato di un account presso un'organizzazione influisce sui dati visibili su costi e utilizzo

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.

Solo gli account membri e gli account autonomi possono accettare o rifiutare un invito

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, tale account non potrà visualizzare l'invito finché non rimuoverà tutti gli account dei membri dall'organizzazione e non eliminerà l'organizzazione.

Accetta o rifiuta l'invito a un account

Per accettare o rifiutare l'invito, completa i seguenti passaggi.

Autorizzazioni minime

Per accettare o rifiutare un invito a far parte di un'organizzazione , è necessario disporre delle seguenti autorizzazioni:

- `organizations:ListHandshakesForAccount`— Obbligatorio 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 altri. AWS Organizations 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 SDKs: AcceptHandshake, DeclineHandshake

Esegui la migrazione di un account in un'altra organizzazione con AWS Organizations

Puoi migrare un uomo Account AWS da un'organizzazione all'altra in qualsiasi momento. Ad esempio, la migrazione di un account può essere utile in caso di fusione e acquisizione quando è necessario consolidare uno o più account Account AWS da più organizzazioni in un'unica organizzazione.

Qualunque sia il caso d'uso, la migrazione di un account tra organizzazioni richiede la rimozione dell'account dalla vecchia organizzazione, la trasformazione dell'account in un account autonomo e l'accettazione dell'invito della nuova organizzazione a entrare a far parte della nuova organizzazione. I tuoi carichi di lavoro e i tuoi servizi continueranno a funzionare in base alle tue specifiche durante la migrazione. Tuttavia, è importante essere consapevoli di eventuali dipendenze all'interno dell'organizzazione.

> **Note**
>
> Gli account chiusi o sospesi non possono essere migrati
> Non è possibile migrare un account chiuso o sospeso. Per riattivare un account, contatta. Supporto
> Età minima richiesta: sette giorni.
> Per migrare un account creato in un'organizzazione, è necessario attendere almeno sette giorni dalla creazione dell'account. Gli account invitati non sono soggetti a questo tempo di attesa.
> Replica dei dati tra account
> La seguente guida AWS prescrittiva fornisce informazioni sulle strategie per la replica dei dati tra Account AWS: replica delle risorse o migrazione tra. Account AWS

Cosa devi fare prima di migrare un account

Prima di effettuare la migrazione Account AWS da un'organizzazione all'altra, assicurati di aver completato i seguenti passaggi.

Passaggio 1: verifica di disporre delle autorizzazioni IAM necessarie per migrare un account

Fase 1

Assicurati di aver applicato le autorizzazioni necessarie per la migrazione di un account verso le rispettive organizzazioni.

Per lasciare un'organizzazione, devi disporre delle seguenti autorizzazioni:

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

Per ulteriori informazioni, consulta Abbandona un'organizzazione dal tuo account membro.

Per invitare un utente Account AWS a entrare a far parte di un'organizzazione, devi disporre delle seguenti autorizzazioni:

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

Per ulteriori informazioni, vedi Invitare un uomo Account AWS a entrare a far parte dell'organizzazione.

Per migrare un account, non è possibile disporre di policy IAM o policy di controllo dei servizi che impediscano la migrazione

Se sei l'account di gestione o un amministratore delegato, puoi controllare l'accesso alle AWS risorse collegando le politiche di autorizzazione alle identità IAM (utenti, gruppi e ruoli) all'interno di un'organizzazione. Per ulteriori informazioni, consulta le politiche IAM per. AWS Organizations

Prima di migrare un account:

- Verifica che non vi siano policy IAM o policy di controllo del servizio (SCPs) che ti impediscano di migrare l'account.
- Identifica le policy IAM e le policy di controllo dei servizi esistenti (SCPs) che devi replicare nell'organizzazione in cui stai migrando l'account.
- Identifica le policy IAM esistenti che specificano l'ID della tua organizzazione. Ad esempio, `aws:PrincipalOrgID`.

Per ulteriori informazioni, consulta Managing IAM policy nella IAM User Guide e Service control policies (SCPs).

Passaggio 2: verifica di aver rimosso le autorizzazioni IAM che consentono l'accesso al vecchio account di gestione

Fase 2

Assicurati di aver rimosso le autorizzazioni IAM che consentono l'accesso al vecchio account di gestione, ad esempio. `OrganizationAccountAccessRole`

Quando rimuovi un account membro da un'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.

Passaggio 3: verifica la verifica telefonica e il metodo di pagamento

Fase 3

L'account di migrazione deve funzionare come account autonomo per un periodo di tempo prima di migrare alla nuova organizzazione.

Per consentire a un account di funzionare come account autonomo, verifica quanto segue:

- Assicurati che la verifica telefonica sia up-to-date valida.
- Assicurati di aver aggiunto un metodo di pagamento valido per l'account per far fronte a eventuali addebiti sostenuti durante la migrazione dell'account.
- Se utilizzi la fatturazione come metodo di pagamento, assicurati che la fattura lo sia. up-to-date

Passaggio 4: Esegui il backup di tutti i report

Fase 4

Assicurati di esportare o eseguire il backup dei report dall'account di gestione, in particolare dei report di fatturazione. I report e la cronologia a livello organizzativo non vengono archiviati quando esegui

la migrazione di un account. Si consiglia di eseguire un'esportazione completa di tutta la cronologia di fatturazione. Puoi comunque accedere ai report relativi all'account dei membri, come la cronologia degli AWS CloudTrail eventi e la cronologia di fatturazione dell'account.

> **Important**
>
> Tutti i report e la cronologia a livello organizzativo, come le informazioni di fatturazione organizzative nell'account di gestione, verranno eliminati dopo la rimozione di un account da un'organizzazione.

Per ulteriori informazioni, consulta Cost and Usage Reports, Cost Explorer Reports, Savings Plans Reports e utilizzo e copertura delle istanze riservate (RI).

Fase 5: Verificare le dipendenze dell'organizzazione

Fase 5

Assicurati che l'account in fase di migrazione non abbia dipendenze relative all'organizzazione.

Dipendenze da controllare:

- Se l'account è un amministratore delegato, è necessario annullare la registrazione delle autorizzazioni di amministratore delegato prima di migrare l'account. Per ulteriori informazioni, consulta Servizi utilizzabili. AWS Organizations
- Se l'account è l'account di gestione, è necessario rimuovere tutti gli account dei membri dall'organizzazione ed eliminare l'organizzazione prima della migrazione. Dopo aver eliminato l'organizzazione, l'account di gestione funzionerà come account autonomo. Dopo la migrazione, l'account di gestione sarà un account membro della nuova organizzazione. Per ulteriori informazioni, vedere Eliminazione di un'organizzazione.
- Se alcune autorizzazioni IAM dipendono dall'account, dovrai modificare le autorizzazioni per la vecchia organizzazione dopo aver migrato l'account nella nuova organizzazione affinché la vecchia organizzazione funzioni come prima. Per ulteriori informazioni, consulta Gestione delle autorizzazioni di accesso per la tua organizzazione.
- Se utilizzi tag di account o unità organizzative (OU), dovrai ricreare i tag nella nuova organizzazione.

(Facoltativo) Passaggio 6: consulta le linee guida se utilizzi AWS Control Tower

(Facoltativo) Fase 6

Se stai migrando un account da o verso un'organizzazione gestita da AWS Control Tower, consulta la seguente Guida AWS prescrittiva: Esegui la migrazione di un account AWS membro da a. AWS Organizations AWS Control Tower

Cosa devi fare per migrare un account

Il processo di migrazione richiede che la nuova organizzazione invii un invito all'account di migrazione, che la vecchia organizzazione rimuova l'account di migrazione e che l'account di migrazione accetti l'invito della nuova organizzazione a entrare a far parte della nuova organizzazione.

Per migrare un account

1. Invia un invito dall'account di gestione della nuova organizzazione all'account di migrazione. È necessario inviare l'invito all'account prima che lasci la vecchia organizzazione. Questo aiuta a ridurre al minimo i costi sostenuti quando l'account in fase di migrazione funziona temporaneamente come account autonomo. Per informazioni su come invitare account, consulta Invitare un utente a entrare a far parte dell'organizzazione Account AWS.
2. Rimuovi l'account in fase di migrazione dalla vecchia organizzazione. Puoi rimuovere un account membro dalla tua organizzazione utilizzando l'account di gestione o lasciare un'organizzazione come account membro.
3. Accetta l'invito a entrare a far parte della nuova organizzazione. Per ulteriori informazioni, vedi Accettazione di un invito da un'organizzazione. Gli account migrati da un'altra organizzazione all'altra verranno aggiunti automaticamente alla cartella principale della nuova organizzazione. Prima di spostare un account in un'unità organizzativa (OU) della nuova organizzazione, si consiglia di verificare che l'account in fase di migrazione disponga dei criteri organizzativi e delle autorizzazioni dell'unità organizzativa appropriati.
4. Se si desidera migrare l'account di gestione, è necessario rimuovere tutti gli account dei membri dall'organizzazione ed eliminare l'organizzazione prima di migrare l'account di gestione nella nuova organizzazione. Dopo aver eliminato la vecchia organizzazione, l'account di gestione funzionerà come account autonomo e potrà accettare l'invito della nuova organizzazione a entrare a far parte della nuova organizzazione. Se accetti l'invito, l'account di gestione sarà un account membro della nuova organizzazione.

Cosa devi fare dopo la migrazione di un account

Dopo la migrazione del tuo account da un'organizzazione all'altra, assicurati di aver completato i seguenti passaggi.

Revisione successiva alla migrazione

1. Valuta tutte le configurazioni degli strumenti di fatturazione per l'account migrato, ad esempio categorie di costi, budget e allarmi di fatturazione.
2. Rivedi e aggiorna le seguenti informazioni monetarie per tutti gli account migrati da un'organizzazione all'altra:
   a. Se necessario, aggiorna le impostazioni fiscali sull'account.
   b. Assicurati che il Supporto piano di migrazione dell'account corrisponda all'account di pagamento della nuova organizzazione.
   c. Esamina tutte le possibili esenzioni fiscali che potresti voler applicare all'account che hai migrato.
3. Convalida e conferma le politiche IAM e le politiche di controllo del servizio esistenti (SCPs) per l'account migrato. Ad esempio, potrebbe essere necessario aggiornare l'ID dell'organizzazione per alcune policy IAM in modo che rispecchino la nuova organizzazione.
4. Aggiorna i tag di allocazione dei costi per la nuova organizzazione in cui hai migrato l'account. Dovrai aggiornare tutti i tag di allocazione dei costi precedenti raccolti dall'account che hai migrato.
5. Tutte le istanze riservate e i piani di risparmio verranno migrati insieme all'account. Questi non vengono mantenuti nella vecchia organizzazione. Contattateci Supporto se è necessario trasferirli alla vecchia organizzazione.

Visualizza i dettagli di un account in AWS Organizations

Quando accedi all'account di gestione dell'organizzazione nella AWS Organizations console, puoi visualizzare i dettagli relativi agli account dei membri.

> **Autorizzazioni minime**
>
> Per visualizzare i dettagli di un Account AWS, devi disporre delle seguenti autorizzazioni:
>
> - `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 AWS Organizations console . 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"
    }
}
```

- AWS SDKs:
  - ListAccounts
  - DescribeAccount

Esporta i dettagli per tutti gli account in AWS Organizations

Con AWS Organizations, gli utenti dell'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.

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

Esporta un elenco di tutti gli elementi della tua organizzazione Account AWS

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 i membri dell' Account AWS organizzazione

1. Accedi alla AWS Organizations console . 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 la AWS Management Console. Non è possibile esportare il file con estensione .csv dell'elenco degli account utilizzando la AWS CLI.

Aggiorna i contatti alternativi per un account in AWS Organizations

Puoi aggiornare i contatti alternativi per gli account all'interno della tua organizzazione utilizzando la console AWS Organizations o programmaticamente utilizzando la AWS CLI o. AWS SDKs Per informazioni su come aggiornare i contatti alternativi, consulta Aggiornare i contatti alternativi per tutti i contatti dell'organizzazione Account AWS nella Guida di riferimento per la gestione degli account. AWS

Aggiorna le informazioni di contatto principali per un account in AWS Organizations

Puoi aggiornare le informazioni di contatto principali per gli account all'interno della tua organizzazione utilizzando la console AWS Organizations o a livello di codice utilizzando la CLI AWS o. AWS SDKs Per informazioni su come aggiornare le informazioni di contatto principali, consulta Aggiornare il contatto principale per qualsiasi contatto dell'organizzazione Account AWS nell' AWSAccount Management Reference.

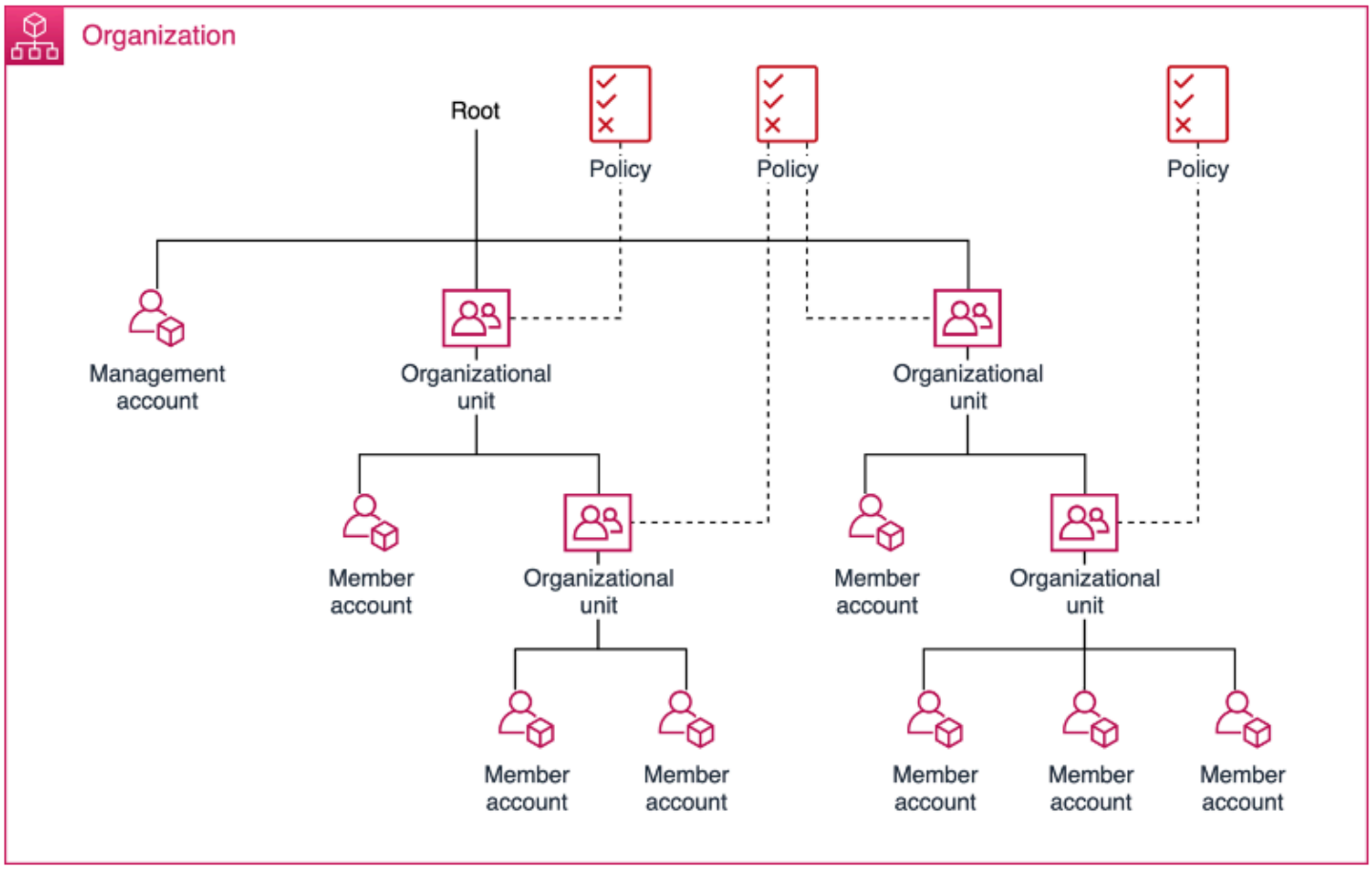
Aggiornamento Regioni AWS per un account in AWS Organizations

Puoi abilitare l'aggiornamento Regioni AWS per gli account all'interno della tua organizzazione utilizzando la AWS Organizations console. Per sapere come abilitare l'aggiornamento Regioni AWS, consulta Abilitare o disabilitare Regioni AWS nel tuo account nella Guida di riferimento alla gestione degli AWS account.

Gestione delle unità organizzative (OUs) con AWS Organizations

È possibile utilizzare le unità organizzative (OUs) per raggruppare gli account e amministrarli come un'unica 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. È possibile crearne di più OUs all'interno di una singola organizzazione e creare OUs all'interno di altre OUs. 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.

Il diagramma seguente mostra un'organizzazione composta da sette account organizzati in quattro OUs sotto la radice. L'organizzazione ha anche alcune politiche a cui vengono applicate OUs.



> **Note**
>
> Nell'organizzazione esiste un'unica radice che viene AWS Organizations creata automaticamente quando si configura l'organizzazione per la prima volta.

Argomenti

Procedure ottimali per la gestione delle unità organizzative (OUs) con AWS Organizations

Segui questi consigli per aiutarti a gestire un ambiente con più account AWS Organizations utilizzando le unità organizzative (OUs).

Argomenti

Comprensione AWS Organizations

La base di un AWS ambiente multi-account ben progettato è AWS Organizations che consente di gestire e governare centralmente più account. Un'unità organizzativa (OU) è un raggruppamento logico di account in un'organizzazione. OUs consentono di organizzare gli account in una gerarchia e di applicare i controlli di gestione. Le policy di Organizations definiscono i controlli che è possibile applicare a un gruppo di Account AWS. Ad esempio, una policy di controllo dei servizi (SCP) è una policy che definisce le Servizio AWS azioni, come Amazon EC2 Run Instance, che gli account dell'organizzazione possono eseguire.

Anche se potresti iniziare il tuo AWS percorso con un solo account, ti AWS consiglia di configurare più account man mano che i carichi di lavoro aumentano in termini di dimensioni e complessità. L'utilizzo di un ambiente con più account è una AWS best practice che può offrire diversi vantaggi:

- Innovazione rapida con requisiti diversi: è possibile assegnarli Account AWS a diversi team, progetti o prodotti all'interno dell'azienda per garantire che ciascuno di essi possa innovare rapidamente, rispettando al contempo i propri requisiti di sicurezza.
- Fatturazione semplificata: l'utilizzo di più Account AWS opzioni può semplificare l'allocazione dei AWS costi, aiutando a identificare il prodotto o la linea di servizi responsabile di un addebito. AWS
- Controlli di sicurezza flessibili: puoi utilizzarne più di uno Account AWS per isolare carichi di lavoro o applicazioni che hanno requisiti di sicurezza specifici o che devono soddisfare rigide linee guida per la conformità, come HIPAA o PCI.
- Adattamento ai processi aziendali: è possibile organizzarne più di uno Account AWS in un modo che rifletta al meglio le diverse esigenze dei processi aziendali dell'azienda, che hanno requisiti operativi, normativi e di budget diversi.

Unità organizzativa di base consigliata () OUs

L'unità organizzativa (OUs) dovrebbe basarsi su una funzione o su un insieme comune di controlli anziché rispecchiare la struttura di rendicontazione della società. AWS consiglia di iniziare pensando alla sicurezza e all'infrastruttura. La maggior parte delle aziende dispone di team centralizzati che servono l'intera organizzazione per tali esigenze. Ti consigliamo di creare un set di funzionalità di base OUs per queste funzioni specifiche:

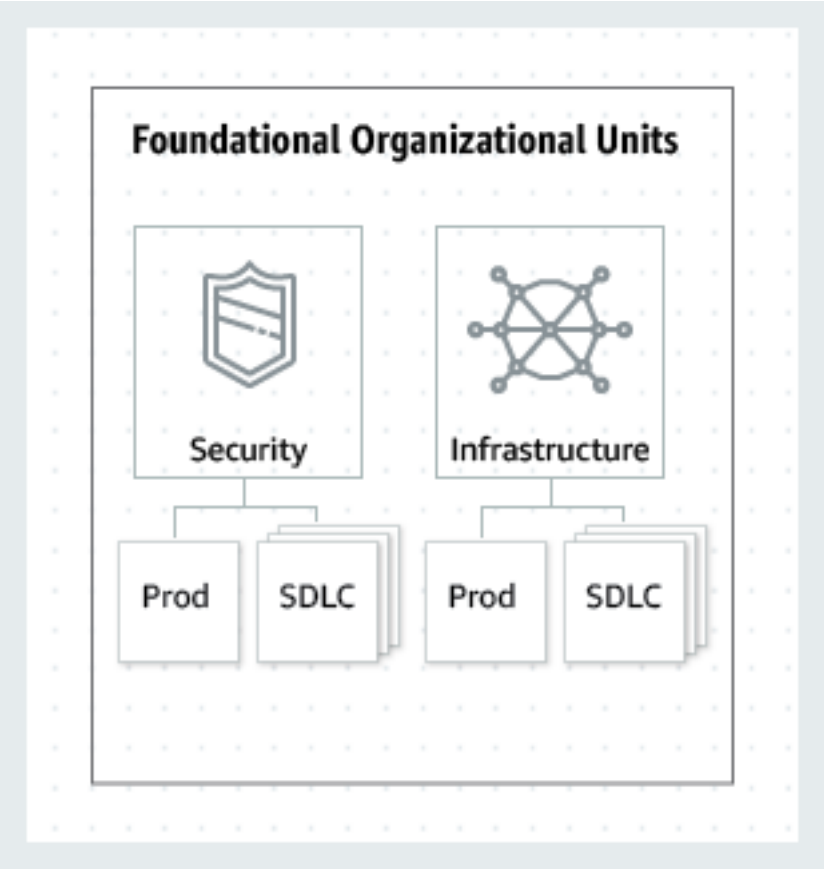
- Sicurezza: utilizzata per i servizi di sicurezza. Crea account per archivi di log, accesso di sicurezza in sola lettura, strumenti di sicurezza e break-glass.

- Infrastruttura: utilizzata per servizi di infrastruttura condivisi come servizi di rete e IT. Crea account per ogni tipo di servizio di infrastruttura richiesto.

Dato che la maggior parte delle aziende ha requisiti politici diversi per i carichi di lavoro di produzione, l'infrastruttura e la sicurezza avrebbero potuto concentrarsi sulla OUs non produzione (SDLC) e sulla produzione (Prod). Gli account dell'unità organizzativa SDLC ospitano carichi di lavoro non di produzione e non devono avere dipendenze di produzione da altri account. In caso di variazioni nelle politiche dell'unità organizzativa tra le fasi del ciclo di vita, SDLC può essere suddiviso in più parti OUs (ad esempio, sviluppo e pre-produzione). Gli account nell'unità organizzativa Prod ospitano i carichi di lavoro di produzione.

Applica le politiche a livello di unità organizzativa per governare l'ambiente Prod e SDLC in base alle tue esigenze. In generale, l'applicazione delle policy a livello di unità organizzativa è una pratica migliore rispetto a quella a livello di singolo account, in quanto semplifica la gestione delle policy e qualsiasi potenziale risoluzione dei problemi.

Il diagramma seguente mostra gli elementi fondamentali OUs (Prod e SDLC) per la sicurezza e l'infrastruttura:



Unità organizzativa aggiuntiva consigliata () OUs

Una volta implementati i servizi centralizzati, ti consigliamo di crearne uno direttamente correlato alla creazione OUs o alla gestione dei tuoi prodotti o servizi. Molti AWS clienti costruiscono quanto segue OUs dopo aver creato una base:

- Sandbox: supporto Account AWS che i singoli sviluppatori possono utilizzare per sperimentare Servizi AWS. Assicurati che questi account possano essere scollegati dalle reti interne.
- Carichi di lavoro: contiene Account AWS che ospitano i servizi applicativi rivolti all'esterno. È necessario strutturarsi OUs in ambienti SDLC e Prod (simili a quelli di base OUs) per isolare e controllare rigorosamente i carichi di lavoro di produzione.

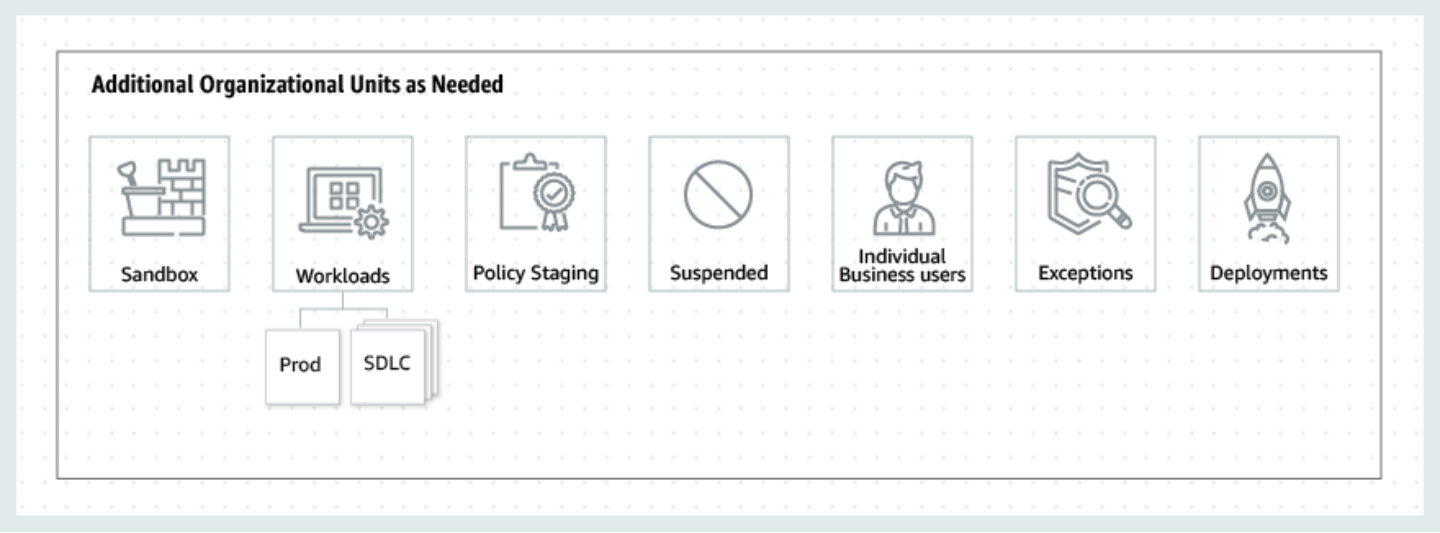
Consigliamo inoltre di aggiungerne altri OUs per la manutenzione e l'espansione continua a seconda delle esigenze specifiche. Di seguito sono riportati alcuni temi comuni basati sulle pratiche dei AWS clienti esistenti:

- Staging delle politiche: conserva AWS account in cui è possibile testare le modifiche alle politiche proposte prima di applicarle a livello generale all'organizzazione. Inizia implementando le modifiche a livello di account nell'unità organizzativa desiderata e applicale lentamente agli altri account e al resto dell'organizzazione. OUs
- Sospesi: contenuti Account AWS che sono stati chiusi e che sono in attesa di essere eliminati dall'organizzazione. Allega un SCP a questa unità organizzativa che nega tutte le azioni. Assicurati che gli account siano etichettati con i dettagli per la tracciabilità se devono essere ripristinati.
- Utenti aziendali individuali: un'unità organizzativa ad accesso limitato destinata Account AWS agli utenti aziendali (non agli sviluppatori) che potrebbero aver bisogno di creare applicazioni relative alla produttività aziendale, ad esempio configurare un bucket S3 per condividere report o file con un partner.
- Eccezioni: Account AWS viene utilizzata per casi d'uso aziendali con requisiti di sicurezza o controllo altamente personalizzati, diversi da quelli definiti nell'unità organizzativa Workloads. Ad esempio, la configurazione di una nuova applicazione o funzionalità Account AWS specifica per una nuova applicazione o funzionalità riservata. SCPs Utilizzalo a livello di account per soddisfare esigenze personalizzate. Prendi in considerazione la possibilità di configurare un sistema Detect and React utilizzando Amazon EventBridge e AWS Config regole.
- Distribuzioni: contiene informazioni Account AWS destinate all'integrazione continua e continua delivery/deployment (CI/CD deployments). You can create this OU if you have a different governance and operational model for CI/CD deployments as compared to accounts in the

Workloads OUs (Prod and SDLC). Distribution of CI/CD helps reduce the organizational dependency on a shared CI/CD environment operated by a central team. For each set of SDLC/Prod Account AWS per un'applicazione nell'unità organizzativa Workloads, crea un account per CI/CD in Deployments OU.

- Transizionale: viene utilizzata come area di archiviazione temporanea per gli account e i carichi di lavoro esistenti prima di spostarli nelle aree standard dell'organizzazione. Ciò potrebbe essere dovuto al fatto che gli account fanno parte di un'acquisizione, precedentemente gestita da una terza parte, o gli account legacy di una vecchia struttura organizzativa.

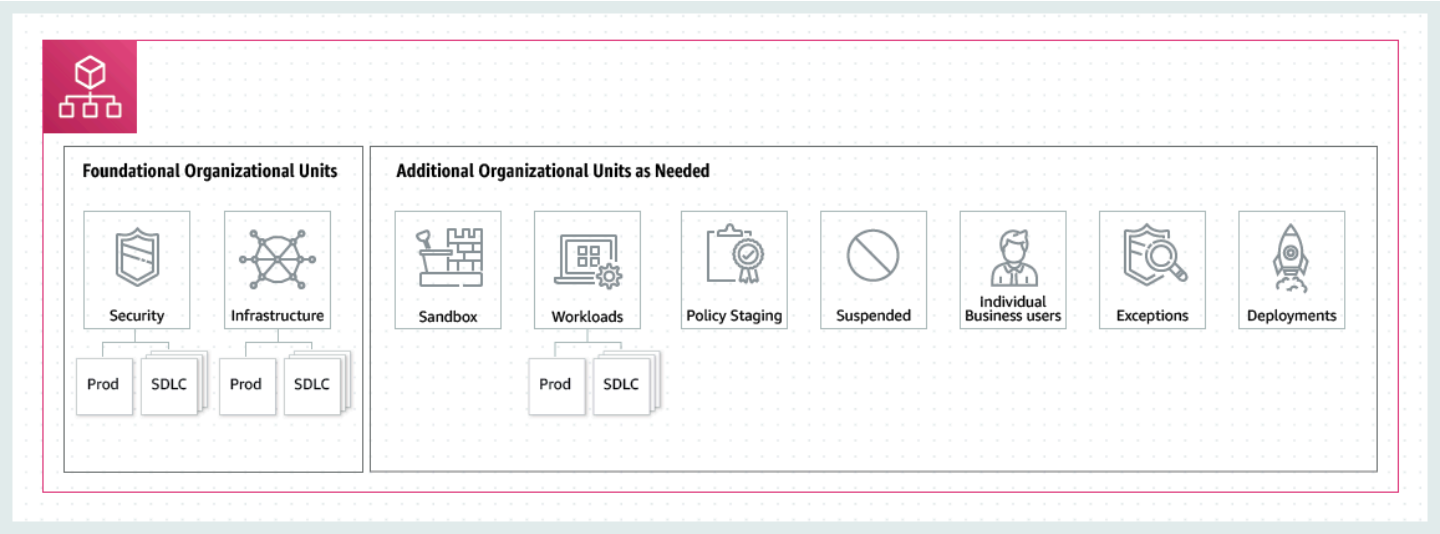
Il diagramma seguente mostra ulteriori informazioni OUs relative a sandbox, carichi di lavoro, gestione temporanea delle policy, utenti aziendali individuali sospesi, eccezioni, implementazioni e account di transizione:



Conclusioni

Una strategia multi-account ben progettata può aiutarti a innovare AWS, garantendo al contempo la soddisfazione delle tue esigenze di sicurezza e scalabilità. Il framework descritto in questo argomento rappresenta le AWS best practice da utilizzare come punto di partenza per il percorso. AWS

Il diagramma seguente mostra le istruzioni di base OUs e quelle aggiuntive consigliate: OUs



Navigazione nella gerarchia delle unità principali e organizzative (OU) con AWS Organizations

Per passare a criteri diversi OUs o alla cartella principale quando si spostano account o si allegano politiche, è possibile utilizzare la visualizzazione «ad albero» predefinita.

AWS Management Console

Per navigare nell'organizzazione come "albero"

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, nella parte superiore della sezione Organization (Organizzazione), seleziona Hierarchy (Gerarchia) (invece che List (Elenco).
3. Inizialmente l'albero appare mostrando la radice, mostrando solo il primo livello di figlio OUs e gli account. 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 OUs o manipolare le politiche ad essi associate.

AWS Management Console

Per visualizzare l'organizzazione come un elenco semplice di account senza gerarchia

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 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.

Visualizzazione dei dettagli di un'unità organizzativa (OU) con AWS Organizations

Quando accedi all'account di gestione dell'organizzazione nella AWS Organizations console, puoi visualizzarne i dettagli OUs 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. 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'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, AWS SDKs:
  - 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"
    }
}
```

- AWS SDKs:
  - ListRoots
  - ListChildren
  - DescribeOrganizationalUnit

Creazione di un'unità organizzativa (OU) con AWS Organizations

Quando si accede all'account di gestione dell'organizzazione, è possibile creare un'unità organizzativa nella directory principale dell'organizzazione. OUs può essere annidato 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 la tua OUs con la AWS Control Tower console o APIs. 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 di AWS 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. 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. 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 in precedenza hai creato OUs e spostato account al loro interno, la console mostra solo

gli account di livello superiore OUs e tutti gli account che non hai ancora spostato in un'unità organizzativa.

3. (Facoltativo) Se si desidera creare un'unità organizzativa all'interno di un'unità organizzativa esistente, accedi all'unità organizzativa secondaria selezionando il nome (non la casella di controllo) dell'unità organizzativa secondaria o selezionando la ▶ successiva OUs nella visualizzazione ad albero finché non viene visualizzata quella desiderata, quindi selezionandone 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

Gli esempi di codice seguenti mostrano come utilizzare `CreateOrganizationalUnit`.

.NET

SDK per .NET

> **Note**
>
> C'è altro da fare GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
```

```
   using System.Threading.Tasks;
   using Amazon.Organizations;
   using Amazon.Organizations.Model;

   /// <summary>
   /// Creates a new organizational unit in AWS Organizations.
   /// </summary>
   public class CreateOrganizationalUnit
   {
       /// <summary>
       /// Initializes an Organizations client object and then uses it to call
       /// the CreateOrganizationalUnit method. If the call succeeds, it
       /// displays information about the new organizational unit.
       /// </summary>
       public static async Task Main()
       {
           // Create the client object using the default account.
           IAmazonOrganizations client = new AmazonOrganizationsClient();

           var orgUnitName = "ProductDevelopmentUnit";

           var request = new CreateOrganizationalUnitRequest
           {
               Name = orgUnitName,
               ParentId = "r-0000",
           };

           var response = await client.CreateOrganizationalUnitAsync(request);

           if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
           {
               Console.WriteLine($"Successfully created organizational unit:
{orgUnitName}.");
               Console.WriteLine($"Organizational unit {orgUnitName} Details");
               Console.WriteLine($"ARN: {response.OrganizationalUnit.Arn} Id:
{response.OrganizationalUnit.Id}");
           }
           else
           {
               Console.WriteLine("Could not create new organizational unit.");
           }
       }
   }
```

- Per i dettagli sull'API, consulta la CreateOrganizationalUnitsezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Per creare un'unità organizzativa in un'unità organizzativa principale o principale

L'esempio seguente mostra come creare un'unità organizzativa denominata AccountingOU:

```
aws organizations create-organizational-unit --parent-id r-examplerootid111 --
name AccountingOU
```

L'output include un oggetto OrganizationalUnit con dettagli sulla nuova unità organizzativa:

```
{
        "OrganizationalUnit": {
                "Id": "ou-examplerootid111-exampleouid111",
                "Arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-
examplerootid111-exampleouid111",
                "Name": "AccountingOU"
        }
}
```

- Per i dettagli sull'API, vedere CreateOrganizationalUnitin AWS CLI Command Reference.

Ridenominazione di un'unità organizzativa (OU) con AWS Organizations

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 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:UpdateOrganizationalUnit`

AWS Management Console

Per rinominare un'unità organizzativa

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, 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 SDKs: UpdateOrganizationalUnit

Etichettare un'unità organizzativa (OU) con AWS Organizations

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 collegati a un'UO che si trova in un root nella tua organizzazione , devi 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. 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, 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 SDKs: TagResource e UntagResource

Spostamento degli account in un'unità organizzativa (OU) o tra la radice e OUs con AWS Organizations

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. L'inserimento di un account all'interno di un'unità organizzativa lo rende soggetto a tutte le politiche associate all'unità organizzativa principale e OUs a tutte le politiche della catena principale fino alla radice. 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. 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 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 gli account in una UO

Per trasferire un account, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: move-account

  L'esempio seguente sposta un Account AWS oggetto dalla radice a un'unità organizzativa. Si noti che è necessario specificare sia il contenitore IDs di origine che quello 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 SDKs: MoveAccount

Visualizzazione dei dettagli della radice con AWS Organizations

Quando si accede all'account di gestione dell'organizzazione nella AWS Organizations console, è possibile visualizzare i dettagli della radice amministrativa.

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

La radice è il contenitore più in alto nella gerarchia delle unità organizzative (OUs) e generalmente si comporta come un'unità organizzativa. Tuttavia, essendo il contenitore in cima alla gerarchia, le modifiche alla radice influiscono su tutte le altre unità organizzative e su tutti i componenti dell'organizzazione. Account AWS

AWS Management Console

Per visualizzare i dettagli del root

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 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"
                }
            ]
        }
    ]
```

```
}
```

- AWS SDKs: ListRoots

Eliminazione di un'unità organizzativa (OU) con AWS Organizations

Quando accedi all'account di gestione della tua organizzazione, puoi eliminare quelli OUs che non ti servono più.

È innanzitutto necessario spostare tutti gli account dall'unità organizzativa e tutti gli account secondari OUs, quindi è possibile eliminare il figlio OUs.

> **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. 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 Account AWSpagina, individua l'unità OUs 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 OUs, inserisci il nome dell'unità organizzativa (se hai scelto di eliminarne solo una) o la parola «elimina» (se ne hai scelte più di una), quindi scegli Elimina.

AWS Organizations li elimina OUs e li rimuove dall'elenco.

AWS CLI & AWS SDKs

Per eliminare un'unità organizzativa

Gli esempi di codice seguenti mostrano come utilizzare `DeleteOrganizationalUnit`.

.NET

SDK per .NET

> **Note**
>
> C'è altro da fare GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing AWS Organizations organizational unit.
/// </summary>
public class DeleteOrganizationalUnit
{
    /// <summary>
    /// Initializes the Organizations client object and calls
    /// DeleteOrganizationalUnitAsync to delete the organizational unit
    /// with the selected ID.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitId = "ou-0000-00000000";

        var request = new DeleteOrganizationalUnitRequest
```

```
            {
                OrganizationalUnitId = orgUnitId,
            };

            var response = await client.DeleteOrganizationalUnitAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted the organizational unit
with ID: {orgUnitId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete the organizational unit with
ID: {orgUnitId}.");
            }
        }
    }
```

- Per i dettagli sull'API, DeleteOrganizationalUnitconsulta AWS SDK per .NET API Reference.

CLI

AWS CLI

Per eliminare un'unità organizzativa

L'esempio seguente mostra come eliminare un'UO. L'esempio presuppone che in precedenza siano stati rimossi tutti gli account e altri account OUs dall'unità organizzativa:

```
aws organizations delete-organizational-unit --organizational-unit-id ou-
examplerootid111-exampleouid111
```

- Per i dettagli sull'API, vedere DeleteOrganizationalUnitin AWS CLI Command Reference.

Gestione delle politiche organizzative con AWS Organizations

Le politiche AWS Organizations consentono di applicare ulteriori tipi di gestione Account AWS all'interno dell'organizzazione. Puoi usare le policy quando tutte le caratteristiche sono abilitate nella tua organizzazione.

La AWS Organizations console mostra lo stato di abilitazione o disabilitazione 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.

Argomenti

Tipi di policy

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

Policy di autorizzazione

Le politiche di autorizzazione consentono di gestire centralmente la sicurezza di Account AWS tutta l'organizzazione.

- Le policy di controllo dei servizi (SCPs) offrono il controllo centralizzato sulle autorizzazioni massime disponibili per gli utenti IAM e i ruoli IAM in un'organizzazione.
- Le politiche di controllo delle risorse (RCPs) offrono il controllo centralizzato sulle autorizzazioni massime disponibili per le risorse in un'organizzazione.

Policy di gestione

Le politiche di gestione consentono di configurare e gestire centralmente Servizi AWS e le relative funzionalità all'interno dell'organizzazione.

- Le politiche dichiarative consentono di dichiarare e applicare a livello centralizzato le configurazioni desiderate per un determinato ambiente su larga scala Servizio AWS all'interno dell'organizzazione. Una volta collegata, la configurazione viene sempre mantenuta quando il servizio aggiunge nuove funzionalità o. APIs
- Le policy di backup consentono di gestire e applicare centralmente i piani di backup alle AWS risorse degli account di un'organizzazione.
- Le politiche relative ai tag consentono di standardizzare i tag allegati alle AWS risorse negli account di un'organizzazione.
- Le politiche delle applicazioni di chat consentono di controllare l'accesso agli account di un'organizzazione da applicazioni di chat come Slack e Microsoft Teams.
- Le politiche di disattivazione dei servizi di intelligenza artificiale consentono di controllare la raccolta dei dati per i servizi di AWS intelligenza artificiale per tutti gli account di un'organizzazione.
- Le policy di Security Hub consentono di colmare le lacune di copertura di sicurezza in linea con i requisiti di sicurezza dell'organizzazione e di applicarle centralmente in tutta l'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 e limiti di servizio per AWS Organizations.

Tipo di policy	Categoria 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	Autorizzazione	 No	5	5.120 caratteri	 No
RCP	Autorizzazione	 No	5	5.120 caratteri	 No
Politica dichiarativa	Gestione	 Sì	10	10,000 caratteri	 Sì
Policy di backup	Gestione	 Sì	10	10,000 caratteri	 Sì
Policy di tag	Gestione	 Sì	10	10,000 caratteri	 Sì

Tipo di policy	Categoria 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
Politica sulle applicazioni di chat	Gestione	 Sì	5	10,000 caratteri	 Sì
Policy di rifiuto dei servizi di IA	Gestione	 Sì	5	2.500 caratteri	 Sì
Politica Security Hub	Gestione	 Sì	10	10,000 caratteri	 Sì

Politiche di autorizzazione in AWS Organizations

Le politiche di autorizzazione AWS Organizations consentono di configurare e gestire centralmente l'accesso ai principali e alle risorse negli account dei membri. Il modo in cui tali politiche influiscono sulle unità organizzative (OUs) e sugli account a cui vengono applicate dipende dal tipo di politica di autorizzazione applicata.

Esistono due diversi tipi di politiche di autorizzazione AWS Organizations: le politiche di controllo dei servizi (SCPs) e le politiche di controllo delle risorse (RCPs).

Argomenti

- Differenze tra SCPs e RCPs
- Usando e SCPs RCPs

- Politiche di controllo del servizio (SCPs)
- Politiche di controllo delle risorse (RCPs)

Differenze tra SCPs e RCPs

SCPs sono controlli incentrati sui principali. SCPs crea una barriera di autorizzazioni, o imposta dei limiti, alle autorizzazioni massime disponibili per i responsabili nei tuoi account membro. È possibile utilizzare un SCP quando si desidera applicare centralmente controlli di accesso coerenti ai dirigenti della propria organizzazione. Ciò può includere la specificazione a quali servizi possono accedere gli utenti IAM e i ruoli IAM, a quali risorse possono accedere o le condizioni in base alle quali possono effettuare richieste (ad esempio, da regioni o reti specifiche).

RCPs sono controlli incentrati sulle risorse. RCPs crea una barriera di autorizzazioni, o imposta dei limiti, alle autorizzazioni massime disponibili per le risorse nei tuoi account membro. È possibile utilizzare un RCP quando si desidera applicare centralmente controlli di accesso coerenti tra le risorse dell'organizzazione. Ciò può limitare l'accesso alle risorse in modo che possano accedervi solo le identità che appartengono all'organizzazione o specificare le condizioni in base alle quali le identità esterne all'organizzazione possono accedere alle risorse.

Alcuni controlli possono essere applicati in modo simile tramite e. SCPs RCPs Ad esempio, potresti voler impedire ai tuoi utenti di caricare oggetti non crittografati su S3, che possono essere scritti come SCP, per imporre un controllo sulle azioni che i tuoi principali possono intraprendere sui tuoi bucket S3. Questo controllo può anche essere scritto come RCP per richiedere la crittografia ogni volta che un principale carica oggetti nel bucket S3. La seconda opzione potrebbe essere preferita se il bucket consente a responsabili esterni all'organizzazione, come fornitori di terze parti, di caricare oggetti nel bucket S3. Tuttavia, alcuni controlli possono essere implementati solo in un RCP e alcuni controlli possono essere implementati solo in un SCP. Per ulteriori informazioni, consulta Casi d'uso generali per e SCPs RCPs.

Usando e SCPs RCPs

SCPs e RCPs sono controlli indipendenti. È possibile scegliere di abilitare solo SCPs o RCPs utilizzare entrambi i tipi di policy insieme. Utilizzando entrambi SCPs e RCPs, puoi creare un perimetro di dati attorno alle tue identità e alle tue risorse.

SCPs offrono la possibilità di controllare a quali risorse possono accedere le identità dell'utente. Ad esempio, potresti voler consentire alle tue identità di accedere alle risorse della tua AWS

organizzazione. Tuttavia, potresti voler impedire alle tue identità di accedere a risorse esterne all'organizzazione. È possibile imporre questo controllo utilizzando. SCPs

RCPs offri la possibilità di controllare quali identità possono accedere alle tue risorse. Ad esempio, potresti voler consentire alle identità della tua organizzazione di accedere alle risorse dell'organizzazione. Tuttavia, potresti voler impedire a identità esterne all'organizzazione di accedere alle tue risorse. È possibile imporre questo controllo utilizzando. RCPs RCPs offrono la possibilità di influire sulle autorizzazioni effettive per i responsabili esterni all'organizzazione che accedono alle risorse dell'utente. SCPs può influire solo sulle autorizzazioni effettive per i dirigenti all'interno dell'organizzazione. AWS

Casi d'uso generali per e SCPs RCPs

La tabella seguente descrive i casi d'uso generali per l'utilizzo di un SCP e RCPs

		Impatti			
Caso d'uso	Tipo di politica	Le tue identità	Identità esterne	Le tue risorse	Risorse esterne (obiettivo della richiesta)
Limita i servizi o le azioni che le tue identità possono utilizzare	SCP	X		X	X
Limita le risorse a cui le tue identità possono accedere	SCP	X		X	X
Applica i requisiti relativi al	SCP	X		X	X

		Impatti		
modo in cui le tue identità possono accedere alle risorse				
Limita le identità che possono accedere alle tue risorse	RCP	X	X	X
Proteggi le risorse sensibili della tua organizzazione	RCP	X	X	X
Applica i requisiti relativi alle modalità di accesso alle risorse	RCP	X	X	X

Politiche di controllo del servizio (SCPs)

Le policy di controllo dei servizi (SCPs) sono un tipo di policy organizzativa che puoi utilizzare per gestire le autorizzazioni all'interno della tua organizzazione. SCPs offrono il controllo centralizzato sulle autorizzazioni massime disponibili per gli utenti IAM e i ruoli IAM nell'organizzazione. SCPs ti aiutano a garantire che i tuoi account rispettino le linee guida per il controllo degli accessi della tua organizzazione. SCPssono disponibili solo in un'organizzazione che ha tutte le funzionalità abilitate. SCPs non sono disponibili se l'organizzazione ha abilitato solo le funzionalità di fatturazione consolidata. Per istruzioni sull'attivazione SCPs, consulta. Abilitazione di un tipo di policy

SCPs non concedete autorizzazioni agli utenti e ai ruoli IAM della vostra 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 all'interno 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. Per ulteriori informazioni, consulta Politiche basate sull'identità e politiche basate sulle risorse nella Guida per l'utente IAM.

Le autorizzazioni effettive sono l'intersezione logica tra ciò che è consentito da SCP e dalle politiche di controllo delle risorse (RCPs) e ciò che è consentito dalle politiche basate sull'identità e sulle risorse.

> ⚠ SCPs non influiscono sugli utenti o sui ruoli nell'account di gestione
>
> SCPs non influiscono sugli utenti o sui ruoli nell'account di gestione. Influiscono solo sugli account membri nell'organizzazione. Ciò significa che SCPs si applicano anche agli account dei membri designati come amministratori delegati.

Argomenti in questa pagina

Effetti dei test di SCPs

AWS ti consiglia vivamente di non dedicarti SCPs alla radice della tua 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 di SCPs

Tutti i caratteri nella SCP sono conteggiati rispetto alla dimensione massima. Gli esempi di questa guida mostrano la SCPs formattazione con spazio bianco 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 SCPs a diversi livelli dell'organizzazione

Per una spiegazione dettagliata del SCPs funzionamento, vedereValutazione SCP.

Effetti di SCP sulle autorizzazioni

SCPs sono simili alle politiche di AWS Identity and Access Management autorizzazione e utilizzano quasi la stessa sintassi. ma non concedono mai le autorizzazioni. SCPs Sono invece controlli di accesso che specificano le autorizzazioni massime disponibili 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.

- SCPs riguardano solo gli utenti e i ruoli IAM gestiti da account che fanno parte dell'organizzazione. SCPs non influiscono direttamente sulle politiche basate sulle 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.
- SCPs riguardano solo gli account dei membri dell'organizzazione. Non hanno alcun effetto sugli utenti o sui ruoli nell'account di gestione. Ciò significa che SCPs si applicano anche agli account dei membri designati come amministratori delegati. Per ulteriori informazioni, consulta Best practice per l'account di gestione.
- Agli utenti e ai ruoli devono ancora essere concesse le autorizzazioni con policy di autorizzazione IAM appropriate. Un utente senza alcuna policy di autorizzazione IAM non ha accesso, anche se la normativa applicabile SCPs consente tutti i servizi e tutte le azioni.
- Se un utente o un ruolo dispone di una politica di autorizzazione IAM che concede l'accesso a un'azione consentita anche dal pertinente SCPs, l'utente o il ruolo può eseguire tale azione.
- Se un utente o un ruolo dispone di una politica di autorizzazione IAM che concede l'accesso a un'azione non consentita o esplicitamente negata dall'applicabile SCPs, l'utente o il ruolo non può eseguire tale azione.
- SCPs 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 da SCPs.
- SCPs non influiscono su alcun ruolo collegato al servizio. I ruoli collegati ai servizi consentono l'integrazione con altri Servizi AWS AWS Organizations e non possono essere limitati da. SCPs
- Quando si disabilita il tipo di policy SCP in una radice, tutte SCPs vengono automaticamente scollegate da tutte le AWS Organizations entità in quella radice. AWS Organizations le entità includono unità organizzative, organizzazioni e account. Se si riattiva SCPs in una radice, tale radice ritorna solo alla `FullAWSAccess` politica predefinita allegata automaticamente a tutte le entità nella radice. Tutti gli allegati SCPs alle AWS Organizations entità precedentemente

SCPs disattivate vengono persi e non sono recuperabili automaticamente, sebbene sia possibile ricollegarli 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 SCPs

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. Puoi utilizzare queste informazioni per identificare le autorizzazioni non utilizzate in modo da perfezionarle per aderire meglio SCPs al principio del privilegio minimo.

Ad esempio, potresti avere una lista di rifiuto SCP che vieta l'accesso a tre di essi. Servizi AWS Sono consentiti tutti i servizi non elencati nella dichiarazione `Deny` della SCP. L'ultimo accesso ai dati del servizio in IAM indica quali dati Servizi AWS 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 da SCPs

Non è possibile utilizzare SCPs 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
- Fornisci funzionalità di firma affidabile per i contenuti CloudFront privati
- Configura il DNS inverso per un server di posta elettronica Amazon Lightsail e un'istanza EC2 Amazon come utente root

- Attività su alcuni servizi correlati AWS:
  - Alexa Top Sites
  - Alexa Web Information Service
  - Amazon Mechanical Turk
  - Amazon Product Marketing API

Valutazione SCP

> **Note**
>
> Le informazioni contenute in questa sezione non si applicano ai tipi di policy di gestione, incluse le policy di backup, le policy di tag, le policy delle applicazioni di chat o le politiche di opt-out dei servizi AI. Per ulteriori informazioni, consulta Comprendere l'ereditarietà delle policy di gestione.

Poiché è possibile allegare più politiche di controllo del servizio (SCPs) a diversi livelli in AWS Organizations, comprendere come SCPs vengono valutate può aiutarti a scrivere SCPs il risultato giusto.

Argomenti

- Come SCPs lavorare con Allow
- Come SCPs lavorare con Deny
- Strategia di utilizzo SCPs

Come SCPs lavorare con 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 abiliti SCPs, AWS Organizations allega una policy SCP AWS gestita denominata Full AWSAccess che consente tutti i servizi e le azioni. Se questa politica viene rimossa e non sostituita a nessun livello dell'organizzazione, a tutti gli account OUs e a tutti gli account al di sotto di quel livello verrebbe impedito di 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 deny-by-default modello, il che significa che tutte le autorizzazioni non esplicitamente consentite in vengono negate SCPs . Se un'istruzione allow non è presente in SCPs a nessuno dei livelli come Root, Production OU 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`.

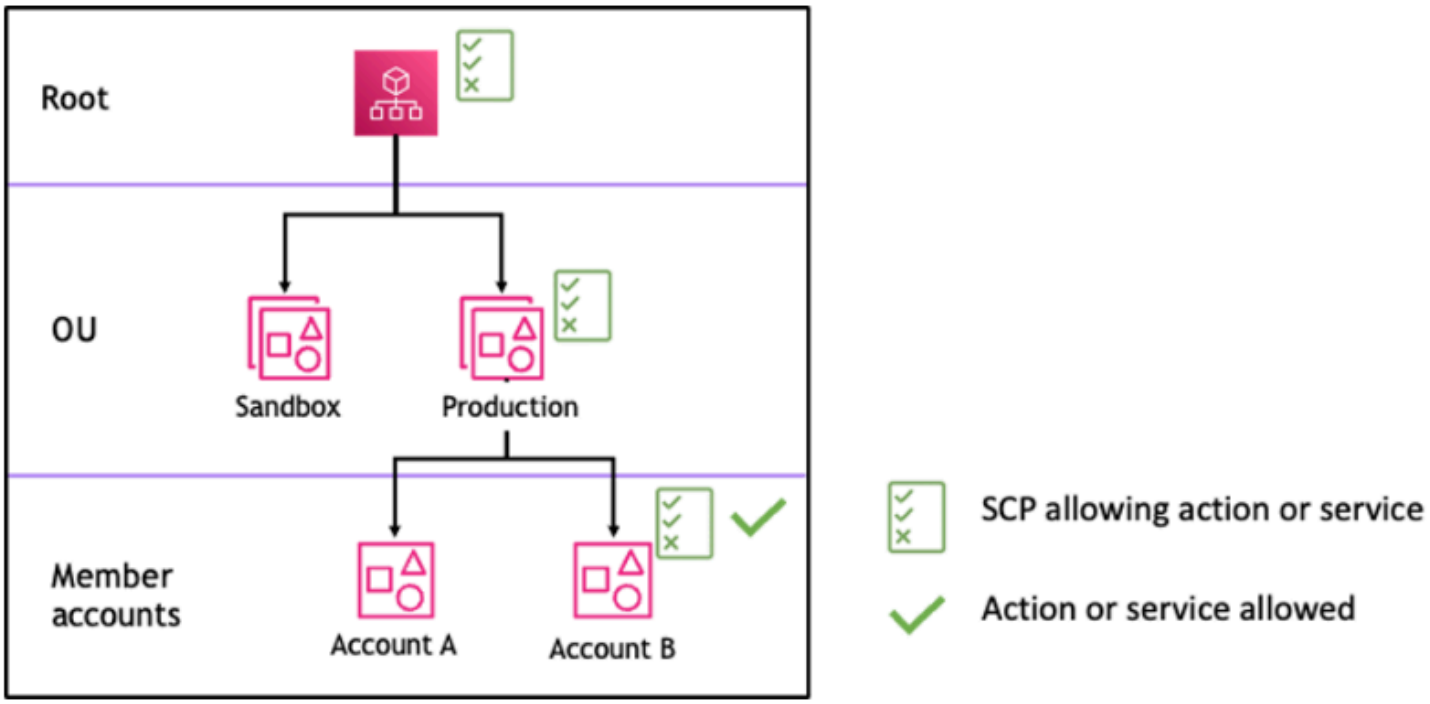


Figura 1: Esempio di struttura organizzativa con una istruzione *`Allow`* collegata alla radice, all'unità organizzativa di produzione e all'account B

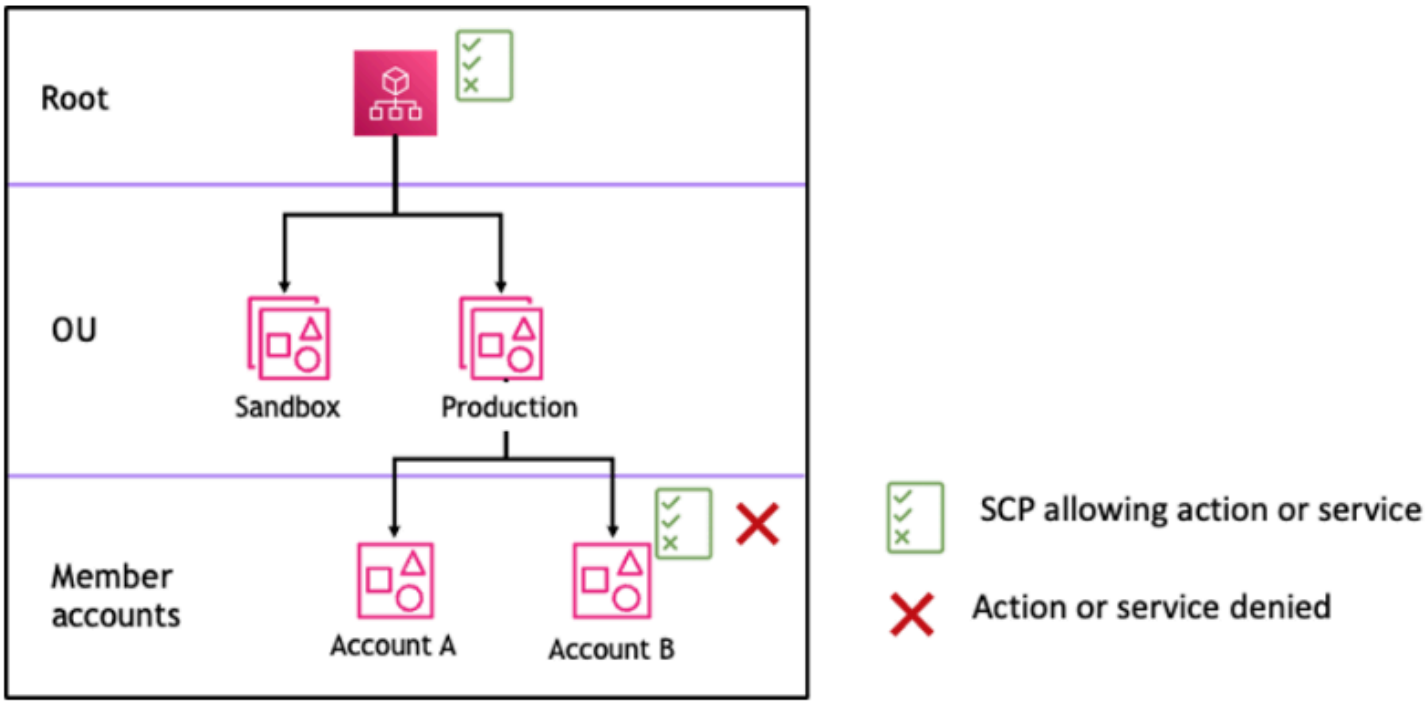


Figura 2: Esempio di struttura organizzativa con una istruzione *`Allow`* mancante sull'unità organizzativa di produzione e relativo impatto sull'account B

Come SCPs lavorare con 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 politica di negazione applicata a qualsiasi livello dell'organizzazione viene valutata per tutti gli account OUs e i membri sottostanti.

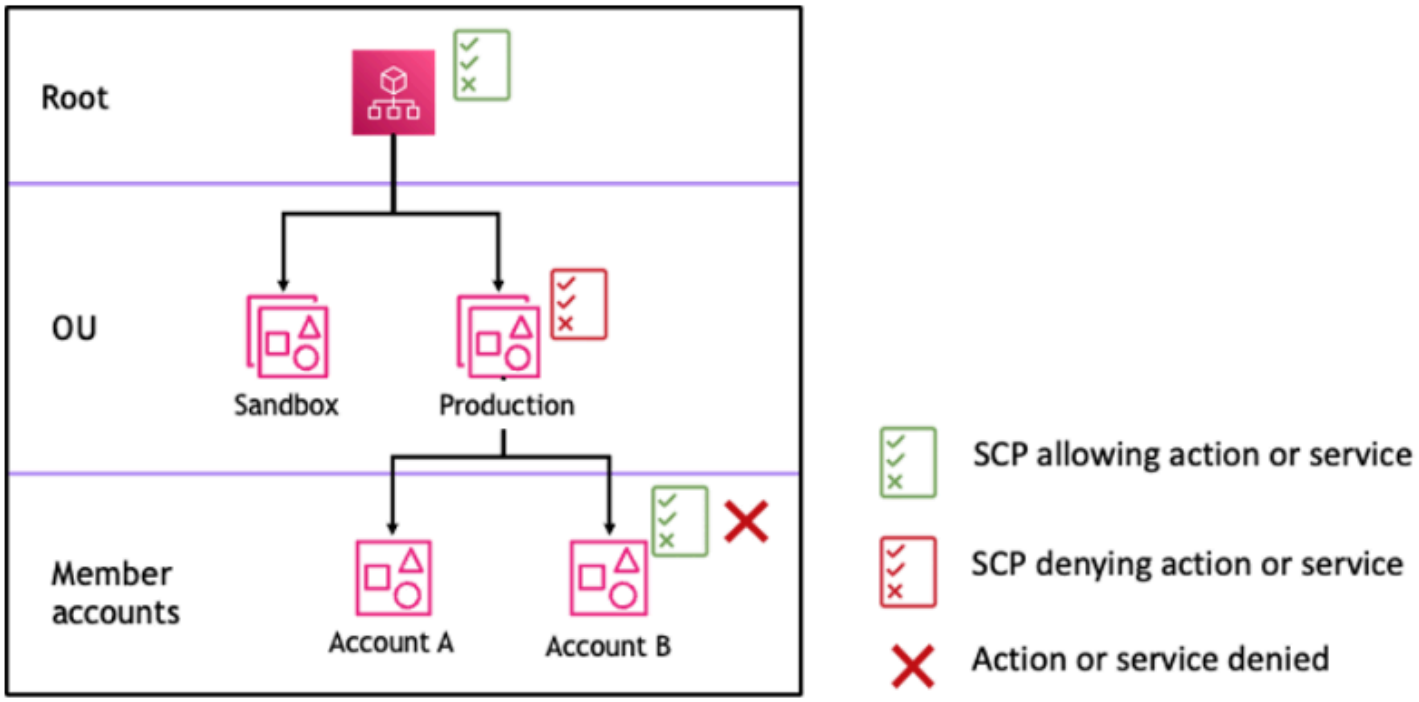


Figura 3: Esempio di struttura organizzativa con una istruzione *Deny* collegata all'unità organizzativa di produzione e relativo impatto sull'account B

Strategia di utilizzo SCPs

Durante la stesura, SCPs è possibile utilizzare una combinazione di `Allow` `Deny` dichiarazioni per consentire le azioni e i servizi previsti all'interno dell'organizzazione. `Deny`le dichiarazioni sono un modo efficace per implementare restrizioni che dovrebbero valere per una parte più ampia dell'organizzazione o OUs perché, 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 politica utilizzando `Deny` le istruzioni L'account di gestione può anche impedire agli account membri di lasciare l'organizzazione. a livello principale, 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**
>
> Puoi utilizzare i dati dell'ultimo accesso al servizio in IAM per aggiornare i tuoi dati e SCPs limitare l'accesso solo a quelli di Servizi AWS cui hai bisogno. Per ulteriori informazioni, consulta Visualizzazione degli ultimi dati di accesso al servizio per Organizations nella Guida per l'utente di IAM.

AWS Organizations Allega un SCP AWS gestito denominato Full AWSAccess a ogni root, unità organizzativa e account al momento della creazione. Questa policy consente tutte le operazioni e i servizi. È possibile sostituire Full AWSAccess con una politica che consenta solo un insieme di servizi, in modo che i nuovi servizi non Servizi AWS siano consentiti a meno che non siano esplicitamente consentiti mediante l'aggiornamento. SCPs 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.

JSON

```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        }
    ]
}
```

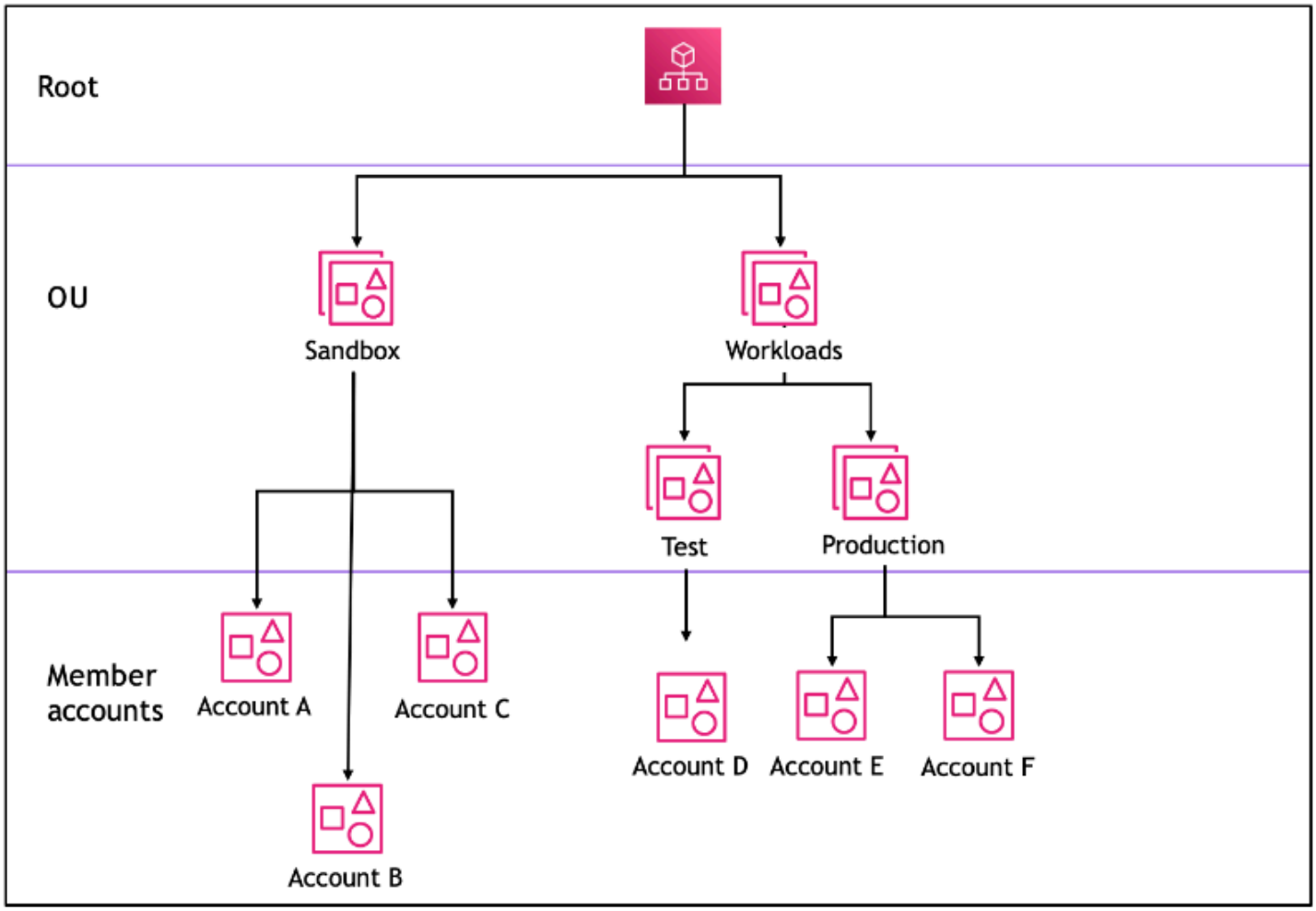
Questa policy, che combina le due istruzioni potrebbe essere simile al seguente esempio, impedisce agli account membri di lasciare l'organizzazione e consente l'uso dei servizi AWS desiderati. L'amministratore dell'organizzazione può scollegare la AWSAccess politica Full e allegare invece questa.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
```

```
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action":"organizations:LeaveOrganization",
            "Resource": "*"
        }
    ]
}
```

Prendiamo ora in considerazione il seguente esempio di struttura organizzativa per capire come applicarne di più SCPs 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 sperimentazione (sandbox)	SCP a livello di account A	Policy risultante sull'account A	Policy risultante sull'account B e sull'account C
1	AWS Accesso completo	AWS Accesso completo + nega l'accesso a S3	AWS Accesso completo + negazione dell'accesso EC2	Nessun S3, nessun accesso EC2	Nessun accesso a S3
2	Accesso completo AWS	Consenti EC2 l'accesso	Consenti EC2 l'accesso	Consenti EC2 l'accesso	Consenti EC2 l'accesso
3	Nega l'accesso a S3	Consenti l'accesso a S3	AWS Accesso completo	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	AWS Accesso completo	AWS Accesso completo	AWS Accesso completo + negazione EC2 dell'accesso	Nessun accesso EC2	AWS Accesso completo
2	AWS Accesso completo	AWS Accesso completo	Consenti EC2 l'accesso	Consenti EC2 l'accesso	AWS Accesso completo
3	Nega l'accesso a S3	AWS Accesso completo	Consenti l'accesso a S3	Nessun accesso al servizio	Nessun accesso a S3

Sintassi delle SCP

Le politiche di controllo dei servizi (SCPs) utilizzano una sintassi simile a quella utilizzata dalle politiche di autorizzazione AWS Identity and Access Management (IAM) e dalle politiche basate sulle risorse (come le policy dei bucket 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 di questa guida mostrano la SCPs formattazione con spazi bianchi aggiuntivi 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 su SCPs, vedere. Politiche di controllo del servizio (SCPs)

Riepilogo degli elementi

La tabella seguente riassume gli elementi della politica che è possibile utilizzare in SCPs. Alcuni elementi della policy sono disponibili solo nella versione SCPs che nega le azioni. La colonna Effetti supportati elenca il tipo di effetto che è possibile utilizzare con ogni elemento della policy in SCPs.

Elemento	Scopo	Effetti supportati
Azione	Specifica AWS il servizio e le azioni consentite o negate da SCP.	`Allow`, `Deny`
Effetto	Definisce se l'istruzione SCP consente o nega l'accesso agli utenti e ai ruoli IAM in un account.	`Allow`, `Deny`
Statement	Serve da container per gli elementi	`Allow`, `Deny`

Elemento	Scopo	Effetti supportati
	di policy. È possibile inserire più istruzioni in. SCPs	
Statement ID (Sid)	(Facoltativo) Fornisce un nome semplice per l'istruzione.	`Allow`, `Deny`
Versione	Specifica le regole di sintassi del linguaggio da utilizzare per elaborare la policy.	`Allow`, `Deny`

Elemento	Scopo	Effetti supportati
Condition	Specifica le condizioni che stabiliscono quando l'istruzione è attiva.	`Deny`
NotAction	Speciifica il AWS servizio e le azioni che sono esenti dall'SCP. Utilizzato invece dell'elemento `Action`.	`Deny`
Risorsa	Speciifica le AWS risorse a cui si applica l'SCP.	`Deny`

Le sezioni seguenti forniscono ulteriori informazioni ed esempi di come vengono utilizzati gli elementi delle politiche. SCPs

Argomenti

- Elementi Action e NotAction
- Elemento Condition
- Elemento Effect
- Elemento Resource
- Elemento Statement
- Elemento Statement ID (Sid)
- Elemento Version
- Elementi non supportati

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 AWS i 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 azioni e le notazioni non fanno distinzione tra maiuscole e minuscole. In genere, vengono tutte inserite con ogni parola che inizia con una lettera maiuscola e il resto con una lettera minuscola. 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 EC2 azioni che iniziano con «Descrivi».
- 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 valido, ma `"servicename:*action"` non `"servicename:some*action"` sono entrambi validi in SCPs.

Per un elenco di tutti i servizi e delle azioni che supportano in entrambi AWS Organizations SCPs e 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 un SCP con un'istruzione che consente agli amministratori dell'account di delegare, descrivere, avviare, interrompere e terminare le autorizzazioni per le istanze dell'account. EC2 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:

JSON

```
{
    "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. Si presuppone che le impostazioni predefinite `"Allow *"` SCPs siano ancora associate a all e alla root. OUs 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.

JSON

```
{
    "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.

JSON

```
{
  "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 **`Condition`**

È possibile specificare un elemento `Condition` nelle istruzioni di rifiuto in una SCP.

JSON

```
{
    "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.

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. Funzionano invece SCPs come filtri che specificano le autorizzazioni massime per gli account di un'organizzazione, di un'unità organizzativa (OU) o di un account. 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'`Effect`elemento ha un valore di`Deny`, è inoltre possibile limitare l'accesso a risorse specifiche o definire le condizioni relative all'entrata SCPs in vigore.

Quanto segue mostra un esempio di come utilizzare una condizione di chiave in un'istruzione di rifiuto.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "ec2:RunInstances",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:InstanceType": "t2.micro"
            }
        }
    }
}
```

Questa dichiarazione in un SCP stabilisce una barriera per impedire agli account interessati (in cui l'SCP è collegato all'account stesso o alla radice dell'organizzazione o all'unità organizzativa che contiene l'account) di avviare EC2 istanze Amazon se l'istanza EC2 Amazon 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.

Elemento **`Resource`**

In istruzioni in cui l'elemento `Effect` ha un valore `Allow`, è possibile specificare solo "*" nell'elemento `Resource` di una SCP. Non puoi specificare una singola risorsa Amazon Resource Names (ARNs).

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.

Nelle istruzioni in cui l'`Effect`elemento ha un valore di`Deny`, puoi specificare individual ARNs, come mostrato nell'esempio seguente.

JSON

```
{
  "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 **`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 azioni, mentre la seconda nega qualsiasi EC2 azione. Il risultato è che un amministratore dell'account può delegare qualsiasi autorizzazione ad eccezione di quelle di 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 **`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.

Elementi non supportati

I seguenti elementi non sono supportati in: SCPs

- `Principal`
- `NotPrincipal`
- `NotResource`

Esempi di policy di controllo dei servizi

Gli esempi di policy di controllo dei servizi (SCPs) visualizzati in questo argomento sono solo a scopo informativo.

> **Prima di utilizzare questi esempi**
>
> Prima di utilizzare questi esempi SCPs nella propria organizzazione, effettuate le seguenti operazioni:
>
> - Esamina e personalizzali attentamente in base alle tue esigenze specifiche. SCPs
> - Testateli accuratamente SCPs nel vostro ambiente con Servizi AWS quello che utilizzate.
>
> Le politiche di esempio in questa sezione dimostrano l'implementazione e l'uso di SCPs. 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 politiche di controllo del servizio basate sulla negazione possono limitare

o bloccare involontariamente l'utilizzo di, Servizi AWS a meno che non si aggiungano le eccezioni necessarie alla politica. Per un esempio di tale eccezione, si veda il primo esempio che esenta i servizi globali dalle regole che bloccano l'accesso agli utenti indesiderati. Regioni AWS

- Ricorda che una SCP influisce su ogni utente e ruolo, incluso l'utente root, in ogni account a cui è collegata.
- Ricordate che un SCP non influisce sui ruoli collegati ai servizi. I ruoli collegati ai servizi consentono l'integrazione con altri AWS Organizations e Servizi AWS non possono essere limitati. SCPs

Tip

Puoi utilizzare i dati dell'ultimo accesso al servizio in IAM per aggiornare i tuoi dati e SCPs limitare l'accesso solo a quelli di Servizi AWS cui hai bisogno. 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 associata per impostazione predefinita alla radice, a tutte le unità organizzative (OUs) e a tutti gli account. In realtà non concede alcuna autorizzazione (nessuna SCP lo fa). Consente invece agli amministratori di quell'account di delegare l'accesso a tali azioni allegando politiche di autorizzazione standard AWS Identity and Access Management (IAM) a utenti, ruoli o gruppi dell'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
  - Negare l'accesso a AWS in base alla richiesta Regione AWS
  - Impedire agli utenti e ai ruoli IAM di apportare alcune modifiche
  - Impedire agli utenti e ai ruoli IAM di apportare modifiche specifiche, con un'eccezione per un ruolo di amministratore specificato
  - Richiedi MFA per eseguire un'operazione API

- Impedire a qualsiasi VPC che non dispone già dell'accesso a Internet di ottenerlo

Esempi generali

Negare l'accesso a AWS in base alla richiesta Regione AWS

Questa SCP nega l'accesso a qualsiasi operazione al di fuori delle Regioni specificate. Sostituisci `eu-central-1` e `eu-west-1` con Regioni AWS quello 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 Region deny SCP con AWS Control Tower, consultate Negare l'accesso a in AWS base a quanto richiesto Regione AWS nella AWS Control Tower Controls Reference Guide.

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'NotActionelemento consente di elencare i servizi le cui operazioni (o singole operazioni) sono esenti 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 tutte le operazioni Servizi AWS o le operazioni 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 devi includerli nell'elenco di esclusione dei servizi globale nell'esempio SCP seguente. Un servizio globale come Amazon richiede CloudFront in genere l'accesso a AWS KMS un 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 globale di esclusione dei servizi. Tuttavia, puoi AWS STS abilitare l'utilizzo degli endpoint regionali anziché 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 Managing AWS STS in an. 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": {
        "ArnNotLike": {
          "aws:PrincipalARN":"arn:aws:iam::*:role/name-of-admin-role-to-allow"
        }
      }
    }
  ]
}
```

Richiedi 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'azione consiste nel fermare un' EC2 istanza Amazon.

```
{
  "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": "*"
        }
    ]
}
```

Esempio SCPs per Amazon Q Developer nelle applicazioni di chat

Esempi in questa categoria

- Nega tutte le operazioni IAM
- Nega le richieste put del bucket S3 da un canale Slack specificato

Nega tutte le operazioni IAM

Il seguente SCP nega tutte le operazioni IAM richiamate tramite tutte le configurazioni di applicazioni di chat di Amazon Q Developer.

```
{
    "Effect": "Deny",
    "Action": "iam:*",
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:ChatbotSourceArn": "arn:aws:chatbot::*:*"
        }
    }
}
```

Nega le richieste put del bucket S3 da un canale Slack specificato

La seguente politica nega le richieste di put di S3 sul bucket specificato per tutte le richieste provenienti da un canale Slack.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ExampleS3Deny",
            "Effect": "Deny",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringLike": {
                      "aws:ChatbotSourceArn": "arn:aws:chatbot::*:chat-
configuration/slack-channel/*"
                }
            }
        }
    ]
}
```

Esempio SCPs per Amazon CloudWatch

Esempi in questa categoria

- Impedisci agli utenti di disabilitarne CloudWatch o modificarne la configurazione

Impedisci agli utenti di disabilitarne CloudWatch o modificarne la configurazione

Un CloudWatch operatore di livello inferiore deve monitorare dashboard e allarmi. Tuttavia, l'operatore non deve essere in grado di eliminare o modificare alcun pannello di controllo o allarme attuati da personale senior. Questo SCP impedisce agli utenti o ai ruoli di qualsiasi account interessato di eseguire CloudWatch i comandi che potrebbero eliminare o modificare i dashboard o gli allarmi.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DeleteDashboards",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:PutDashboard",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:SetAlarmState"
      ],
      "Resource": "*"
    }
  ]
}
```

Esempio SCPs per AWS Config

Esempi in questa categoria

- Impedire agli utenti di disabilitarne AWS Config o modificarne le regole

Impedire agli utenti di disabilitarne AWS Config o modificarne le regole

Questo SCP impedisce agli utenti o ai ruoli di qualsiasi account interessato di eseguire AWS Config operazioni che potrebbero disabilitarne AWS Config o modificarne le regole o i trigger.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "config:DeleteConfigRule",
        "config:DeleteConfigurationRecorder",
        "config:DeleteDeliveryChannel",
        "config:StopConfigurationRecorder"
      ],
      "Resource": "*"
    }
  ]
}
```

Esempio SCPs per Amazon Elastic Compute Cloud (Amazon EC2)

Esempi in questa categoria

- Richiedi alle EC2 istanze Amazon di utilizzare un tipo specifico
- Impedisci l'avvio EC2 di istanze senza IMDSv2
- Impedire la disabilitazione della crittografia Amazon EBS predefinita
- Impedisci la creazione e il collegamento di volumi non gp3

Richiedi alle EC2 istanze Amazon di utilizzare 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"
        }
      }
    }
  ]
}
```

Impedisci l'avvio EC2 di istanze senza IMDSv2

La seguente politica impedisce a tutti gli utenti di avviare EC2 istanze 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":"2"
         }
      }
   },
   {
      "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 EC2 istanze senza farlo, 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": "2"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*",
    "Condition": {
      "ArnNotLike": {
        "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": "*"
}
```

Impedisci la creazione e il collegamento di volumi non gp3

La seguente policy impedisce a tutti gli utenti di creare o allegare volumi Amazon EBS che non siano del tipo di volume gp3. Per ulteriori informazioni, consulta i tipi di volume di Amazon EBS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreationAndAttachmentOfNonGP3Volumes",
      "Effect": "Deny",
      "Action": [
        "ec2:AttachVolume",
        "ec2:CreateVolume",
        "ec2:RunInstances"
      ],
      "Resource": "arn:aws:ec2:*:*:volume/*",
      "Condition": {
        "StringNotEquals": {
          "ec2:VolumeType": "gp3"
        }
      }
    }
  ]
}
```

Questo può aiutare a imporre una configurazione di volume standardizzata all'interno di un'organizzazione.

> **Le modifiche al tipo di volume non vengono impedite**
>
> Non è possibile limitare l'azione di modifica di un volume gp3 esistente a un volume Amazon EBS di un altro tipo utilizzando. SCPs Ad esempio, questo SCP non ti impedirebbe di modificare un volume gp3 esistente in un volume gp2. Questo perché la chiave condition `ec2:VolumeType` controlla il tipo di volume prima che venga modificato.

Esempio SCPs per Amazon GuardDuty

Esempi in questa categoria

- Impedisci agli utenti di disabilitarne GuardDuty o modificarne la configurazione

Impedisci agli utenti di disabilitarne GuardDuty o modificarne la configurazione

Questo SCP impedisce agli utenti o ai ruoli di qualsiasi account interessato di disabilitarne GuardDuty o alterarne la configurazione, direttamente come comando o 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": "*"
        }
    ]
}
```

Esempio SCPs 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 (OUs)
- 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 (OUs)

Il seguente SCP impedisce agli utenti di creare condivisioni di risorse che condividono risorse con un'organizzazione o OUs.

```
{
    "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:StringEquals": {
                    "ram:Principal": [
                        "arn:aws:organizations::123456789012:organization/
o-12345abcdef",
                        "arn:aws:organizations::123456789012:ou/o-12345abcdef/
ou-98765fedcba",
                        "111111111111"
                    ]
```

```
                }
            }
        }
    ]
}
```

Esempio SCPs di Amazon Application Recovery Controller (ARC)

Esempi in questa categoria

- Impedisci agli utenti di aggiornare gli stati di controllo del routing ARC

Impedisci agli utenti di aggiornare gli stati di controllo del routing ARC

Un operatore ARC di livello inferiore deve monitorare i dashboard e visualizzare le informazioni ARC. Tuttavia, l'operatore non deve essere in grado di aggiornare i controlli di routing per eseguire il failover dell'applicazione da uno Regione AWS all'altro, come potrebbe essere consentito a un operatore senior. Questo SCP impedisce agli utenti o ai ruoli di qualsiasi account interessato di eseguire operazioni ARC che aggiornano i controlli di routing 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"
                    ]
                }
            }
        }
    ]
}
```

Esempio SCPs per Amazon S3

> **Note**
>
> Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) applica automaticamente la crittografia lato server (SSE-S3) per ogni nuovo oggetto, a meno che non venga specificata un'opzione di crittografia diversa. Per ulteriori informazioni, consulta Amazon S3 ora crittografa automaticamente tutti i nuovi oggetti nella Amazon S3 User Guide.

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 politica 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 degli oggetti nei loro 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"
      }
    }
  }
]
```

Esempio SCPs di etichettatura delle 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 di creazione di segreti senza tag o di esecuzione di istanze EC2 Amazon senza tag e non include alcuna eccezione.
> La seguente politica di esempio non è compatibile con AWS CloudFormation quella scritta, perché quel servizio crea un segreto e poi lo contrassegna in due passaggi separati.
> Questa policy di esempio AWS CloudFormation impedisce efficacemente la creazione di un segreto come parte di uno stack, poiché un'azione di questo tipo comporterebbe, anche se brevemente, un segreto che non è etichettato 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/*"
      ],
      "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/*"
      ],
```

```
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    }
  ]
}
```

Per un elenco di tutti i servizi e delle azioni che supportano sia AWS Organizations SCPs nelle policy di autorizzazione di IAM che nelle policy di autorizzazione IAM, consulta Actions, Resources and Condition Keys Servizi AWS nella IAM User Guide.

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 sugli attributi (ABAC) come parte della strategia di sicurezza del cloud AWS . 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 conceda esplicitamente l'`Allow`autorizzazione per i tag pertinenti. APIs 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 politica completa e non deve essere utilizzata come mostrato qui. 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
                }
            }
        }
    ]
}
```

Esempio SCPs di 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

Questo SCP impedisce agli utenti o ai ruoli di qualsiasi account interessato di eliminare i log di flusso o i gruppi di CloudWatch log o i flussi di log di Amazon Elastic Compute Cloud (Amazon EC2).

```
{
  "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

Questo SCP impedisce agli utenti o ai ruoli di qualsiasi account interessato di modificare la configurazione dei tuoi cloud privati EC2 virtuali Amazon (VPCs) per garantire 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": "*"
```

```
    }
  ]
}
```

Risoluzione dei problemi relativi alle politiche di controllo del servizio (SCPs) con AWS Organizations

Utilizzate le informazioni riportate qui per diagnosticare e correggere gli errori più comuni riscontrati nelle politiche di controllo del servizio (SCPs).

Le policy di controllo dei servizi (SCPs) in 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 politiche IAM si basa su questo concetto definendo quali nomi e valori hanno significato e sono compresi da coloro Servizi AWS che utilizzano le politiche per concedere le autorizzazioni.

AWS Organizations utilizza un sottoinsieme della sintassi e della grammatica IAM. Per informazioni dettagliate, consultare 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 non è corretto perché contiene due oggetti al livello superiore (richiamati in): *red*

JSON

```
{
  "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:

JSON

```
{
  "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:

JSON

```
{
  "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:

JSON

```
{
  "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.

> **Note**
>
> Se si salva la policy utilizzando il AWS Management Console, lo spazio bianco aggiuntivo tra gli elementi JSON e al di fuori delle virgolette viene rimosso e non conteggiato. Se si salva la policy utilizzando un'operazione SDK o la AWS CLI, la policy viene salvata esattamente come è stata fornita e non si verifica alcuna rimozione automatica dei caratteri.

Politiche di controllo delle risorse (RCPs)

> **Note**
>
> Politiche di controllo dei servizi (SCPs) e politiche di controllo delle risorse () RCPs
> Utilizza un SCP quando devi limitare le autorizzazioni dei responsabili IAM all'interno degli account dei membri della tua organizzazione.
> Utilizza un RCP quando devi limitare i responsabili IAM esterni agli account dell'organizzazione che effettuano richieste di accesso alle risorse all'interno degli account dei membri dell'organizzazione.
> Per ulteriori informazioni, consulta Understanding SCPs and. RCPs

Le politiche di controllo delle risorse (RCPs) sono un tipo di politica organizzativa che è possibile utilizzare per gestire le autorizzazioni all'interno dell'organizzazione. RCPs offrono il controllo centralizzato sulle autorizzazioni massime disponibili per le risorse dell'organizzazione. RCPs ti aiutano a garantire che le risorse dei tuoi account rispettino le linee guida per il controllo degli accessi della tua organizzazione. RCPs sono disponibili solo in un'organizzazione che ha tutte le funzionalità abilitate. RCPs non sono disponibili se l'organizzazione ha abilitato solo le funzionalità di fatturazione consolidata. Per istruzioni sull'attivazione RCPs, consulta. Abilitazione di un tipo di policy

RCPs da soli non sono sufficienti a concedere le autorizzazioni alle risorse dell'organizzazione. Nessun permesso viene concesso da un RCP. Un RCP definisce una barriera di autorizzazioni, o impone dei limiti, alle azioni che le identità possono intraprendere sulle risorse delle organizzazioni. L'amministratore deve comunque collegare politiche basate sull'identità agli utenti o ai ruoli IAM o politiche basate sulle risorse alle risorse dei tuoi account per concedere effettivamente le autorizzazioni. Per ulteriori informazioni, consulta Politiche basate sull'identità e politiche basate sulle risorse nella Guida per l'utente IAM.

Le autorizzazioni effettive sono l'intersezione logica tra ciò che è consentito dalle politiche di controllo del servizio (SCPs) RCPs e ciò che è consentito dalle politiche basate sull'identità e sulle risorse.

> **RCPs non influiscono sulle risorse dell'account di gestione**
>
> RCPs non influiscono sulle risorse dell'account di gestione. Influiscono solo sulle risorse degli account dei membri all'interno dell'organizzazione. Ciò significa che RCPs si applicano anche agli account dei membri designati come amministratori delegati.

Argomenti in questa pagina

Elenco di tale supporto Servizi AWS RCPs

RCPs si applicano alle azioni relative a quanto segue Servizi AWS:

- Amazon S3
- AWS Security Token Service
- AWS Key Management Service
- Amazon SQS
- AWS Secrets Manager
- Amazon Elastic Container Registry
- Amazon OpenSearch Serverless

Effetti dei test di RCPs

AWS ti consiglia vivamente di non dedicarti RCPs alla radice della tua organizzazione senza aver testato a fondo l'impatto che la politica ha sulle risorse dei tuoi account. Puoi iniziare collegandoti RCPs ai singoli account di prova, spostandoli verso l' OUs alto nella gerarchia e poi avanzando all'interno della struttura organizzativa, se necessario. Un modo per determinarne l'impatto consiste nell'esaminare AWS CloudTrail i log per verificare la presenza di errori di accesso negato.

Dimensione massima di RCPs

Tutti i caratteri del tuo RCP vengono conteggiati ai fini della dimensione massima. Gli esempi di questa guida mostrano i caratteri RCPs formattati con spazi bianchi aggiuntivi 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**
>
> Usa l'editor visivo per creare il tuo RCP. Rimuove automaticamente lo spazio vuoto aggiuntivo.

Collegamento RCPs a diversi livelli dell'organizzazione

È possibile RCPs collegarlo direttamente ai singoli account o alla radice dell'organizzazione. OUs Per una spiegazione dettagliata del RCPs funzionamento, consultaValutazione RCP.

Effetti RCP sulle autorizzazioni

RCPs sono un tipo di politica AWS Identity and Access Management (IAM). Sono strettamente correlate alle politiche basate sulle risorse. Tuttavia, un RCP non concede mai le autorizzazioni. RCPs Sono invece controlli di accesso che specificano le autorizzazioni massime disponibili per le risorse dell'organizzazione. Per ulteriori informazioni, consulta Logica di valutazione delle policy nella Guida per l'utente di IAM.

- RCPs si applicano alle risorse per un sottoinsieme di. Servizi AWS Per ulteriori informazioni, consulta Elenco di tale supporto Servizi AWS RCPs.
- RCPs riguardano solo le risorse gestite da account che fanno parte dell'organizzazione che ha allegato il RCPs. Non influiscono sulle risorse degli account esterni all'organizzazione. Ad esempio, considera un bucket Amazon S3 di proprietà dell'account A di un'organizzazione. La bucket policy (una politica basata sulle risorse) consente l'accesso agli utenti dell'Account B esterni all'organizzazione. All'account A è associato un RCP. Tale RCP si applica al bucket S3 nell'Account A anche quando vi accedono utenti dell'Account B. Tuttavia, tale RCP non si applica alle risorse dell'Account B quando vi accedono gli utenti dell'Account A.
- Un RCP limita le autorizzazioni per le risorse negli account dei membri. Qualsiasi risorsa in un account dispone solo delle autorizzazioni consentite da ogni genitore superiore a tale account. Se un'autorizzazione è bloccata a qualsiasi livello superiore a quello dell'account, una risorsa nell'account interessato non dispone di tale autorizzazione, anche se il proprietario della risorsa stabilisce una politica basata sulle risorse che consente l'accesso completo a qualsiasi utente.

- RCPs si applicano alle risorse autorizzate come parte di una richiesta operativa. Queste risorse sono disponibili nella colonna «Tipo di risorsa» della tabella Azione del Service Authorization Reference. Se una risorsa è specificata nella colonna «Tipo di risorsa», viene applicato l'account principale chiamante. RCPs Ad esempio, `s3:GetObject` autorizza la risorsa oggetto. Ogni volta che viene effettuata una `GetObject` richiesta, verrà applicato un RCP applicabile per determinare se il principale richiedente può richiamare l'operazione. `GetObject` Un RCP applicabile è un RCP collegato a un account, a un'unità organizzativa (OU) o alla radice dell'organizzazione proprietaria della risorsa a cui si accede.
- RCPs influiscono solo sulle risorse degli account dei membri dell'organizzazione. Non hanno alcun effetto sulle risorse dell'account di gestione. Ciò significa che RCPs si applicano anche agli account dei membri designati come amministratori delegati. Per ulteriori informazioni, consulta Best practice per l'account di gestione.
- Quando un principale effettua una richiesta di accesso a una risorsa all'interno di un account a cui è collegato un RCP (una risorsa con un RCP applicabile), l'RCP viene incluso nella logica di valutazione delle politiche per determinare se al principale è consentito o negato l'accesso.
- RCPs influiscono sulle autorizzazioni effettive dei responsabili che cercano di accedere alle risorse in un account membro con un RCP applicabile, indipendentemente dal fatto che i responsabili appartengano o meno alle stesse organizzazioni. Ciò include gli utenti root. L'eccezione è quando i principali sono ruoli collegati ai servizi perché RCPs non si applicano alle chiamate effettuate da ruoli collegati ai servizi. I ruoli collegati ai servizi consentono di eseguire le azioni necessarie Servizi AWS per conto dell'utente e non possono essere limitati. RCPs
- Agli utenti e ai ruoli devono comunque essere concesse le autorizzazioni con politiche di autorizzazione IAM appropriate, comprese le politiche basate sull'identità e sulle risorse. Un utente o un ruolo senza alcuna policy di autorizzazione IAM non ha accesso, anche se un RCP applicabile consente tutti i servizi, tutte le azioni e tutte le risorse.

Risorse ed entità non limitate da RCPs

Non è possibile utilizzare RCPs per limitare quanto segue:

- Qualsiasi azione sulle risorse dell'account di gestione.
- RCPs non influiscono sulle autorizzazioni effettive di alcun ruolo collegato al servizio. I ruoli collegati ai servizi sono un tipo unico di ruolo IAM collegato direttamente a un AWS servizio e includono tutte le autorizzazioni necessarie al servizio per chiamare altri servizi per tuo conto. AWS Le autorizzazioni dei ruoli collegati ai servizi non possono essere limitate da. RCPs RCPs inoltre

non influiscono sulla capacità AWS dei servizi di assumere un ruolo collegato ai servizi; vale a dire, anche la politica di fiducia del ruolo collegato ai servizi non è influenzata da. RCPs

- RCPs non si applicano a for.Chiavi gestite da AWSAWS Key Management Service Chiavi gestite da AWS vengono creati, gestiti e utilizzati per tuo conto da un Servizio AWS. Non puoi modificare o gestire le loro autorizzazioni.
- RCPs non influiscono sulle seguenti autorizzazioni:

Servizio	API	Risorse non autorizzate da RCPs
AWS Key Management Service	`kms:RetireGrant`	RCPs non influisco no sull'`kms:RetireGrant` autorizzazione. Per ulteriori informazioni su come *`kms:RetireGrant`* viene determinata l'autorizzazione a, consulta Ritiro e revoca delle sovvenzioni nella Guida per gli sviluppatori.AWS KMS

Valutazione RCP

> **Note**
>
> Le informazioni contenute in questa sezione non si applicano ai tipi di policy di gestione, incluse le politiche di backup, le politiche di tag, le politiche delle applicazioni di chat o le politiche di opt-out dei servizi AI. Per ulteriori informazioni, consulta Comprendere l'ereditarietà delle policy di gestione.

Poiché puoi allegare più politiche di controllo delle risorse (RCPs) a diversi livelli AWS Organizations, comprendere come RCPs vengono valutate può aiutarti a scrivere RCPs il risultato giusto.

Strategia di utilizzo RCPs

La `RCPFullAWSAccess` politica è una politica AWS gestita. Viene automaticamente collegata alla radice dell'organizzazione, a ogni unità organizzativa e a ogni account dell'organizzazione, quando

si abilitano le politiche di controllo delle risorse (RCPs). Non è possibile scollegare questa politica. Questo RCP predefinito consente a tutti i principali e alle azioni di passare attraverso la valutazione RCP, il che significa che fino a quando non inizi a creare e allegare RCPs, tutte le autorizzazioni IAM esistenti continuano a funzionare come facevano. Questa policy AWS gestita non concede l'accesso.

È possibile utilizzare le `Deny` istruzioni per bloccare l'accesso alle risorse dell'organizzazione. Affinché venga negata l'autorizzazione per una risorsa in un account specifico, qualsiasi RCP dalla radice a ciascuna unità organizzativa nel percorso diretto verso l'account (incluso l'account di destinazione stesso) può negare tale autorizzazione.

`Deny`le dichiarazioni sono uno strumento efficace per implementare restrizioni che dovrebbero valere per una parte più ampia dell'organizzazione. Ad esempio, è possibile allegare una politica per impedire che identità esterne all'organizzazione accedano alle risorse a livello principale. Tale politica sarà valida per tutti gli account dell'organizzazione. AWS consiglia vivamente di non RCPs collegarsi alla radice dell'organizzazione senza aver testato a fondo l'impatto che la politica ha sulle risorse dei propri account. Per ulteriori informazioni, consulta Effetti dei test di RCPs.

Nella Figura 1, all'unità organizzativa di produzione è allegato un RCP con una `Deny` dichiarazione esplicita specificata per un determinato servizio. Di conseguenza, sia all'Account A che all'Account B verrà negato l'accesso al servizio in quanto una politica di rifiuto associata a qualsiasi livello dell'organizzazione viene valutata per tutti gli account OUs e i membri sottostanti.

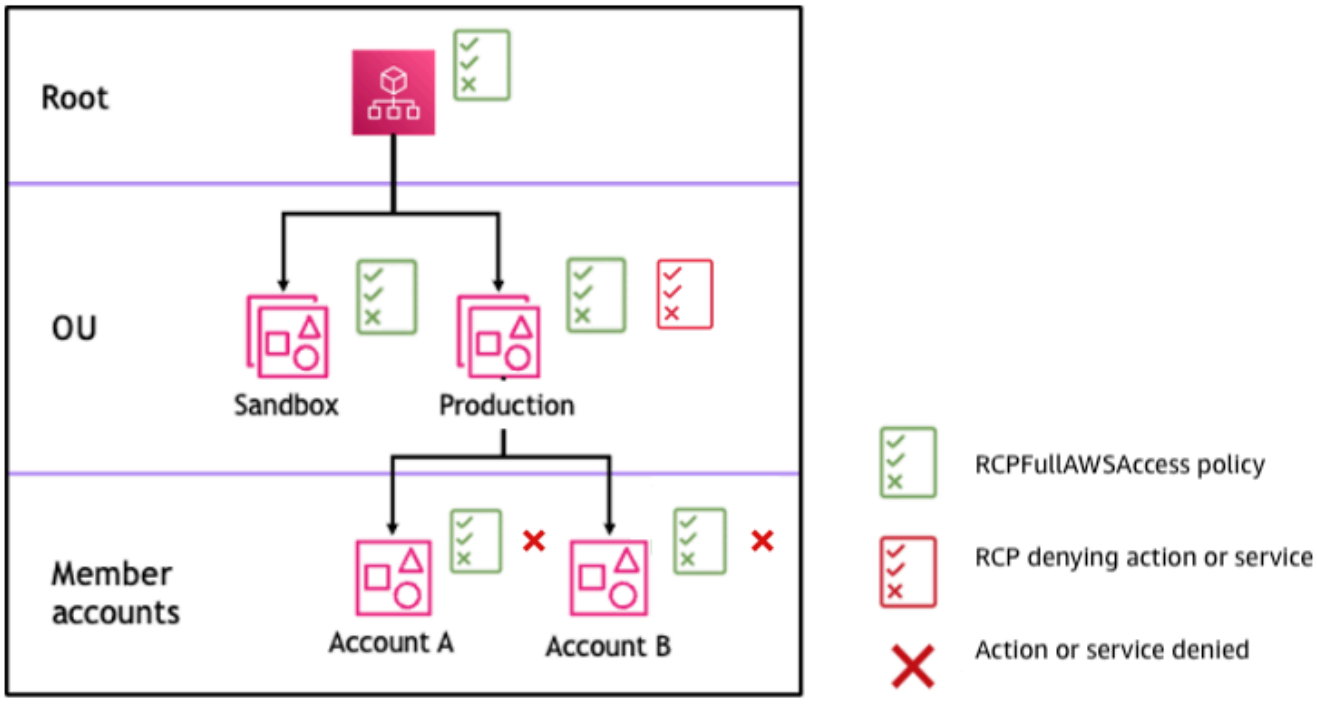


Figura 1: Esempio di struttura organizzativa con una *Deny* dichiarazione allegata a Production OU e relativo impatto sull'Account A e sull'Account B

Sintassi delle RCP

Le politiche di controllo delle risorse (RCPs) utilizzano una sintassi simile a quella utilizzata dalle politiche basate sulle risorse. Per ulteriori informazioni sulle policy IAM consulta Panoramica sulle policy IAM nella Guida per l'utente di IAM.

Un RCP è strutturato secondo le regole di JSON. Utilizza gli elementi descritti in questo argomento.

> **Note**
>
> Tutti i caratteri del tuo RCP vengono conteggiati ai fini della sua dimensione massima. Gli esempi di questa guida mostrano i caratteri RCPs formattati con spazi bianchi aggiuntivi 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 su RCPs, vedere. Politiche di controllo delle risorse (RCPs)

Riepilogo degli elementi

La tabella seguente riassume gli elementi della politica che è possibile utilizzare in RCPs.

> **Note**
>
> L'effetto di **`Allow`** è supportato solo per la politica **`RCPFullAWSAccess`**
> L'effetto di `Allow` è supportato solo per la `RCPFullAWSAccess` politica. Questa politica viene automaticamente allegata alla radice dell'organizzazione, a ogni unità organizzativa e a ogni account dell'organizzazione, quando si abilitano le politiche di controllo delle risorse (RCPs). Non è possibile scollegare questa politica. Questo RCP predefinito consente a tutti i principali e alle azioni di passare attraverso la valutazione RCP, il che significa che fino a quando non inizi a creare e allegare RCPs, tutte le autorizzazioni IAM esistenti continuano a funzionare come facevano. Questo non concede l'accesso.

Elemento	Scopo
Versione	Specifica le regole di sintassi del linguaggio da utilizzare per elaborare la policy.
Statement	Serve da container per gli elementi di policy. È possibile inserire più istruzioni RCPs.
Statement ID (Sid)	(Facoltativo) Fornisce un nome semplice per l'istruzione.
Effetto	Definisce se l'istruzione RCP nega l'accesso alle risorse di un account.
Principale	Speciifica il principale a cui è consentito o negato l'accesso alle risorse di un account.
Azione	Specifica il AWS servizio e le azioni consentit e o negate dal protocollo RCP.

Elemento	Scopo
Risorsa	Speciifica le AWS risorse a cui si applica l'RCP.
NotResource	Speciifica le AWS risorse che sono esenti dall'RCP. Utilizzato invece dell'elemento `Resource`.
Condition	Specifica le condizioni che stabiliscono quando l'istruzione è attiva.

Argomenti

- Elemento Version
- Elemento Statement
- Elemento Statement ID (Sid)
- Elemento Effect
- Elemento Principal
- Elemento Action
- Elementi Resource e NotResource
- Elemento Condition
- Elementi non supportati

Elemento **`Version`**

Ogni RCP deve includere un `Version` elemento 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 RCP è composto da uno o più `Statement` elementi. È possibile avere una sola parola chiave `Statement` in una policy, ma il valore può essere una matrice JSON di istruzioni (circondata da caratteri [ ]).

L'esempio seguente mostra una singola istruzione composta da `Resource` elementi singoli `EffectPrincipal`,`Action`, e.

```
 {
    "Statement": {
        "Effect": "Deny",
        "Principal": "*",
        "Action": "*",
        "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. L'esempio seguente RCP mostra un'`Sid`istruzione di esempio.

```
{
    "Statement": {
        "Sid": "DenyAllActions",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "*",
        "Resource": "*"
    }
```

```
}
```

Per ulteriori informazioni, consulta IAM JSON Policy Elements: Sid nella IAM User Guide.

Elemento **`Effect`**

Ogni istruzione deve contenere un elemento `Effect`. Utilizzando il valore di `Deny` nell'`Effect`elemento, puoi limitare l'accesso a risorse specifiche o definire le condizioni relative al momento in cui RCPs entrano in vigore. Per RCPs ciò che crei, il valore deve essere`Deny`. Per ulteriori informazioni, consulta Valutazione RCP e IAM JSON Policy Elements: Effect in the IAM User Guide.

Elemento **`Principal`**

Ogni istruzione deve contenere l'`Principal`elemento. È possibile specificare «*» solo nell'`Principal`elemento di un RCP. Utilizzate l'`Conditions`elemento per limitare i principi specifici.

Per ulteriori informazioni, consulta IAM JSON Policy Elements: Principal nella IAM User Guide.

Elemento **`Action`**

Ogni istruzione deve contenere l'`Action`elemento.

Il valore dell'`Action`elemento è una stringa o un elenco (un array JSON) di stringhe che identificano AWS i servizi e le azioni consentiti o negati dall'istruzione.

Ogni stringa è composta dall'abbreviazione del servizio (ad esempio «s3", «sqs» o «sts»), tutta minuscola, seguita da due punti e quindi da un'azione del servizio. In genere, vengono tutti immessi con ogni parola che inizia con una lettera maiuscola e il resto con una lettera minuscola. Ad esempio: `"s3:ListAllMyBuckets"`.

È inoltre possibile utilizzare caratteri jolly come l'asterisco (*) o il punto interrogativo (?) in un RCP:

- 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 `"sts:Get*"` corrisponde solo alle AWS STS azioni che iniziano con «Get».
- Utilizzare il punto interrogativo (?) come carattere jolly per abbinare un singolo carattere.

> **Note**
>
> Wild card (*) e punti interrogativi (?) può essere usato in qualsiasi punto del nome dell'azione

A differenza di con SCPs, puoi usare caratteri jolly come l'asterisco (*) o il punto interrogativo (?) in un punto qualsiasi del nome dell'azione.

Per un elenco dei servizi che supportano RCPs, consultaElenco di tale supporto Servizi AWS RCPs. Per un elenco delle azioni e dei Servizio AWS supporti, vedere Azioni, risorse e chiavi di condizione per AWS i servizi nel riferimento di autorizzazione del servizio.

Per ulteriori informazioni, consulta Elementi delle policy JSON IAM: Action nella Guida per l'utente di IAM.

Elementi **`Resource`** e **`NotResource`**

Ogni istruzione deve contenere l'`NotResource`elemento `Resource` or.

È possibile utilizzare caratteri jolly come l'asterisco (*) o il punto interrogativo (?) nell'elemento risorsa:

- Usa un asterisco (*) come carattere jolly per abbinare più risorse che condividono parte di un nome.
- Utilizzare il punto interrogativo (?) come carattere jolly per abbinare un singolo carattere.

Per ulteriori informazioni, consulta IAM JSON Policy Elements: Resource e consulta IAM JSON Policy Elements: NotResource nella IAM User Guide.

Elemento **`Condition`**

È possibile specificare un `Condition` elemento nelle dichiarazioni di deny in un RCP.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition:": {
                "BoolIfExists": {
```

```
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

Questo RCP nega l'accesso alle operazioni e alle risorse di Amazon S3 a meno che la richiesta non avvenga tramite trasporto sicuro (la richiesta è stata inviata tramite TLS).

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 in: RCPs

- `NotPrincipal`
- `NotAction`

Esempi di policy di controllo delle risorse

Gli esempi di politiche di controllo delle risorse (RCPs) visualizzati in questo argomento sono solo a scopo informativo. Per esempi di perimetri dei dati, vedere Esempi di policy perimetrali dei dati in. GitHub

> **Prima di utilizzare questi esempi**
>
> Prima di utilizzare questi esempi RCPs nella tua organizzazione, procedi come segue:
>
> - Esamina e personalizzali attentamente in base alle tue esigenze specifiche. RCPs
> - Esegui test approfonditi RCPs nel tuo ambiente con i AWS servizi che utilizzi.
>
> Le politiche di esempio in questa sezione dimostrano l'implementazione e l'uso di RCPs. Non devono essere interpretate come suggerimenti o best practice AWS ufficiali da implementare esattamente come mostrato. È responsabilità dell'utente testare attentamente qualsiasi politica per verificarne l'idoneità a risolvere i requisiti aziendali del proprio ambiente. Le politiche di controllo delle risorse basate sulla negazione possono limitare o bloccare

involontariamente l'uso dei AWS servizi, a meno che non si aggiungano le eccezioni necessarie alla politica.

Esempi generali

Argomenti

- RCPFullAWSAccess
- Protezione dei deputati confusa tra diversi servizi
- Limita l'accesso alle sole connessioni HTTPS alle tue risorse
- Controlli coerenti delle policy relative ai bucket Amazon S3

RCPFullAWSAccess

La seguente politica è una politica AWS gestita e viene automaticamente associata alla radice dell'organizzazione, a ogni unità organizzativa e a ogni account dell'organizzazione, quando si abilitano le politiche di controllo delle risorse (). RCPs Non è possibile scollegare questa politica. Questo RCP predefinito consente a tutti i principali e le azioni di accedere alle tue risorse, il che significa che finché non inizi a creare e allegare RCPs, tutte le tue autorizzazioni IAM esistenti continueranno a funzionare come facevano. Non è necessario testare l'effetto di questa politica in quanto consentirà il proseguimento del comportamento di autorizzazione esistente per le risorse.

JSON

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

Protezione dei deputati confusa tra diversi servizi

Alcuni Servizi AWS (servizi di chiamata) utilizzano il proprio Servizio AWS principale per accedere alle AWS risorse di altri Servizi AWS (denominati servizi). Quando un attore non destinato ad avere accesso a una AWS risorsa tenta di sfruttare la fiducia di un Servizio AWS committente per interagire con risorse a cui non è destinato ad avere accesso, si parla del problema del vicario confuso tra servizi. Per ulteriori informazioni, consulta The confused deputy problem nella IAM User Guide

La seguente politica richiede che Servizio AWS i responsabili accedano alle tue risorse solo per conto di richieste provenienti dalla tua organizzazione. Questa politica applica il controllo solo sulle richieste `aws:SourceAccount` presenti, in modo da non influire sulle integrazioni di servizi che non richiedono l'uso di`aws:SourceAccount`. Se `aws:SourceAccount` è presente nel contesto della richiesta, la `Null` condizione verrà valutata come ugualetrue, causando l'applicazione della `aws:SourceOrgID` chiave.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceConfusedDeputyProtection",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "s3:*",
                "sqs:*",
                "kms:*",
                "secretsmanager:*",
                "sts:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceOrgID": "my-org-id",
                    "aws:SourceAccount": [
                        "third-party-account-a",
                        "third-party-account-b"
                    ]
                },
                "Bool": {
```

```
                    "aws:PrincipalIsAWSService": "true"
                },
                 "Null": {
                    "aws:SourceArn": "false"
                }
            }
        }
    ]
}
```

Limita l'accesso alle sole connessioni HTTPS alle tue risorse

La seguente politica richiede che l'accesso alle risorse avvenga solo su connessioni crittografate tramite HTTPS (TLS). Questo può aiutarti a impedire a potenziali aggressori di manipolare il traffico di rete.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceSecureTransport",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "sts:*",
                "s3:*",
                "sqs:*",
                "secretsmanager:*",
                "kms:*"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

Controlli coerenti delle policy relative ai bucket Amazon S3

Il seguente RCP contiene più istruzioni per applicare controlli di accesso coerenti sui bucket Amazon S3 della tua organizzazione.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceS3TlsVersion",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "NumericLessThan": {
                    "s3:TlsVersion": [
                        "1.2"
                    ]
                }
            }
        },
        {
            "Sid": "EnforceKMSEncryption",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "s3:x-amz-server-side-encryption-aws-kms-key-id": "true"
                }
            }
        }
    ]
}
```

- L'ID dell'istruzione`EnforceS3TlsVersion`: è necessaria una versione TLS minima 1.2 per l'accesso ai bucket S3.

- L'ID dell'istruzione`EnforceKMSEncryption`: richiede che gli oggetti siano crittografati sul lato server con chiavi KMS.

Politiche di gestione in AWS Organizations

Le politiche di gestione consentono di configurare e gestire centralmente Servizi AWS e le relative funzionalità. Il OUs modo in cui tali politiche influiscono sugli account che le ereditano dipende dal tipo di politica di gestione a AWS Organizations cui si applica. Consulta gli argomenti di questa sezione per saperne di più sui termini e sui concetti pertinenti relativi alle policy di gestione.

Argomenti

Prerequisiti e autorizzazioni per le politiche di gestione per AWS Organizations

Questa pagina descrive i prerequisiti e le autorizzazioni richieste per le politiche di gestione per. AWS Organizations

Argomenti

Prerequisiti per le politiche di gestione

L'utilizzo delle politiche di gestione per un'organizzazione richiede quanto segue:

- L'organizzazione deve avere tutte le caratteristiche abilitate.
- È necessario accedere all'account di gestione dell'organizzazione o essere un amministratore delegato.
- Il tuo utente o ruolo AWS Identity and Access Management (IAM) deve disporre delle autorizzazioni elencate nella sezione seguente.

Autorizzazioni per le politiche di gestione

Il seguente esempio di politica IAM fornisce le autorizzazioni per utilizzare tutti gli aspetti delle politiche di gestione in un'organizzazione.

JSON

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

Comprendere l'ereditarietà delle policy di gestione

> **Important**
>
> Le informazioni contenute in questa sezione non si applicano alle politiche di autorizzazione: politiche di controllo del servizio (SCPs) e politiche di controllo delle risorse (RCPs). Per ulteriori informazioni su come SCPs e come RCPs lavorare in una AWS Organizations gerarchia, vedere Valutazione SCP eValutazione RCP.

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

- Quando si associa una politica di gestione alla radice dell'organizzazione, tutti OUs e gli account dell'organizzazione ereditano tale politica.
- 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.

I seguenti argomenti spiegano come le politiche relative ai genitori e alle politiche relative ai figli vengono trasformate in politiche efficaci per 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 allegare le politiche alla radice dell'organizzazione OUs, ai singoli account e a qualsiasi combinazione di queste entità organizzative. 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. Per ulteriori informazioni, consulta Visualizzazione di politiche di gestione efficaci.

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

L' OUs esatto modo in cui le politiche influiscono sugli account che le ereditano dipende dal tipo di politica di gestione scelto. I tipi di policy di gestione includono:

- Policy dichiarative
- Policy di backup
- Policy di tag
- Politiche relative alle applicazioni di chat
- Politiche di disattivazione dei servizi di intelligenza artificiale

La sintassi per i tipi di policy di gestione include Operatori di ereditarietà, che consente di specificare con grande granularità quali elementi delle policy principali vengono applicati e quali elementi possono essere sovrascritti o modificati se ereditati dal figlio e dagli account. OUs

La politica efficace è l'insieme di regole ereditate dalla radice dell'organizzazione e OUs insieme a quelle direttamente collegate 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 di politiche di gestione efficaci.

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 AWS Organizations console, è possibile utilizzare solo l'`@@assign`operatore. 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.

Per informazioni su come funziona l'ereditarietà delle politiche in un'organizzazione, vedere. Esempi di ereditarietà

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.

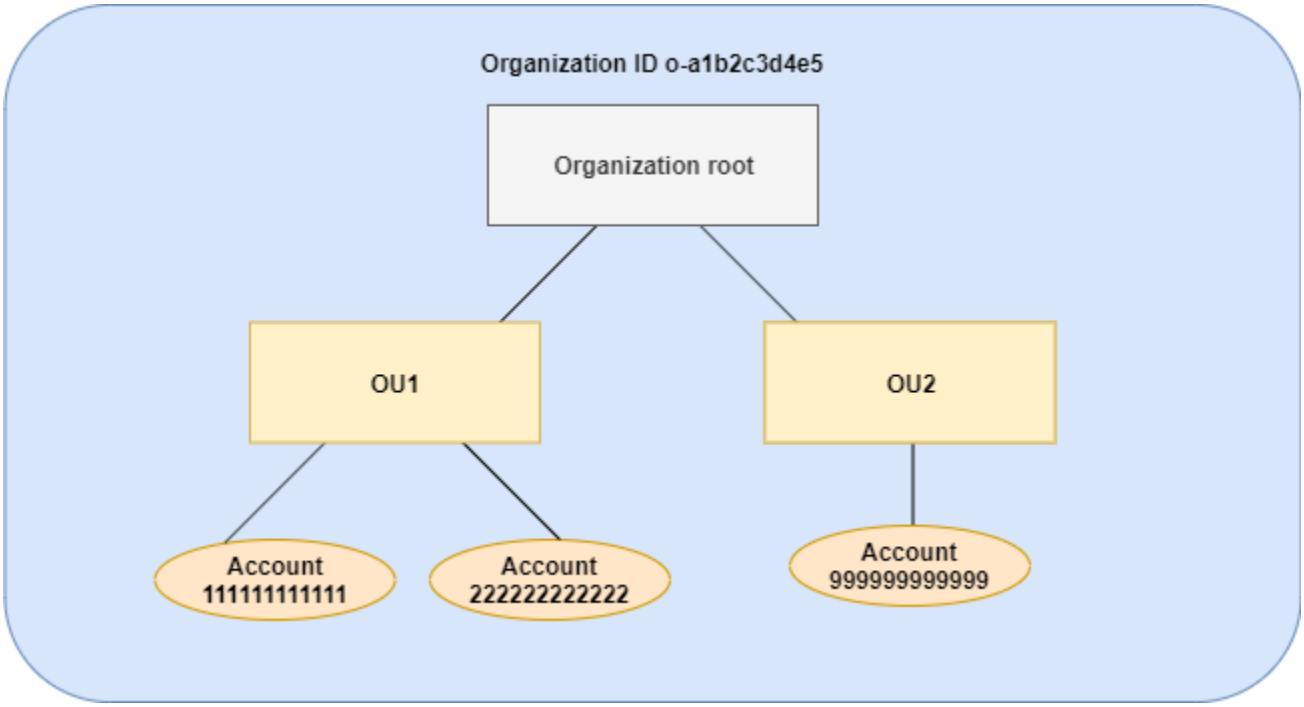
- `"@@operators_allowed_for_child_policies": ["@@all"]` — I bambini OUs e gli account possono utilizzare qualsiasi operatore nelle politiche. Per impostazione predefinita, tutti gli operatori sono consentiti nelle policy figlio.
- `"@@operators_allowed_for_child_policies": ["@@assign", "@@append", "@@remove"]` — I bambini OUs e gli account possono utilizzare solo gli operatori specificati nelle politiche per bambini. Puoi specificare uno o più operatori di impostazione del valore in questo operatore di controllo figlio.
- `"@@operators_allowed_for_child_policies": ["@@none"]` — I bambini OUs e gli account non possono utilizzare gli operatori nelle politiche. 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"
                ]
            }
        }
    }
}
```

Supponiamo che vogliate OU1 che gli utenti utilizzino un valore di tag diverso per una chiave e che vogliate applicare la politica dei tag per tipi di risorse specifici. Poiché la policy A non specifica quali operatori di controllo figlio sono consentiti, tutti gli operatori sono consentiti. È possibile utilizzare l'`@@assign`operatore e creare una politica di tag come la seguente a cui allegare OU1.

Politica B: politica dei OU1 tag

```
{
    "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 mostrato nel diagramma, OU1 include due account: 1111 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"
                ]
            }
        }
    }
}
```

Per questo esempio, allega il criterio 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: politica di OU2 tag per l'aggiunta di valori

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

```
        }
    }
}
```

L'associazione della politica C a OU2 ha i seguenti effetti quando la politica A e la politica C si uniscono per formare la politica di tag efficace per 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: 9999. 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, i criteri B, C e C sono criteri secondari di A. I criteri B sono associati solo a OU1, quindi non ha alcun effetto sull'account 99999.
- 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 aggiungessi altri account OU2, le loro politiche di tag efficaci sarebbero diverse da quelle per l'account 9999. 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"
            ]
        }
    }
}
```

Visualizzazione di politiche di gestione efficaci

Determina la politica di gestione efficace per un account nella tua organizzazione.

Cos'è una politica di gestione efficace?

La politica efficace specifica le regole finali che si applicano a un tipo Account AWS di politica di gestione. È l'aggregazione di una politica di gestione che l'account eredita, più tutte le politiche

per quel tipo di politica di gestione che sono direttamente collegate all'account. Quando si allega una politica di gestione alla radice dell'organizzazione, questa si applica a tutti gli account dell'organizzazione. Quando si allega una politica di gestione a un'unità organizzativa (OU), questa si applica a tutti gli account OUs che appartengono all'unità organizzativa. Quando si allega una politica di gestione direttamente a un account, questa si applica solo a quell'account. Account AWS

Per informazioni su come le policy vengono combinate nella policy effettiva finale, consulta Comprendere l'ereditarietà delle policy di gestione.

Esempio di policy di Backup

La policy di backup allegata alla cartella principale dell'organizzazione potrebbe specificare che tutti gli account dell'organizzazione eseguano il backup di tutte le tabelle Amazon DynamoDB con una frequenza di backup predefinita di 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.

Esempio di politica dei tag

La politica dei tag allegata alla radice dell'organizzazione potrebbe definire un `CostCenter` tag 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.

Esempio di policy sulle applicazioni di chat

Amazon Q Developer nelle applicazioni di chat rivaluterà le configurazioni di applicazioni di chat Amazon Q Developer in chat create in precedenza rispetto alle politiche effettive delle applicazioni di chat e negherà qualsiasi azione precedentemente consentita se è coerente con le impostazioni e i limiti consentiti nella politica effettiva. La politica efficace per un account membro definisce le impostazioni e i guardrail consentiti. Ad esempio, se a un account membro viene applicata una policy per le applicazioni di chat con negazione dell'accesso ai canali Slack pubblici, lo sviluppatore Amazon Q esistente nelle configurazioni delle applicazioni di chat per i canali Slack pubblici nell'account membro verrà disabilitato. Le applicazioni di chat di Amazon Q Developer non invieranno notifiche e

i membri del canale non saranno in grado di eseguire alcuna attività nel canale bloccato. La console delle applicazioni di chat di Amazon Q Developer contrassegnerà i canali interessati come disabilitati con un messaggio di errore appropriato accanto ad esso.

Esempio di disattivazione dei servizi di intelligenza artificiale

La politica di disattivazione dei servizi di intelligenza artificiale allegata alla cartella principale dell'organizzazione potrebbe specificare che tutti gli account dell'organizzazione disattivino l'uso dei contenuti da parte di tutti i servizi di apprendimento AWS automatico. 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 vengono esclusi da tutti Servizi AWS, ad eccezione di un account che attiva Amazon Rekognition.

Come visualizzare la politica di gestione efficace

È possibile visualizzare la politica efficace di un tipo di politica di gestione per un account dall' AWS Management Console AWS API o AWS Command Line Interface.

> **Autorizzazioni minime**
>
> Per visualizzare la politica efficace di un tipo di politica di gestione per un account, è necessario disporre dell'autorizzazione a eseguire le seguenti azioni:
>
> - `organizations:DescribeEffectivePolicy`
> - `organizations:DescribeOrganization` - Obbligatorio solo quando si utilizza la console Organizations

AWS Management Console

Per visualizzare la politica efficace di un tipo di politica di gestione per un account

1. Accedi alla AWS Organizations console . 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, scegli il nome dell'account per il quale desideri visualizzare la politica efficace. Potrebbe essere necessario espandere OUs (scegliere

il ▶)

per trovare l'account desiderato.

3. Nella scheda Politiche, scegli il tipo di politica di gestione per cui desideri visualizzare la politica efficace.
4. Scegli Visualizza la politica efficace per questo Account AWS.

   Nella console viene visualizzata la policy effettiva applicata all'account specificato.

   > **Note**
   >
   > Non puoi copiare e incollare una politica efficace e utilizzarla come JSON per un'altra politica senza modifiche significative. I documenti relativi alle policy devono includere gli operatori di ereditarietà che specificano in che modo ogni impostazione viene unita alla policy definitiva effettiva.

AWS CLI & AWS SDKs

Per visualizzare la politica efficace di un tipo di politica di gestione per un account

È possibile utilizzare uno dei seguenti strumenti per visualizzare la politica efficace:

- 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"
    }
}
```

- AWS SDKs: DescribeEffectivePolicy

Quando una politica di gestione efficace potrebbe essere considerata non valida

Le politiche efficaci relative a un account possono diventare non valide se violano i vincoli definiti per quel particolare tipo di policy. Ad esempio, una politica potrebbe non avere un parametro obbligatorio nella politica definitiva effettiva o superare determinate quote definite per il tipo di politica.

Esempio di policy di backup

Supponiamo di creare una policy di backup con nove regole di backup e di collegarla alla radice dell'organizzazione. Successivamente, si crea un'altra policy di backup per lo stesso piano di backup, con altre due regole, e la si allega a qualsiasi account dell'organizzazione. In tale situazione, esiste una politica efficace non valida per l'account. Non è valida perché l'aggregazione delle due politiche definisce 11 regole per il piano di backup. Il limite è di 10 regole di backup per piano.

> **Warning**
>
> Se un account dell'organizzazione dispone di una politica effettiva non valida, tale account non riceverà aggiornamenti delle politiche efficaci per il particolare tipo di politica. Continua con l'ultima politica valida valida applicata per l'account, a meno che tutti gli errori non vengano corretti.

Policy dichiarative

Le politiche dichiarative consentono di dichiarare e applicare a livello centralizzato la configurazione desiderata per una determinata configurazione su larga scala Servizio AWS all'interno dell'organizzazione. Una volta collegata, la configurazione viene sempre mantenuta quando il servizio aggiunge nuove funzionalità o. APIs Utilizza politiche dichiarative per prevenire azioni non conformi. Ad esempio, puoi bloccare l'accesso pubblico a Internet alle risorse Amazon VPC in tutta l'organizzazione.

I vantaggi principali dell'utilizzo di politiche dichiarative sono:

- Facilità d'uso: è possibile applicare la configurazione di base per an Servizio AWS con poche selezioni nelle AWS Control Tower console AWS Organizations e o con alcuni comandi utilizzando &. AWS CLI AWS SDKs
- Imposta una sola volta e dimentica: la configurazione di base per an Servizio AWS viene sempre mantenuta, anche quando il servizio introduce nuove funzionalità o. APIs La configurazione di base

viene mantenuta anche quando vengono aggiunti nuovi account a un'organizzazione o quando vengono creati nuovi responsabili e risorse.

- Trasparenza: il rapporto sullo stato dell'account consente di esaminare lo stato attuale di tutti gli attributi supportati dalle politiche dichiarative per gli account interessati. È inoltre possibile creare messaggi di errore personalizzabili, che possono aiutare gli amministratori a reindirizzare gli utenti finali alle pagine wiki interne o fornire un messaggio descrittivo che può aiutare gli utenti finali a capire perché un'azione non è riuscita.

Per un elenco completo degli attributi Servizi AWS e degli attributi supportati, consulta. Supportato Servizi AWS e attributi

Argomenti

Come funzionano le politiche dichiarative

Le politiche dichiarative vengono applicate nel piano di controllo del servizio, il che rappresenta un'importante distinzione dalle politiche di autorizzazione come le politiche di controllo dei servizi (SCPs) e le politiche di controllo delle risorse (). RCPs Sebbene le politiche di autorizzazione regolino l'accesso APIs, le politiche dichiarative vengono applicate direttamente a livello di servizio per imporre un intento duraturo. Ciò garantisce che la configurazione di base venga sempre applicata, anche quando vengono introdotte nuove funzionalità o APIs vengono introdotte dal servizio.

La tabella seguente aiuta a illustrare questa distinzione e fornisce alcuni casi d'uso.

	Policy di controllo dei servizi	Politiche di controllo delle risorse	Policy dichiarative		
Perché?	Definire e applicare centralmente controlli di accesso coerenti sui principali (come gli utenti IAM e i ruoli IAM) su larga scala.	Per definire e applicare centralmente controlli di accesso coerenti sulle risorse su larga scala	Per definire e applicare centralmente la configurazione di base per i AWS servizi su larga scala.		
Come?	Controllando le autorizzazioni di accesso massime disponibili dei principali a livello di API.	Controllando le autorizzazioni di accesso massime disponibili per le risorse a livello di API.	Applicando la configurazione desiderata di un Servizio AWS senza utilizzare azioni API.		
Gestisce i ruoli collegati ai servizi?	No	No	Sì		
Meccanismo di feedback	Errore SCP negato dall'accesso non personalizzabile.	Errore RCP negato di accesso non personalizzabile.	Messaggio di errore personalizzabile. Per ulteriori informazioni, consulta Messaggi		

	Policy di controllo dei servizi	Politiche di controllo delle risorse	Policy dichiarative		
			di errore personalizzati per le politiche dichiarative.		
Policy di esempio	Negare l'accesso a AWS in base alla richiesta Regione AWS	Limita l'accesso alle sole connessioni HTTPS alle tue risorse	Impostazioni delle immagini consentite		

Dopo aver creato e allegato una politica dichiarativa, questa viene applicata e applicata in tutta l'organizzazione. Le politiche dichiarative possono essere applicate a un'intera organizzazione, a unità organizzative (OUs) o a conti. Gli account che entrano a far parte di un'organizzazione erediteranno automaticamente la politica dichiarativa dell'organizzazione. Per ulteriori informazioni, consulta Comprendere l'ereditarietà delle policy di gestione.

La politica efficace è l'insieme di regole ereditate dalla radice dell'organizzazione e OUs insieme a quelle direttamente collegate all'account. La policy effettiva specifica l'insieme finale di regole applicabili all'account. Per ulteriori informazioni, consulta Visualizzazione di politiche di gestione efficaci.

Se una politica dichiarativa viene scollegata, lo stato dell'attributo tornerà allo stato precedente prima che la politica dichiarativa fosse allegata.

Messaggi di errore personalizzati per le politiche dichiarative

Le politiche dichiarative consentono di creare messaggi di errore personalizzati. Ad esempio, se un'operazione API fallisce a causa di una politica dichiarativa, è possibile impostare il messaggio di errore o fornire un URL personalizzato, ad esempio un collegamento a un wiki interno o un collegamento a un messaggio che descrive l'errore. Se non si specifica un messaggio di errore

personalizzato, AWS Organizations fornisce il seguente messaggio di errore predefinito:`Example: This action is denied due to an organizational policy in effect.`

È inoltre possibile controllare il processo di creazione di politiche dichiarative, aggiornamento delle politiche dichiarative ed eliminazione delle politiche dichiarative con. AWS CloudTrail CloudTrail può segnalare gli errori operativi dell'API dovuti a politiche dichiarative. Per ulteriori informazioni, consulta Registrazione e monitoraggio.

> **Important**
>
> Non includere informazioni di identificazione personale (PII) o altre informazioni sensibili in un messaggio di errore personalizzato. Le PII includono informazioni generali che possono essere utilizzate per identificare o localizzare un individuo. Copre dati come quelli finanziari, medici, educativi o occupazionali. Gli esempi di PII includono indirizzi, numeri di conto corrente e numeri di telefono.

Rapporto sullo stato dell'account per le politiche dichiarative

Il rapporto sullo stato dell'account consente di esaminare lo stato corrente di tutti gli attributi supportati dalle politiche dichiarative per gli account interessati. Puoi scegliere gli account e le unità organizzative (OUs) da includere nell'ambito del rapporto oppure scegliere un'intera organizzazione selezionando la radice.

Questo rapporto consente di valutare lo stato di preparazione fornendo una suddivisione per regione e indicando se lo stato corrente di un attributo è uniforme tra gli account (tramite`numberOfMatchedAccounts`) o incoerente (tramite). `numberOfUnmatchedAccounts` È inoltre possibile visualizzare il valore più frequente, ovvero il valore di configurazione osservato più frequentemente per l'attributo.

Nella Figura 1, è disponibile un rapporto sullo stato dell'account generato, che mostra l'uniformità tra gli account per i seguenti attributi: Accesso pubblico a blocchi VPC e Accesso pubblico a blocchi di immagini. Ciò significa che, per ogni attributo, tutti gli account inclusi nell'ambito hanno la stessa configurazione per quell'attributo.

Il rapporto sullo stato dell'account generato mostra account incoerenti per i seguenti attributi: impostazioni delle immagini consentite, impostazioni predefinite dei metadati delle istanze, Serial Console Access e Snapshot Block Public Access. In questo esempio, ogni attributo con un account non coerente è dovuto al fatto che esiste un account con un valore di configurazione diverso.

Se esiste un valore più frequente, questo viene visualizzato nella rispettiva colonna. Per informazioni più dettagliate su ciò che controlla ogni attributo, consulta Sintassi delle politiche dichiarative ed esempi di policy.

Puoi anche espandere un attributo per visualizzare una suddivisione per regione. In questo esempio, Image Block Public Access è stato ampliato e in ogni regione, puoi vedere che c'è anche uniformità tra gli account.

La scelta di allegare una politica dichiarativa per l'applicazione di una configurazione di base dipende dal caso d'uso specifico. Utilizza il rapporto sullo stato dell'account per valutare la tua preparazione prima di allegare una politica dichiarativa.

Per ulteriori informazioni, consulta Generazione del rapporto sullo stato dell'account.

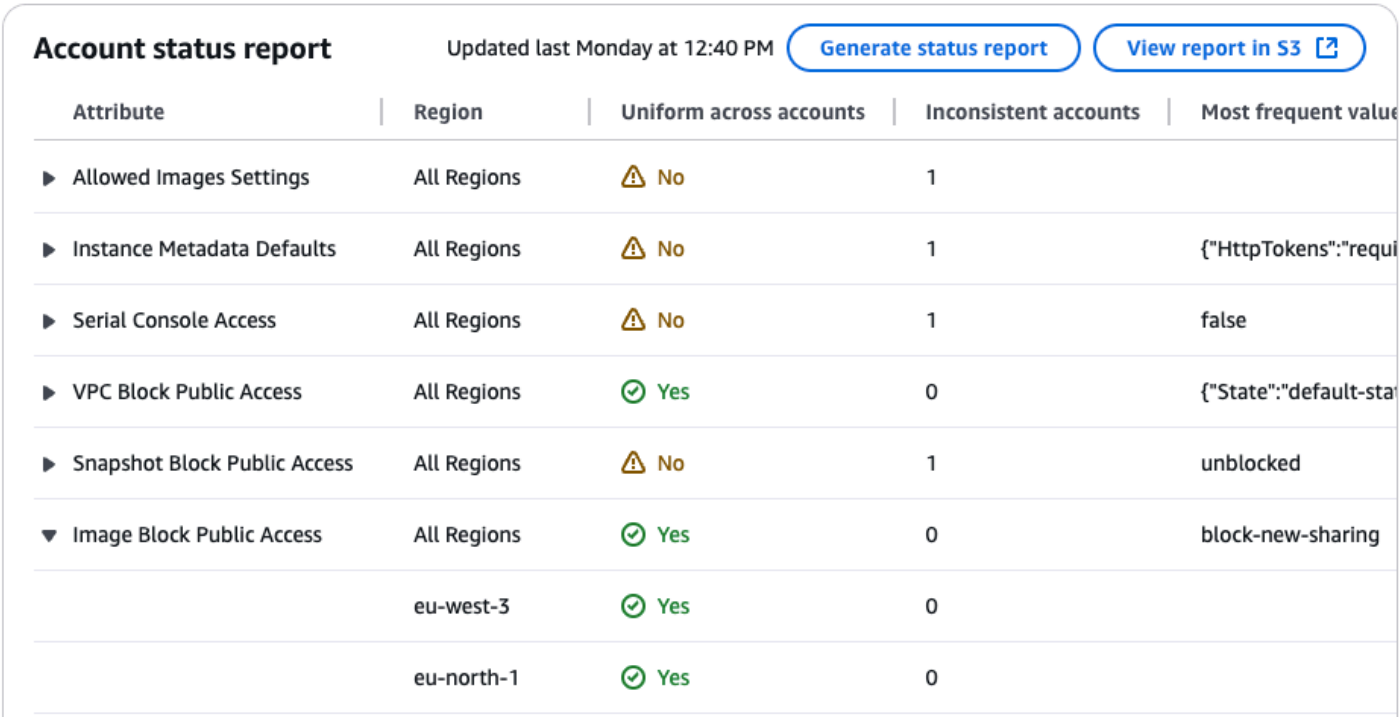


Figura 1: Esempio di rapporto sullo stato dell'account con uniformità tra gli account per VPC Block Public Access e Image Block Public Access.

Supportato Servizi AWS e attributi

Attributi supportati per le politiche dichiarative per EC2

La tabella seguente mostra gli attributi supportati per i servizi EC2 correlati ad Amazon.

Politiche dichiarative per EC2

AWS servizio	Attributo	Effetto politico	Contenuto della politica	Ulteriori informazioni
Amazon VPC	VPC blocca l'accesso pubblico	Controlla se le risorse in Amazon VPCs e le sottoreti possono raggiungere Internet tramite gateway Internet (). IGWs	Visualizza la politica	Per ulteriori informazioni, consulta Bloccare l'accesso pubblico alle sottoreti VPCs e alle sottoreti nella Amazon VPC User Guide.
Amazon EC2	Accesso alla console seriale	Controlla se la console EC2 seriale è accessibile.	Visualizza la politica	Per ulteriori informazioni, consulta Configurare l'accesso alla console EC2 seriale nella Guida per l'utente di Amazon Elastic Compute Cloud.
	Image Block Public Access	Controlla se Amazon Machine Images (AMIs) è condivisibile pubblicamente.	Visualizza la politica	Per ulteriori informazioni, consulta Understand block public access AMIs nella Amazon Elastic Compute

AWS servizio	Attributo	Effetto politico	Contenuto della politica	Ulteriori informazioni
				Cloud User Guide.
	Impostazioni delle immagini consentite	Controlla l'individuazione e l'uso di Amazon Machine Images (AMI) in Amazon EC2 con Allowed AMIs.	Visualizza la politica	Per ulteriori informazioni, consulta Amazon Machine Images (AMIs) nella Amazon Elastic Compute Cloud User Guide.
	Impostazioni predefinite dei metadati delle istanze	Controlla le impostazioni predefinite IMDS per il lancio di tutte le nuove istanze. EC2	Visualizza la politica	Per ulteriori informazioni, consulta Configurare le opzioni di metadati delle istanze per le nuove istanze nella Amazon Elastic Compute Cloud User Guide.

AWS servizio	Attributo	Effetto politico	Contenuto della politica	Ulteriori informazioni
Amazon EBS	Snapshot Block Public Access	Controlla se gli snapshot di Amazon EBS sono accessibili pubblicamente.	Visualizza la politica	Per ulteriori informazioni, consulta Bloccare l'accesso pubblico agli snapshot di Amazon EBS nella Guida per l'utente di Amazon Elastic Block Store.

Guida introduttiva alle politiche dichiarative

Segui questi passaggi per iniziare a utilizzare le politiche dichiarative.

1. Scopri le autorizzazioni necessarie per eseguire attività relative alle politiche dichiarative.
2. Abilita le politiche dichiarative per la tua organizzazione.

> **Note**
>
> È necessario abilitare l'accesso fiduciario
> È necessario abilitare l'accesso affidabile per il servizio in cui la politica dichiarativa applicherà una configurazione di base. In questo modo viene creato un ruolo collegato al servizio di sola lettura che viene utilizzato per generare il rapporto sullo stato dell'account contenente la configurazione esistente per gli account dell'organizzazione.
> Utilizzo della console
> Se utilizzi la console Organizations, questo passaggio fa parte del processo di abilitazione delle politiche dichiarative.
> Utilizzando la AWS CLI
> Se si utilizza il AWS CLI, ce ne sono due distinti APIs:
>
> - EnablePolicyType, che si utilizza per abilitare le politiche dichiarative.

- Enable AWSService Access, che viene utilizzato per abilitare l'accesso attendibile.

Per ulteriori informazioni su come abilitare l'accesso affidabile per un servizio specifico, AWS CLI consulta, Servizi AWS che puoi utilizzare con AWS Organizations.

3. Esegui il rapporto sullo stato dell'account.
4. Crea una politica dichiarativa.
5. Allega la politica dichiarativa alla radice, all'unità organizzativa o all'account dell'organizzazione.
6. Visualizza la politica dichiarativa efficace combinata che si applica 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

- Scopri la sintassi delle politiche dichiarative e guarda esempi di politiche

Best practice per l'utilizzo delle policy dichiarative

AWS consiglia le seguenti best practice per l'utilizzo delle policy dichiarative.

Sfrutta le valutazioni di preparazione

Utilizza il rapporto sullo stato dell'account relativo alla politica dichiarativa per valutare lo stato attuale di tutti gli attributi supportati dalle politiche dichiarative per i conti interessati. Puoi scegliere gli account e le unità organizzative (OUs) da includere nell'ambito del rapporto oppure scegliere un'intera organizzazione selezionando la radice.

Questo rapporto consente di valutare lo stato di preparazione fornendo una suddivisione per regione e indicando se lo stato corrente di un attributo è uniforme tra gli account (tramite`numberOfMatchedAccounts`) o incoerente (tramite). `numberOfUnmatchedAccounts` È inoltre possibile visualizzare il valore più frequente, ovvero il valore di configurazione osservato più frequentemente per l'attributo.

La scelta di allegare una policy dichiarativa per l'applicazione di una configurazione di base dipende dal caso d'uso specifico.

Per ulteriori informazioni e un esempio illustrativo, consultaRapporto sullo stato dell'account per le politiche dichiarative.

Inizia in piccolo e poi scala

Per semplificare il debug, inizia con una policy di test. 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.

Ad esempio, puoi iniziare con una politica di test collegata a un singolo account in un ambiente di test non critico. Dopo aver verificato che funziona secondo le vostre specifiche, potete quindi spostare la politica in modo incrementale verso l'alto nella struttura organizzativa verso più account e più unità organizzative ()OUs.

Stabilisci processi di revisione

Implementa processi per monitorare i nuovi attributi dichiarativi, valutare le eccezioni alle politiche e apportare modifiche per mantenere l'allineamento con i requisiti operativi e di sicurezza dell'organizzazione.

Convalida le modifiche utilizzando **`DescribeEffectivePolicy`**

Dopo aver apportato una modifica a una politica dichiarativa, verifica le politiche efficaci per gli account rappresentativi al di sotto del livello in cui hai apportato la modifica. Puoi visualizzare la politica efficace utilizzando o utilizzando AWS Management Console l'operazione DescribeEffectivePolicyAPI o una delle sue AWS CLI varianti o dell' AWS SDK. Assicurati che l'impatto della modifica apportata sulla policy effettiva sia quello previsto.

Comunica e allenati

Assicuratevi che le vostre organizzazioni comprendano lo scopo e l'impatto delle vostre politiche dichiarative. Fornisci indicazioni chiare sui comportamenti previsti e su come gestire gli errori dovuti all'applicazione delle politiche.

Generazione del rapporto sullo stato dell'account per le politiche dichiarative

Il rapporto sullo stato dell'account consente di esaminare lo stato corrente di tutti gli attributi supportati dalle politiche dichiarative per gli account interessati. Puoi scegliere gli account e le unità organizzative (OUs) da includere nell'ambito del rapporto oppure scegliere un'intera organizzazione selezionando la radice.

Questo rapporto consente di valutare lo stato di preparazione fornendo una suddivisione per regione e indicando se lo stato corrente di un attributo è uniforme tra gli account

(tramite`numberOfMatchedAccounts`) o incoerente (tramite). `numberOfUnmatchedAccounts` È inoltre possibile visualizzare il valore più frequente, ovvero il valore di configurazione osservato più frequentemente per l'attributo.

La scelta di allegare una politica dichiarativa per l'applicazione di una configurazione di base dipende dal caso d'uso specifico.

Per ulteriori informazioni e un esempio illustrativo, vedere. Rapporto sullo stato dell'account per le politiche dichiarative

Prerequisiti

Prima di poter generare un rapporto sullo stato dell'account, è necessario eseguire le seguenti operazioni

1. L'`StartDeclarativePoliciesReport`API può essere richiamata solo dall'account di gestione o dagli amministratori delegati di un'organizzazione.
2. È necessario disporre di un bucket S3 prima di generare il report (crearne uno nuovo o utilizzarne uno esistente), deve trovarsi nella stessa regione in cui viene effettuata la richiesta e deve avere una politica di bucket S3 appropriata. Per un esempio di policy S3, consulta Esempio di policy Amazon S3 in Esempi nell'Amazon EC2 API Reference
3. È necessario abilitare l'accesso affidabile per il servizio in cui la politica dichiarativa applicherà una configurazione di base. In questo modo viene creato un ruolo collegato al servizio di sola lettura che viene utilizzato per generare il rapporto sullo stato dell'account contenente la configurazione esistente per gli account dell'organizzazione.

   Utilizzo della console

   Per la console Organizations, questo passaggio fa parte del processo di abilitazione delle politiche dichiarative.

   Utilizzo del AWS CLI

   Per AWS CLI, utilizza l'API Enable AWSService Access.

   Per ulteriori informazioni su come abilitare l'accesso affidabile per un servizio specifico, AWS CLI consulta, Servizi AWS che puoi utilizzare con AWS Organizations.
4. È possibile generare un solo report per organizzazione alla volta. Il tentativo di generare un report mentre ne è in corso un altro genererà un errore.

Accedi al rapporto sullo stato di conformità

> **Autorizzazioni minime**
>
> Per generare un rapporto sullo stato di conformità, è necessaria l'autorizzazione per eseguire le seguenti azioni:
>
> - `ec2:StartDeclarativePoliciesReport`
> - `ec2:DescribeDeclarativePoliciesReports`
> - `ec2:GetDeclarativePoliciesReportSummary`
> - `ec2:CancelDeclarativePoliciesReport`
> - `organizations:DescribeAccount`
> - `organizations:DescribeOrganization`
> - `organizations:DescribeOrganizationalUnit`
> - `organizations:ListAccounts`
> - `organizations:ListDelegatedAdministrators`
> - `organizations:ListAWSServiceAccessForOrganization`
> - `s3:PutObject`

> **Note**
>
> Se il tuo bucket Amazon S3 utilizza la crittografia SSE-KMS, devi includere anche l'autorizzazione nella policy. `kms:GenerateDataKey`

AWS Management Console

Utilizza la seguente procedura per generare un rapporto sullo stato dell'account.

Per generare un rapporto sullo stato dell'account

1. Accedi alla AWS Organizations console . 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 Politiche, scegli Politiche dichiarative per EC2.

3. Nella EC2 pagina Politiche dichiarative per, scegli Visualizza il rapporto sullo stato dell'account dal menu a discesa Azioni.
4. Nella pagina Visualizza il rapporto sullo stato dell'account, scegli Genera rapporto sullo stato.
5. Nel widget Struttura organizzativa, specifica quali unità organizzative (OUs) desideri includere nel rapporto.
6. Scegli Invia.

AWS CLI & AWS SDKs

Per generare un rapporto sullo stato dell'account

Utilizza le seguenti operazioni per generare un rapporto sullo stato di conformità, verificarne lo stato e visualizzare il rapporto:

- `ec2:start-declarative-policies-report`: genera un rapporto sullo stato dell'account. Il rapporto viene generato in modo asincrono e il completamento può richiedere diverse ore. Per ulteriori informazioni, StartDeclarativePoliciesReportconsulta Amazon EC2 API Reference.
- `ec2:describe-declarative-policies-report`: descrive i metadati di un rapporto sullo stato dell'account, incluso lo stato del rapporto. Per ulteriori informazioni, DescribeDeclarativePoliciesReportsconsulta Amazon EC2 API Reference.
- `ec2:get-declarative-policies-report-summary`: recupera un riepilogo del rapporto sullo stato dell'account. Per ulteriori informazioni, GetDeclarativePoliciesReportSummaryconsulta Amazon EC2 API Reference.
- `ec2:cancel-declarative-policies-report`: annulla la generazione di un rapporto sullo stato dell'account. Per ulteriori informazioni, CancelDeclarativePoliciesReportconsulta Amazon EC2 API Reference.

Prima di generare un report, concedi alle politiche EC2 dichiarative l'accesso principale al bucket Amazon S3 in cui verrà archiviato il report. A tale scopo, collega la seguente policy al bucket. Sostituiscilo `amzn-s3-demo-bucket` con il nome effettivo del bucket Amazon S3 e `identity_ARN` con l'identità IAM utilizzata per chiamare l'API. `StartDeclarativePoliciesReport`

JSON

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DeclarativePoliciesReportDelivery",
            "Effect": "Allow",
            "Principal": {
                "AWS": "identity_ARN"
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "report.declarative-policies-
ec2.amazonaws.com"
                }
            }
        }
    ]
}
```

Sintassi ed esempi delle politiche dichiarative

Questa pagina descrive la sintassi delle politiche dichiarative e fornisce esempi.

Considerazioni

- Quando si configura un attributo di servizio utilizzando una politica dichiarativa, ciò potrebbe influire su più fattori. APIs Qualsiasi azione non conforme fallirà.
- Gli amministratori degli account non saranno in grado di modificare il valore dell'attributo di servizio a livello di account individuale.

Sintassi per le politiche dichiarative

Una policy dichiarativa è un file di testo normale strutturato in base alle regole di JSON. La sintassi per le policy dichiarative 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 dichiarativa.

L'esempio seguente mostra la sintassi dichiarativa della policy dichiarativa

```
{
    "ec2_attributes": {
        "exception_message": {
            "@@assign": "Your custom error message.https://myURL"
        },

        ...

        [Insert supported service attributes]

        ...
    }
}
```

- Il nome della chiave di campo `ec2_attributes`. Le politiche dichiarative iniziano sempre con un nome di chiave fisso per il dato. Servizio AWSÈ la prima riga nella policy di esempio precedente. Attualmente le politiche dichiarative supportavano solo i servizi EC2 correlati ad Amazon.
- In`ec2_attributes`, puoi utilizzare `exception_message` per impostare un messaggio di errore personalizzato. Per ulteriori informazioni, consulta Messaggi di errore personalizzati per le politiche dichiarative.
- In`ec2_attributes`, puoi inserire una o più delle politiche dichiarative supportate. Per questi schemi, vedi. Policy dichiarative supportate

Policy dichiarative supportate

Di seguito sono riportati gli attributi Servizi AWS e supportati dalle politiche dichiarative. In alcuni degli esempi seguenti, la formattazione degli spazi bianchi JSON potrebbe essere compressa per risparmiare spazio.

- Blocco dell'accesso pubblico
- Accesso alla console seriale
- Blocco dell'accesso pubblico
- Impostazioni consentite per le immagini
- Impostazioni predefinite dei metadati delle istanze
- Blocco dell'accesso pubblico

VPC Block Public Access

Effetto della politica

Controlla se le risorse in Amazon VPCs e le sottoreti possono raggiungere Internet tramite gateway Internet (). IGWs Per ulteriori informazioni, consulta Configurazione per l'accesso a Internet nella Guida per l'utente di Amazon Virtual Private Cloud.

Contenuto della policy

```
"vpc_block_public_access": {
    "internet_gateway_block": { // (optional)
        "mode": { // (required)
            "@@assign": "block_ingress" // off | block_ingress | block_bidirectional
        },
        "exclusions_allowed": { // (required)
            "@@assign": "enabled" // enabled | disabled
        }
    }
}
```

Di seguito vengono mostrati i campi disponibili per questo attributo

- `"internet_gateway"`:
  - `"mode"`:
    - `"off"`: VPC BPA non è abilitato.
    - `"block_ingress"`: tutto il traffico Internet verso VPCs (a eccezione VPCs delle sottoreti escluse) è bloccato. È consentito solo il traffico da e verso i gateway NAT e i gateway Internet egress-only, poiché questi gateway consentono solo di stabilire connessioni in uscita.
    - `"block_bidirectional"`: tutto il traffico da e verso i gateway Internet e i gateway Internet egress-only (a eccezione delle sottoreti VPCs e delle sottoreti esclusi) è bloccato.
- `"exclusions_allowed"`: Un'esclusione è una modalità che può essere applicata a un singolo VPC o a una singola sottorete che lo esenta dalla modalità VPC BPA dell'account e consentirà l'accesso bidirezionale o egress-only.
  - `"enabled"`: Le esclusioni possono essere create dall'account.
  - `"disabled"`: Le esclusioni non possono essere create dall'account.

> **Note**
>
> Puoi utilizzare l'attributo per configurare se le esclusioni sono consentite, ma non puoi creare esclusioni con questo attributo stesso. Per creare esclusioni, devi crearle nell'account che possiede il VPC. Per ulteriori informazioni sulla creazione di esclusioni VPC BPA, consulta Creazione ed eliminazione delle esclusioni nella Guida per l'utente di Amazon VPC VPC BPA.

Considerazioni

Se utilizzi questo attributo in una politica dichiarativa, non puoi utilizzare le seguenti operazioni per modificare la configurazione applicata per gli account inclusi nell'ambito. L'elenco non è completo:

- `ModifyVpcBlockPublicAccessOptions`
- `CreateVpcBlockPublicAccessExclusion`
- `ModifyVpcBlockPublicAccessExclusion`

Serial Console Access

Effetto politico

Controlla se la console EC2 seriale è accessibile. Per ulteriori informazioni sulla console EC2 seriale, consulta EC2 Serial Console nella Amazon Elastic Compute Cloud User Guide.

Contenuto della policy

```
"serial_console_access": {
    "status": { // (required)
        "@@assign": "enabled" // enabled | disabled
    }
}
```

Di seguito vengono mostrati i campi disponibili per questo attributo

- `"status"`:
  - `"enabled"`: l'accesso alla console EC2 seriale è consentito.
  - `"disabled"`: l'accesso alla console EC2 seriale è bloccato.

Considerazioni

Se si utilizza questo attributo in una politica dichiarativa, non è possibile utilizzare le seguenti operazioni per modificare la configurazione applicata per gli account inclusi nell'ambito. L'elenco non è completo:

- `EnableSerialConsoleAccess`
- `DisableSerialConsoleAccess`

Image Block Public Access

Effetto politico

Controlla se Amazon Machine Images (AMIs) è condivisibile pubblicamente. Per ulteriori informazioni AMIs, consulta Amazon Machine Images (AMIs) nella Amazon Elastic Compute Cloud User Guide.

Contenuto della policy

```
"image_block_public_access": {
    "state": { // (required)
        "@@assign": "block_new_sharing" // unblocked | block_new_sharing
    }
}
```

Di seguito vengono mostrati i campi disponibili per questo attributo

- `"state"`:
  - `"unblocked"`: Nessuna restrizione alla condivisione pubblica di AMIs.
  - `"block_new_sharing"`: Blocca la nuova condivisione pubblica di AMIs. AMIs quelli che erano già stati condivisi pubblicamente rimangono disponibili pubblicamente.

Considerazioni

Se si utilizza questo attributo in una politica dichiarativa, non è possibile utilizzare le seguenti operazioni per modificare la configurazione applicata per gli account inclusi nell'ambito. L'elenco non è completo:

- `EnableImageBlockPublicAccess`

- `DisableImageBlockPublicAccess`

Allowed Images Settings

Effetto politico

Controlla l'individuazione e l'uso di Amazon Machine Images (AMI) in Amazon EC2 con Allowed AMIs.. Per ulteriori informazioni AMIs, consulta Amazon Machine Images (AMIs) nella Amazon Elastic Compute Cloud User Guide.

Contenuto della policy

Di seguito vengono mostrati i campi disponibili per questo attributo

```
"allowed_images_settings": {
    "state": { // (required)
        "@@assign": "enabled" // enabled | disabled | audit_mode
    },
    "image_criteria": { // (optional)
        "criteria_1": {
            "allowed_image_providers": { // limit 200
                "@@append": [
                    "amazon" // amazon | aws_marketplace | aws_backup_vault | 12
 digit account ID
                ]
            }
        }
    }
}
```

- `"state"`:
  - `"enabled"`: L'attributo è attivo e applicato.
  - `"disabled"`: l'attributo è inattivo e non applicato.
  - `"audit_mode"`: L'attributo è in modalità di controllo. Ciò significa che identificherà le immagini non conformi ma non ne bloccherà l'utilizzo.
- `"image_criteria"`: un elenco di `allowed_image_providers` oggetti che definiscono le sorgenti AMI consentite.
  - `"allowed_image_providers"`: un elenco separato da virgole di nomi o account di provider. IDs

Considerazioni

Se si utilizza questo attributo in una politica dichiarativa, non è possibile utilizzare le seguenti operazioni per modificare la configurazione applicata per gli account inclusi nell'ambito. L'elenco non è completo:

- `EnableAllowedImagesSettings`
- `ReplaceImageCriteriaInAllowedImagesSettings`
- `DisableAllowedImagesSettings`

Instance Metadata Defaults

Effetto politico

Controlla le impostazioni predefinite IMDS per tutti i lanci di nuove EC2 istanze. Nota che questa configurazione imposta solo i valori predefiniti e non impone le impostazioni della versione IMDS. Per ulteriori informazioni sulle impostazioni predefinite IMDS, consulta IMDS nella Amazon Elastic Compute Cloud User Guide.

Contenuto della policy

Di seguito vengono mostrati i campi disponibili per questo attributo

```
"instance_metadata_defaults": {
    "http_tokens": { // (required)
        "@@assign": "required" // no_preference | required | optional
    },
    "http_put_response_hop_limit": { // (required)
        "@@assign": "4" // -1 | 1 -> 64
    },
    "http_endpoint": { // (required)
        "@@assign": "enabled" // no_preference | enabled | disabled
    },
    "instance_metadata_tags": { // (required)
        "@@assign": "enabled" // no_preference | enabled | disabled
    }
}
```

- `"http_tokens"`:

- "no_preference": si applicano altre impostazioni predefinite. Ad esempio, i valori predefiniti AMI, se applicabile.
- "required": IMDSv2 deve essere usato. IMDSv1 non è consentito.
- "optional": Sono IMDSv1 IMDSv2 consentiti entrambi.

> **Note**
>
> Versione dei metadati
> Prima di http_tokens impostare su required (IMDSv2 deve essere usato), assicurati che nessuna delle tue istanze stia effettuando IMDSv1 chiamate.

- "http_put_response_hop_limit":
  - "*Integer*": Valore intero compreso tra -1 e 64, che rappresenta il numero massimo di hop che il token dei metadati può percorrere. Per non indicare alcuna preferenza, specificare -1.

> **Note**
>
> Limite di hop
> Se http_tokens è impostato surequired, si consiglia di http_put_response_hop_limit impostarlo su un minimo di 2. Per ulteriori informazioni, consulta Considerazioni sull'accesso ai metadati dell'istanza nella Guida per l'utente di Amazon Elastic Compute Cloud.

- "http_endpoint":
  - "no_preference": si applicano altre impostazioni predefinite. Ad esempio, i valori predefiniti AMI, se applicabile.
  - "enabled": L'endpoint del servizio di metadati dell'istanza è accessibile.
  - "disabled": l'endpoint del servizio di metadati dell'istanza non è accessibile.
- "instance_metadata_tags":
  - "no_preference": si applicano altre impostazioni predefinite. Ad esempio, i valori predefiniti AMI, se applicabile.
  - "enabled": È possibile accedere ai tag di istanza dai metadati dell'istanza.
  - "disabled": Non è possibile accedere ai tag di istanza dai metadati dell'istanza.

Snapshot Block Public Access

Effetto della politica

Controlla se gli snapshot di Amazon EBS sono accessibili al pubblico. Per ulteriori informazioni sugli snapshot EBS, consulta gli snapshot di Amazon EBS nella Amazon Elastic Block Store User Guide.

Contenuto della policy

```
"snapshot_block_public_access": {
    "state": { // (required)
        "@@assign": "block_new_sharing" // unblocked | block_new_sharing |
 block_all_sharing
    }
}
```

Di seguito vengono mostrati i campi disponibili per questo attributo

- `"state"`:
  - `"block_all_sharing"`: blocca tutte le condivisioni pubbliche di snapshot. Gli snapshot che erano già stati condivisi pubblicamente vengono trattati come privati e non sono più disponibili pubblicamente.
  - `"block_new_sharing"`: blocca la nuova condivisione pubblica di istantanee. Gli snapshot che erano già stati condivisi pubblicamente rimangono disponibili pubblicamente.
  - `"unblocked"`: nessuna restrizione alla condivisione pubblica delle istantanee.

Considerazioni

Se si utilizza questo attributo in una politica dichiarativa, non è possibile utilizzare le seguenti operazioni per modificare la configurazione applicata per gli account inclusi nell'ambito. L'elenco non è completo:

- `EnableSnapshotBlockPublicAccess`
- `DisableSnapshotBlockPublicAccess`

Policy di backup

Le policy di backup consentono di gestire e applicare centralmente i piani di backup alle AWS risorse degli account di un'organizzazione.

AWS Backupconsente di creare piani di backup che definiscono come eseguire il backup AWS delle risorse. Le regole del piano includono una serie di impostazioni, come la frequenza di backup, la finestra temporale durante la quale viene eseguito il backup, il Regione AWS contenitore delle risorse di cui eseguire il backup e l'archivio in cui archiviare il backup. È quindi possibile applicare un piano di backup a gruppi di AWS risorse identificati tramite tag. È inoltre necessario identificare un ruolo AWS Identity and Access Management (IAM) che conceda l' AWS Backup autorizzazione a eseguire l'operazione di backup per conto dell'utente.

Le politiche di backup AWS Organizations combinano tutti questi pezzi in documenti di testo JSON. È possibile allegare una policy di backup a qualsiasi elemento della struttura dell'organizzazione, come la radice, le unità organizzative (OUs) e i singoli account. Organizations applica le regole di ereditarietà per combinare le politiche nella radice dell'organizzazione, in qualsiasi elemento principale OUs o allegate all'account. Ciò si traduce in una policy di backup effettiva per ogni account. Questa politica efficace indica AWS Backup come eseguire automaticamente il backup delle risorse. AWS

Come funzionano le policy di backup

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. È quindi possibile allegare una policy di backup OUs che sostituisca 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. È possibile collegare queste politiche a diverse parti dell'albero organizzativo, ad esempio l'unità organizzativa principale o l'unità organizzativa principale, con l'intenzione che tali politiche parziali vengano ereditate dagli account e di livello inferiore OUs . 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 politica non valida e non esegue il backup delle risorse interessate.

> **Important**
>
> AWS Backup può eseguire un backup con successo solo quando viene richiamato da una policy completa ed efficace che contenga 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 efficace per ogni Account AWS membro dell'organizzazione viene visualizzato nella AWS Backup console come piano immutabile per quell'account. Puoi visualizzarlo, ma non modificarlo. Tuttavia, puoi aggiungere o rimuovere i tag del piano di backup utilizzando TagResourcee. UntagResource APIs

Quando AWS Backup inizia un backup basato su un piano di backup creato da policy, è possibile visualizzare lo stato del processo di backup nella AWS Backup console. Un utente di un account membro può visualizzare lo stato e gli eventuali errori relativi ai processi di backup in tale account membro. Se si abilita anche l'accesso affidabile al servizio con AWS Backup, un utente dell'account di gestione dell'organizzazione può visualizzare lo stato e gli errori di tutti i job di backup dell'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

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 efficace utilizzando o utilizzando l' AWS Management Consoleoperazione GetEffectivePolicyAPI o una delle sue varianti AWS CLI o dell' AWS SDK. 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.

Archivia le copie dei backup in altri account Regioni AWS e in altri account dell'organizzazione

Per migliorare la posizione di disaster recovery, è possibile archiviare copie dei backup.

- Un'altra regione: se si archiviano copie del backup in altre aree geografiche Regioni AWS, si contribuisce a proteggere il backup da danneggiamenti o eliminazioni accidentali 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 un altro account Account AWS, aggiungi una barriera di sicurezza che aiuta a proteggerti da un malintenzionato che compromette 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 degli AWS CloudFormation stack set con Organizations per creare automaticamente gli archivi di backup e i ruoli AWS Identity and Access Management (IAM) richiesti in ciascuno degli account membro della tua organizzazione. Puoi creare un set di stack che includa le risorse che desideri siano disponibili automaticamente Account AWS in ogni parte 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. Questo passaggio va

oltre la semplice analisi delle politiche efficaci e garantisce che AWS Backup interpreti le politiche e implementi i piani di backup nel modo previsto.

Utilizzo AWS CloudTrail degli eventi per monitorare le politiche di backup nell'organizzazione

È possibile utilizzare AWS CloudTrail gli eventi per monitorare quando le politiche di backup vengono create, aggiornate o eliminate da qualsiasi account dell'organizzazione 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 ulteriori informazioni, vedere Sintassi della policy ed ereditarietà per i tipi di policy di gestione. Questo argomento è incentrato sull'applicazione della sintassi generale ai requisiti specifici del tipo di policy di backup.

Per ulteriori informazioni sui AWS Backup piani, consulta la Guida per CreateBackupPlangli AWS Backup sviluppatori.

Considerazioni

Sintassi delle politiche

I nomi di chiavi duplicati verranno rifiutati in JSON.

Le politiche devono specificare le risorse Regioni AWS e le risorse di cui eseguire il backup.

Le policy devono specificare il ruolo IAM che AWS Backup assume.

L'utilizzo `@@assign` dell'operatore allo stesso livello può sovrascrivere le impostazioni esistenti. Per ulteriori informazioni, consulta Una politica secondaria sostituisce le impostazioni in una politica principale.

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.

Per ulteriori informazioni, consulta Operatori di ereditarietà ed esempi di policy di Backup.

Ruoli IAM

Il ruolo IAM deve esistere quando si crea un piano di backup per la prima volta.

Il ruolo IAM deve avere l'autorizzazione ad accedere alle risorse identificate tramite tag query.

Il ruolo IAM deve disporre dell'autorizzazione a eseguire il backup.

Casseforti di Backup

I vault devono esistere in ogni area specificata Regioni AWS prima che un piano di backup possa essere eseguito.

I vault devono esistere per ogni AWS account che riceve la policy valida. Per ulteriori informazioni, consulta la sezione Creazione ed eliminazione di Backup vault nella AWS Backup Developer Guide.

Si consiglia di utilizzare gli AWS CloudFormation stack set 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 di AWS CloudFormation .

Quote

Per un elenco delle AWS Backup quote, consulta la sezione Quotas nella Developer Guide.AWS Backup

Sintassi di backup: panoramica

La sintassi della policy di backup include i seguenti componenti:

```
{
    "plans": {
        "PlanName": {
            "rules": { ... },
            "regions": { ... },
            "selections": { ... },
            "advanced_backup_settings": { ... },
            "backup_plan_tags": { ... }
        }
```

```
    }
}
```

Elementi delle policy di backup

Elemento	Descrizione	Richiesto
regole	Elenco delle regole di backup. Ogni regola definisce quando vengono avviati i backup e la finestra di esecuzione per le risorse specificate negli `selections` elementi `regions` and.	Sì
regioni	Elenco delle aree Regioni AWS in cui una politica di backup può proteggere le risorse.	Sì
selezioni	Uno o più tipi di risorse entro i limiti specificati `regions` che il backup `rules` protegge.	Sì
impostazioni di backup_avanzate	Opzioni di configurazione per scenari di backup specifici. Al momento, l'unica impostazione di backup avanzata supportata abilita i backup di Microsoft VSS (VSS) per Windows o SQL Server in esecuzione su un'istanza Amazon EC2 .	No
backup_plan_tags	Tag che desideri associare a un piano di backup. Ogni tag è un'etichetta composta da una chiave e da un valore definiti dall'utente. Con i tag è possibile a gestire, identificare, organizzare, cercare e filtrare i piani di backup.	No

Sintassi di backup: regole

La chiave `rules` politica specifica le attività di backup pianificate AWS Backup eseguite sulle risorse selezionate.

Elementi regola di backup

Elemento	Descrizione	Richiesto
`schedule_expression`	Espressione Cron in formato UTC che specifica quando AWS Backup avvia un processo di backup. Per informazioni sull'espressione cron, consulta Using cron and rate expression to schedule rules nella Amazon EventBridge User Guide.	Sì
`target_backup_vault_name`	Vault di backup in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.	Sì
`start_backup_window_minutes`	Il numero di minuti di attesa prima di annullare un processo di backup verrà annullato se non viene avviato correttamente. Se questo valore è incluso, devono essere necessari almeno 60 minuti per evitare errori.	No
`complete_backup_window_minutes`	Un processo di backup viene avviato correttamente prima che sia completato o annullato da. AWS Backup	No
`enable_continuous_backup`	Specificate se AWS Backup crea backup continui. `True`crea backup continui con funzionalità di point-in-time ripristino (PITR). AWS Backup `False`(o non specificata), crea backup AWS Backup di istantanee.	No

Elemento	Descrizione	Richiesto
	Per ulteriori informazioni sui backup continui, consulta P oint-in-time recovery nella Developer Guide.AWS Backup Nota: i backup compatibili con PITR hanno una conservazione massima di 35 giorni.	

Elemento	Descrizione	Richiesto
`lifecycle`	Specifica quando esegue la AWS Backup transizione di un backup a storage fredda e quando scade. I tipi di risorse che possono passare alla conservazione a freddo sono elencati nella tabella Disponibilità delle funzionalità per risorse La disponibilità delle funzionalità per risorse nella Guida per gli AWS Backup sviluppatori. Ogni ciclo di vita contiene i seguenti elementi: • `move_to_cold_storage_after_days` : Numero di giorni dopo il backup prima che il punto di ripristino venga AWS Backup spostato nella cella frigorifera. • `delete_after_days` : Numero di giorni dopo l'esecuzione del backup prima dell' AWS Backup eliminazione del punto di ripristino. • `opt_in_to_archive_for_supported_resources` : Se viene assegnato come`true`, un piano di backup esegue la transizione delle risorse supportate al livello di archiviazione (a freddo) in base alle impostazioni del ciclo di vita. Nota: I backup trasferiti allo storage fredda devono essere archiviati nello storage fredda per un minimo di 90 giorni. Ciò significa che `delete_after_days` deve essere superiore di 90 giorni a. `move_to_cold_storage_after_days`	No

Elemento	Descrizione	Richiesto

`copy_actions`	Speciifica se AWS Backup copia un backup in una o più posizioni aggiuntive.
	
	Ogni operazione di copia contiene i seguenti elementi:
	
	• `target_backup_vault_arn` : Vault in cui AWS Backup archivia una copia aggiuntiv a del backup.
	  • Utilizzabile `$account` per copie dello stesso account
	  • Usa l'ID account effettivo per le copie tra account
	• `lifecycle` : specifica quando esegue la AWS Backup transizione di un backup a storage fredda e quando scade.
	
	  Ogni ciclo di vita contiene i seguenti elementi:
	  • `move_to_cold_storage_after_days` : Numero di giorni dopo il backup prima che il punto di ripristino venga AWS Backup spostato nella cella frigorifera.
	  • `delete_after_days` : Numero di giorni dopo l'esecuzione del backup prima dell' AWS Backup eliminazione del punto di ripristino.
	
	Nota: I backup trasferiti allo storage fredda devono essere archiviati nello storage fredda per un minimo di 90 giorni.
		No

Elemento	Descrizione	Richiesto
	Ciò significa che `delete_after_days` deve essere superiore di 90 giorni a. `move_to_cold_storage_after_days`	
`recovery_point_tags`	Tag da assegnare alle risorse ripristinate dal backup. Ogni tag contiene i seguenti elementi: • `tag_key`: nome del tag (con distinzione tra maiuscole e minuscole) • `tag_value` : Valore del tag (distinzione tra maiuscole e minuscole)	No
`index_actions`	Specifica se AWS Backup crea un indice di backup degli snapshot di Amazon EBS e/o dei backup di Amazon S3. Gli indici di backup vengono creati per cercare i metadati dei backup. Per ulteriori informazioni sulla creazione dell'indice di backup e sulla ricerca di backup, vedere Ricerca di backup. Nota: sono necessarie autorizzazioni aggiuntive per i ruoli IAM per la creazione dell'indice di backup degli snapshot di Amazon EBS. Ogni azione di indicizzazione contiene il seguente elemento: `resource_types` dove i tipi di risorse supportati per l'indicizzazione sono Amazon EBS e Amazon S3. Questo parametro specifica quale tipo di risorsa verrà attivato per l'indicizzazione.	No

Sintassi di backup: regioni

La chiave di `regions` policy specifica le Regioni AWS che AWS Backup vengono ricercate da per trovare le risorse corrispondenti alle condizioni nella `selections` chiave.

Elementi delle regioni di Backup

Elemento	Descrizione	Richiesto
`regions`	Specifica i Regione AWS codici. Ad esempio: `["us-east-1", "eu-north-1"]` .	Sì

Sintassi di backup: selezioni

La chiave di `selections` policy specifica le risorse di cui è eseguito il backup in base alle regole di una policy di backup.

Esistono due elementi che si escludono a vicenda: e. `tags` `resources` Per essere valida, una politica efficace deve includere `resources` i tag `have` o la selezione.

Se desideri una selezione con condizioni sia per i tag che per le risorse, usa i `resources` tasti.

Elementi di selezione di backup: Tag

Elemento	Descrizione	Richiesto
`iam_role_arn`	Ruolo IAM che AWS Backup presuppone l'interrogazione, l'individuazione e il backup delle risorse nelle regioni specificate. Il ruolo deve disporre di autorizzazioni sufficien ti per interrogare le risorse in base alle condizioni dei tag ed eseguire operazioni di backup sulle risorse corrispondenti.	Sì
`tag_key`	Nome chiave del tag da cercare.	Sì
`tag_value`	Valore che deve essere associato alla tag_key corrispondente.	Sì

Elemento	Descrizione	Richiesto
	AWS Backup include la risorsa solo se tag_key e tag_value corrispondono (distinzione tra maiuscole e minuscole).	
`conditions`	Tagga le chiavi e i valori che desideri includere o escludere Usa string_equals o string_not_equals per includere o escludere tag con una corrispon denza esatta. Usa string_like e string_not_like per includere o escludere tag che contengono o non contengon o caratteri specifici Nota: limitato a 30 condizioni per ogni selezione .	No

Elementi di selezione del backup: Risorse

Elemento	Descrizione	Richiesto
`iam_role_arn`	Ruolo IAM che AWS Backup presuppone l'interrogazione, l'individuazione e il backup delle risorse nelle regioni specificate. Il ruolo deve disporre di autorizzazioni sufficien ti per interrogare le risorse in base alle condizioni dei tag ed eseguire operazioni di backup sulle risorse corrispondenti. Nota: In AWS GovCloud (US) Regions, è necessario aggiungere il nome della partizione all'ARN.	Sì

Elemento	Descrizione	Richiesto
	Ad esempio, "`arn:aws:ec2:*:*:volume/*`" deve essere "»`arn:aws-us-gov:ec2:*:*:volume/*` .	
`resource_types`	Tipi di risorsa da includere in un piano di backup.	Sì
`not_resource_types`	Tipi di risorsa da escludere da un piano di backup.	No
`conditions`	Etichetta le chiavi e i valori che desideri includere o escludere Usa string_equals o string_not_equals per includere o escludere tag con una corrispondenza esatta. Usa string_like e string_not_like per includere o escludere tag che contengono o non contengono caratteri specifici Nota: limitato a 30 condizioni per ogni selezione .	No

Tipi di risorse supportati

Organizations supporta i seguenti tipi di risorse per gli `not_resource_types` elementi `resource_types` and:

- AWS Backup gateway macchine virtuali: "`arn:aws:backup-gateway:*:*:vm/*`"
- AWS CloudFormation pile: "`arn:aws:cloudformation:*:*:stack/*`"
- Tabelle Amazon DynamoDB: "`arn:aws:dynamodb:*:*:table/*`"
- EC2 Istanze Amazon: "`arn:aws:ec2:*:*:instance/*`"
- Volumi Amazon EBS: "`arn:aws:ec2:*:*:volume/*`"
- File system Amazon EFS: "`arn:aws:elasticfilesystem:*:*:file-system/*`"

- Cluster Amazon Aurora/Amazon DocumentDB/Amazon Neptune: `"arn:aws:rds:*:*:cluster:*"`
- Database Amazon RDS: `"arn:aws:rds:*:*:db:*"`
- Cluster Amazon Redshift: `"arn:aws:redshift:*:*:cluster:*"`
- Amazon S3: `"arn:aws:s3:::*"`
- AWS Systems Manager per SAP Database HANA: `"arn:aws:ssm-sap:*:*:HANA/*"`
- AWS Storage Gateway gateway: `"arn:aws:storagegateway:*:*:gateway/*"`
- Database Amazon Timestream: `"arn:aws:timestream:*:*:database/*"`
- FSx File system Amazon: `"arn:aws:fsx:*:*:file-system/*"`
- FSx Volumi Amazon: `"arn:aws:fsx:*:*:volume/*"`

Esempi di codice

Per ulteriori informazioni, consulta Specificare le risorse con il blocco tags e Specificare le risorse con il blocco resources.

Sintassi di backup: impostazioni di backup avanzate

La `advanced_backup_settings` chiave specifica le opzioni di configurazione per scenari di backup specifici. Ogni impostazione contiene i seguenti elementi:

Elementi delle impostazioni di backup e avanzate

Elemento	Descrizione	Richiesto
`advanced_backup_settings`	Specificate 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: Al momento l'unica impostazione di backup avanzata supportata abilita i backup di Microsoft VSS (VSS) per	No

Elemento	Descrizione	Richiesto
	Windows o SQL Server in esecuzione su un'istanza Amazon EC2. Ogni backup avanzato imposta i seguenti elementi: • `Object key name`: Stringa che specifica il tipo di risorsa a cui si applicano le seguenti impostazioni avanzate. Il nome della chiave deve essere il tipo di `"ec2"` risorsa • `Object value`: Stringa contenente una o più impostazioni di backup specifiche per il tipo di risorsa associato. Il valore specifica che il `"windows_vss"` supporto è `enabled` o `disabled` per i backup eseguiti sulle istanze Amazon EC2.	

Esempio:

```
"advanced_backup_settings": {
    "ec2": {
        "windows_vss": {
            "@@assign": "enabled"
        }
```

```
    }
},
```

Sintassi di backup: tag del piano di backup

La chiave di `backup_plan_tags` policy specifica i tag associati a un piano di backup stesso. Ciò non influisce sui tag specificati per `rules` `oselections`.

Elementi tag del piano di backup

Elemento	Descrizione	Richiesto
`backup_plan_tags`	Ogni tag è un'etichetta composta da una chiave e da un valore definiti dall'utente: • `tag_key`: Nome chiave da cercare. Il valore prevede la distinzione tra lettere maiuscole e minuscole. • `tag_value` : Valore collegato al piano di backup e associato `atag_key`. Il valore prevede la distinzione tra lettere maiuscole e minuscole.	No

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: politica assegnata a un nodo principale
- Esempio 2: una politica principale viene unita a una politica secondaria
- Esempio 3: una politica principale impedisce qualsiasi modifica da parte di una politica relativa ai figli
- Esempio 4: una politica principale impedisce la modifica di un piano di backup da parte di una politica secondaria
- Esempio 5: una politica per i figli ha la precedenza sulle impostazioni di una politica principale
- Esempio 6: Specificazione delle risorse con il blocco tags

- Esempio 7: Specificazione delle risorse con il blocco resources

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"
                        },
                        "opt_in_to_archive_for_supported_resources": {
                            "@@assign": "false"
                        }
                    },
                    "target_backup_vault_name": {
```

```
                        "@@assign": "FortKnox"
                    },
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "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"
                                },
                                "opt_in_to_archive_for_supported_resources": {
                                    "@@assign": "false"
                                }
                            }
                        },
                        "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"
                                },
                                "opt_in_to_archive_for_supported_resources": {
                                    "@@assign": "false"
```

```
                                }
                            }
                        }
                    }
                }
            },
            "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 nessuna altra policy viene ereditata o collegata agli account, l'aspetto della policy effettiva resa in ogni applicabile sarà 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",
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": "false"
                    },
                    "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": {
                                "delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180",
                                "opt_in_to_archive_for_supported_resources": "false"
                            }
                        },
                        "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": {
                                "delete_after_days": "28",
```

```
                            "move_to_cold_storage_after_days": "180",
                            "opt_in_to_archive_for_supported_resources": "false"
                        }
                    }
                }
            }
        },
        "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 policy padre ereditata e una policy figlia ereditata o collegata direttamente a un vengono Account AWS unite per formare la policy 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" },
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "28" },
                        "delete_after_days": { "@@assign": "180" },
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "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":
 "28" },
                                "delete_after_days": { "@@assign": "180" },
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                }
            },
            "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" },
                        "delete_after_days": { "@@assign": "365" },
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:Default" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "30" },
                                "delete_after_days": { "@@assign": "365" },
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                },
            "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",
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "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": "28",
                                "delete_after_days": "180",
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [ "PII", "RED" ]
                    }
                }
            }
        },
        "Monthly_Backup_Plan": {
            "regions": [ "us-east-1", "eu-central-1" ],
            "rules": {
                "monthly": {
                    "schedule_expression": "cron(0 5 1 * ? *)",
                    "start_backup_window_minutes": "480",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30",
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:Default" : {
                            "target_backup_vault_arn": {
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "30",
                                "delete_after_days": "365",
```

```
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                }
            },
            "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"
                },
                "index_actions": {
                   "@@operators_allowed_for_child_policies": ["@@none"],
                    "resource_types": {
                        "@@assign": [
                            "EBS",
                            "S3"
                        ]
                    }
                 },
                "lifecycle": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "move_to_cold_storage_after_days": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "28"
                    },
                    "delete_after_days": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "180"
                    },
                    "opt_in_to_archive_for_supported_resources": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "false"
                    }
                },
```

```
                    "copy_actions": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault",
                                "@@operators_allowed_for_child_policies": ["@@none"]
                            },
                            "lifecycle": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "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"
                                },
                                 "opt_in_to_archive_for_supported_resources": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "false"
                                }
                            }
                        }
                    }
                },
                "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",
                    "index_actions": {
```

```
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": "false"
                    },
                    "copy_actions": {
                        "target_backup_vault_arn": "arn:aws:backup:us-
east-1:123456789012:backup-vault:secondary_vault",
                        "lifecycle": {
                            "move_to_cold_storage_after_days": "28",
                            "delete_after_days": "180",
                            "opt_in_to_archive_for_supported_resources": "false"
                        }
                    }
                }
            },
            "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"},
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "delete_after_days": {"@@assign": "2"},
                        "move_to_cold_storage_after_days": {"@@assign": "180"},
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:t2": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:backup-vault:t2"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "28"},
                                "delete_after_days": {"@@assign": "180"},
                                "opt_in_to_archive_for_supported_resources":
 {"@@assign": false}
                            }
                        }
                    }
                }
            },
            "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"},
                        "delete_after_days": {"@@assign": "365"},
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
                    }
                }
            }
        }
    }
}
```

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 anziché. `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",
                     "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30",
                        "opt_in_to_archive_for_supported_resources": "false"

                    },
                    "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": "28",
                                "delete_after_days": "180",
                                "opt_in_to_archive_for_supported_resources": "false"
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                            "tag_key": "dataType",
                            "tag_value": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            }
        }
}
```

Esempio 6: Specificazione delle risorse con il blocco **`tags`**

L'esempio seguente include tutte le risorse con `tag_key` = “`env`” e `tag_value` = `"prod"` e`"gamma"`. Questo esempio esclude le risorse con `tag_key` = `"backup"` e `tag_value` =`"false"`.

```
...
"selections":{
    "tags":{
        "selection_name":{
            "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/IAMRole"},
            "tag_key":{"@@assign": "env"},
            "tag_value":{"@@assign": ["prod", "gamma"]},
            "conditions":{
                "string_not_equals":{
                    "condition_name1":{
                        "condition_key": { "@@assign": "aws:ResourceTag/backup"  },
                        "condition_value": {  "@@assign": "false" }
                    }
```

```
                }
            }
        }
    }
},
...
```

Esempio 7: Specificazione delle risorse con il blocco **`resources`**

Di seguito sono riportati alcuni esempi di utilizzo del `resources` blocco per specificare le risorse.

Example: Select all resources in my account

La logica booleana è simile a quella che potresti usare nelle policy IAM. Il `"resource_types"` blocco utilizza un valore booleano `AND` per combinare i tipi di risorse.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        }
    }
},
...
```

Example: Select all resources in my account, but exclude Amazon EBS volumes

La logica booleana è simile a quella che potresti usare nelle politiche IAM. I `"not_resource_types"` blocchi `"resource_types"` and utilizzano un valore booleano `AND` per combinare i tipi di risorse.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
```

```
            ]
        },
        "not_resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*"
            ]
        }
    }
},
...
```

Example: Select all resources tagged with "backup" : "true", but exclude Amazon EBS volumes

La logica booleana è simile a quella che potresti usare nelle policy IAM. I `"not_resource_types"` blocchi `"resource_types"` and utilizzano un valore booleano `AND` per combinare i tipi di risorse. Il `"conditions"` blocco utilizza un valore booleano. `AND`

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        },
        "not_resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*"
            ]
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key": { "@@assign":"aws:ResourceTag/backup"},
                    "condition_value": {  "@@assign":"true" }
                }
            }
        }
    }
},
...
```

Example: Select all Amazon EBS volumes and Amazon RDS DB instances tagged with both "backup" : "true" and "stage" : "prod"

La logica booleana è simile a quella che potresti usare nelle politiche IAM. Il `"resource_types"` blocco utilizza un valore booleano `AND` per combinare i tipi di risorse. Il `"conditions"` blocco utilizza un valore booleano `AND` per combinare i tipi di risorse e le condizioni dei tag.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:rds:*:*:db:*"
            ]
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@@assign":"true"}
                },
                "condition_name2":{
                    "condition_key":{"@@assign":"aws:ResourceTag/stage"},
                    "condition_value":{"@@assign":"prod"}
                }
            }
        }
    }
},
...
```

Example: Select all Amazon EBS volumes and Amazon RDS instances tagged with "backup" : "true" but not "stage" : "test"

La logica booleana è simile a quella che potresti usare nelle politiche IAM. Il `"resource_types"` blocco utilizza un valore booleano `AND` per combinare i tipi di risorse. Il `"conditions"` blocco utilizza un valore booleano `AND` per combinare i tipi di risorse e le condizioni dei tag.

```
...
"resources":{
```

```
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:rds:*:*:db:*"
            ]
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@@assign":"true"}
                  }
            },
            "string_not_equals":{
                "condition_name2":{
                    "condition_key":{"@@assign":"aws:ResourceTag/stage"},
                    "condition_value":{"@@assign":"test"}
                }
            }
        }
    }
},
...
```

Example: Select all resources tagged with "key1" and a value which begins with "include" but not with "key2" and value that contains the word "exclude"

La logica booleana è simile a quella che potresti usare nelle politiche IAM. Il `"resource_types"` blocco utilizza un valore booleano `AND` per combinare i tipi di risorse. Il `"conditions"` blocco utilizza un valore booleano `AND` per combinare i tipi di risorse e le condizioni dei tag.

In questo esempio, nota l'uso del carattere jolly (`*`) in`include*`, `*exclude*` e. `arn:aws:rds:*:*:db:*` È possibile utilizzare il carattere jolly (`*`) all'inizio, alla fine e al centro di una stringa.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
```

```
                "*"
            ]
        },
        "conditions":{
            "string_like":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/key1"},
                    "condition_value":{"@@assign":"include*"}
                }
            },
            "string_not_like":{
                "condition_name2":{
                    "condition_key":{"@@assign":"aws:ResourceTag/key2"},
                    "condition_value":{"@@assign":"*exclude*"}
                }
            }
        }
    }
},
...
```

Example: Select all resources tagged with "backup" : "true" except Amazon FSx file systems and Amazon RDS resources

La logica booleana è simile a quella che potresti usare nelle policy IAM. I `"not_resource_types"` blocchi `"resource_types"` and utilizzano un valore booleano AND per combinare i tipi di risorse. Il `"conditions"` blocco utilizza un valore booleano AND per combinare i tipi di risorse e le condizioni dei tag.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
            "resource_types":{
                "@@assign": [
                    "*"
               ]
            },
            "not_resource_types":{
                "@@assign":[
                    "arn:aws:fsx:*:*:file-system/*",
                    "arn:aws:rds:*:*:db:*"
                ]
```

```
            },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@@assign":"true"}
                }
            }
        }
    }
},
...
```

Policy di tag

Le politiche relative ai tag consentono di standardizzare i tag associati alle AWS risorse negli account di un'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.

Cosa sono i tag?

I tag sono etichette di attributi personalizzate assegnate o assegnate alle AWS 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 Tagging Resources User Guide. AWS
- 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 Taggare le risorse AWS Organizations.
- Per informazioni sull'etichettatura delle risorse in altri Servizi AWS, 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 politiche di tag implica 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. È possibile correggere i tag non conformi nel AWS servizio in cui è stata creata la risorsa. Puoi anche utilizzare Tag Editor e l'API Resource Groups Tagging per etichettare e rimuovere i tag da più servizi.

  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 le politiche di gestione per AWS Organizations.

> **Important**
>
> Per iniziare con le politiche sui tag, ti AWS consigliamo vivamente di seguire il flusso di lavoro di esempio descritto in Nozioni di base sulle policy di tag prima di passare a politiche 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.

Best practice per l'utilizzo delle policy di tag

AWS consiglia le seguenti best practice per l'utilizzo delle politiche relative ai 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, potresti voler specificare che quando un `CostCenter` tag è associato a AWS Secrets Manager segreti, deve utilizzare il trattamento dei casi 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. Chiedi agli amministratori di trovare e correggere i tag non conformi sulle risorse del loro account utilizzando la procedura descritta nella sezione Evaluating Compliance for an Account nella Tagging Resource User Guide. AWS 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 AWS servizio supporta il controllo dell'accesso tramite tag, consulta That Work with IAM nella IAM Servizi AWS User Guide. Cerca i servizi con Sì nella colonna ABAC (autorizzazione basata sui 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 politiche dei tag implica l'utilizzo di più criteri 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 le politiche di gestione per AWS Organizations
- 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.

Attività	Account a cui accedere	AWS console di servizio da usare
Fase 1: abilita le policy di tag per l'organizzazione.	Account di gestione dell'organizzazione.[1]	AWS Organizations
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.	Qualsiasi AWS servizio con cui ti senti a tuo agio. Ad esempio, puoi utilizzare AWS Secrets Manager e seguire la procedura in Creazione di un segreto di base per creare

Attività	Account a cui accedere	AWS console di servizio da usare
		segreti con segreti conformi e non conformi.
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 AWS servizio 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 AWS servizio 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	AWS console di servizio da utilizzare
Creare policy di tag avanzate. Segui lo stesso processo degli utenti inesperti, ma prova altre 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.	Account di gestione dell'organizzazione.[1]	AWS Organizations
Allega le politiche sui tag ad account aggiuntivi o OUs. 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 vedere un esempio, consulta Richiedere un tag sulle risorse create specificate.	Account di gestione dell'organizzazione.[1]	AWS Organizations

Attività avanzata	Account a cui accedere	AWS console di servizio 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 AWS servizio 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	AWS console di servizio 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	AWS console di servizio 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.	Qualsiasi AWS servizio con cui ti senti a tuo agio. 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.
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 AWS servizio in cui è stata creata la risorsa.

Attività di applicazione	Account a cui accedere	AWS console di servizio da utilizzare
Fase 5: 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 AWS servizio 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.

Utilizzo di Amazon EventBridge per monitorare i tag non conformi

Puoi utilizzare Amazon EventBridge, precedentemente Amazon CloudWatch Events, 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 Amazon EventBridge User Guide.

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 hanno raggruppamenti di risorse simili a contenitori che creano automaticamente risorse per te e i tag possono propagarsi da una

risorsa di un servizio all'altro. Ad esempio, i tag sui gruppi Amazon EC2 Auto Scaling e sui cluster Amazon EMR possono propagarsi automaticamente alle istanze Amazon contenute. EC2 Potresti avere politiche di tag per Amazon EC2 più rigide rispetto ai gruppi di 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.

Argomenti

- Ricerca di risorse non conformi per un account con AWS Organizations
- Correzione dei tag non conformi nelle risorse con AWS Organizations
- Generazione di un rapporto di conformità a livello di organizzazione con AWS Organizations
- Servizi e tipi di risorse che supportano l'applicazione

Ricerca di risorse non conformi per un account con AWS Organizations

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 risorse non conformi per un account con una politica di tag, esegui il comando seguente per salvare i risultati in un file:

```
$ aws resourcegroupstaggingapi get-resources  --region us-east-1 \
    --include-compliance-details \
    --exclude-compliant-resources > outputfile.txt
```

Correzione dei tag non conformi nelle risorse con AWS Organizations

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 per etichettare le operazioni API del AWS servizio che ha creato le risorse non conformi.
- Utilizza le UntagResourcesoperazioni AWS Resource Groups TagResourcesand per aggiungere tag conformi alla politica effettiva o per rimuovere tag non conformi.

Generazione di un rapporto di conformità a livello di organizzazione con AWS Organizations

In qualsiasi momento, puoi generare un rapporto che elenca tutte le risorse etichettate dell' Account AWS 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 start-report-creation --region us-east-1
```

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:

- Amazon API Gateway
  - Chiavi API
  - Piani di utilizzo
  - Tipi di risorsa

Tipo di risorsa

- "apigateway:apikey"
- "apigateway:domainnames"
- "apigateway:restapis"
- "apigateway:restapis/stages"

Tipo di risorsa

Chiavi condizione supportate

Tipi di risorse ARN

- AWS Amplify Amplify Builder: Component
- Tema

- "amplifyuibuilder:app/environment/components"

- "amplifyuibuilder:app/environment/themes"

Tipo di risorsa	Chiavi condizione supportate	ARN
AWS AppConfig Application	aws:ResourceTag/${TagKey}	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}
Profilo di configurazione	aws:ResourceTag/${TagKey}	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/configurationprofile/${ConfigurationProfileId}
Strategia di distribuzione	aws:ResourceTag/${TagKey}	arn:${Partition}:appconfig:${Region}:${Account}:deploymentstrategy/${DeploymentStrategyId}
Ambiente	aws:ResourceTag/${TagKey}	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}

- "appconfig:deploymentstrategy"
- "appconfig:application/environment"

Tipo di risorsa

Tipi di servizio supportati

Chiavi condizione supportate

AWS App Mesh Application Mesh

- "appmesh:ALL_SUPPORTED"
- gateway
- Mesh
- Route
- VirtualGateway
- Gateway virtuale
- Nodo virtuale
- Router virtuale
- Servizio virtuale

- "appmesh:gateway"
- "appmesh:mesh"
- "appmesh:route"
- "appmesh:mesh/virtualGateway"
- "appmesh:mesh/virtualRouter/route"
- "appmesh:mesh/virtualNode"
- "appmesh:mesh/virt

Servizio	Tipo di risorsa	Sintassi JSON
		ualRouter" • "appmesh:mesh/virtualService"
Amazon Athena	• Tutto • Gruppo di lavoro	• "athena:ALL_SUPPORTED" • "athena:workgroup"
AWS Audit Manager	• Tutti • Valutazione • Framework della valutazione • Controllo	• "auditmanager:ALL_SUPPORTED" • "auditmanager:assessment " • "auditmanager:assessmentFramework " • "auditmanager:control "

Tipo di risorsa

Tipo di risorsa

- AWS Backup Plan
- Backup vault
- Gateway
- Hypervisor
- VM

"backup:BackupPlan"

"backup:backup-vault"

"backup-gateway:gateway"

"backup-gateway:hypervisor"

"backup-gateway:vm"

Tipo di risorsa	Chiavi condizione supportate	Tipi di risorsa ARN
AWS Batch	aws:TagKeys aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey}	• batch:AL • batch:SUPPORTED • Processo • Definizione processo • Coda processo
AWS Bug Bust	aws:TagKeys aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey}	• bugbust:AllBugBustEvents • bugbust:SUPPORTED • Evento
AWS Certificate Manager	aws:TagKeys aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey}	• acm:ALL_SUPPORTED • Certificati • Private Certificate Authority

Tipo di risorsa

Tipi di risorsa supportati dal servizio

Tipi di risorsa ARN

Tabulazione JSON

- Amazon Chime SDK Istanza dell'applicazione
- Configurazione
- Canale
- Pipeline
- Riunione
- Applicazione/oni channel multimediali
- SIP media-pipeline dell'applicazione
- Connettore e profilo vocale

- "chime:AllResources"
- "chime:SUPPORTED_RESOURCES"
- "chime:appinstance"
- "chime:appinstancemultimediachannel"
- "chime:appinstancepipeline"
- "chime:meeting"
- "chime:sma"
- "chime:voiceprofile"
- "chime:appinstanceuser"
- "chime:vc"

Servizio	Tipo di risorsa	Sintassi JSON
AWS Clean Rooms	• Tutti • Collaborazione • Tabella configurata • Appartenenza • Associazione della tabella configurata	• "cleanrooms:ALL_SUPPORTED" • "cleanrooms:collaboration" • "cleanrooms:configuredtable" • "cleanrooms:membership" • "cleanrooms:membership/configuredtableassociation"
AWS Cloud9	• Tutti • Ambiente	• "cloud9:ALL_SUPPORTED" • "cloud9:environment"

Amazon CloudFront	Tabella di distribuzione	• "cloudfront:TagResource" • "cloudfront:UntagResource" • "cloudfront:ListTagsForResource" • "cloudfront:distribution"	SUPPORTED
AWS CloudTrail	Trail	• "cloudtrail:AddTags" • "cloudtrail:RemoveTags" • "cloudtrail:ListTags" • "cloudtrail:trail"	SUPPORTED
Amazon CloudWatch	Allarme Regole di Contributor Insights Flusso del parametro	• "cloudwatch:TagResource" • "cloudwatch:UntagResource" • "cloudwatch:ListTagsForResource" • "cloudwatch:alarm" • "cloudwatch:insight-rule" • "cloudwatch:metric-stream"	SUPPORTED

Servizio	Tipo di risorsa	Sintassi JSON
Amazon CloudWatch Internet Monitor	• Monitor	• "internetmonitor:monitor"
CloudWatch Registri Amazon	• Destinazione • Gruppo log	• "logs:destination" • "logs:log-group"
Amazon CloudWatch Observability Access Manager	• Link • Sink	• "oam:link" • "oam:sink"
AWS CodeBuild	• Tutto • Progetto	• "codebuild:ALL_SUPPORTED" • "codebuild:project"

Servizio	Tipo di risorsa	Sintassi JSON
Amazon CodeCatalyst	• Tutto • Connessioni	• "codecatalyst:ALL_SUPPORTED" • "codecatalyst:connections"
AWS CodeCommit	• Tutti • Repository	• "codecommit:ALL_SUPPORTED" • "codecommit:repository"
AWS CodePipeline	• Tutti • Tipo di operazione • Pipeline • Webhook	• "codepipeline:ALL_SUPPORTED" • "codepipeline:actiontype" • "codepipeline:pipeline" • "codepipeline:webhook"

Servizio	Tipo di risorsa	Sintassi JSON
Amazon Cognito Identity	• Tutto • Pool di identità	• "cognito-identity:ALL_SUPPORTED" • "cognito-identity:identitypool"
Pool di utenti Amazon Cognito	• Tutto • Bacino d'utenza	• "cognito-idp:ALL_SUPPORTED" • "cognito-idp:userpool"
Amazon Comprehend	• Tutto • Classificatore di documenti • Riconoscimento delle entità	• "comprehend:ALL_SUPPORTED" • "comprehend:document-classifier" • "comprehend:entity-recognizer"

Nome servizio	Tipo di risorsa	Sintassi JSON
AWS Config	• Tutti • Autorizzazione dell'aggregazione • Aggregatore di configurazione • Regola di configurazione	• "config:ALL_SUPPORTED" • "config:aggregation-authorization" • "config:config-aggregator" • "config:config-rule"
Amazon CodeGuru Revisore	• Tutti • Associazione	• "codeguru-reviewer:ALL_SUPPORTED" • "codeguru-reviewer:association"

Tipo di risorsa

Chiavi condizione supportate

ARN del servizio

CodeGuru Sicurezza Amazon

- CodeGuru Security Scan
- "codeguru-security:ALL_SUPPORTED"
- "codeguru-security:scans"

CodeStar Connections

- Connessione
- Host

- "codestar-connections:ALL_SUPPORTED"

- "codestar-connections:connection"
- "codestar-connections:host"

Tipo di risorsa

Tipi di risorsa ARN

Chiavi condizione

Amazon Connect

- Flusso di contatto
- Associazione di integrazione
- Queue
- Connessione rapida
- Profilo di routing
- Utente

"connect:SUPPORTED"

"connect:instance/contact-flow"

"connect:instance/integration-association"

"connect:instance/queue"

"connect:instance/transfer-destination"

"connect:instance/routing-profile"

"connect:instance/agent"

Servizio	Tipo di risorsa	Sintassi JSON
Amazon Connect Wisdom	Tutto • Assistente • Associazione • Contenuti • Knowledge Base • Sessione	"wisdom:ALL_SUPPORTED" • "wisdom:assistant" • "wisdom:association" • "wisdom:content" • "wisdom:knowledge-base" • "wisdom:session"
AWS Database Migration Service	Tutti • Endpoint • ES • Rep • Subgrp • Attività	"dms:ALL_SUPPORTED" • "dms:endpoint" • "dms:es" • "dms:rep" • "dms:subgrp" • "dms:task"

Tipi di risorsa supportati dal servizio

Tipi di risorsa supportati dal servizio

Tipi di risorsa supportati dal servizio

- Amazon Data Lifecycle Manager
  - Tutti: `ALL_SUPPORTED`
  - Policy: `"dlm:policy"`
- AWS Direct Connect
  - Tutti: `directconnect:ALL_SUPPORTED`
  - Connessione: `"directconnect:dxcon"`
  - Gruppo: `"directconnect:dxlag"`
  - Interfaccia virtuale: `"directconnect:dxvif"`
- Amazon DynamoDB
  - Tutti: `dynamodb:ALL_SUPPORTED`
  - Tabella: `"dynamodb:table"`

Nome servizio	Tipo di risorsa	Sintassi JSON
Amazon EC2	Tutti: ALL_SUPPORTED • Prenotazione di capacità • Flotta di prenotazione della capacità • Gateway carrier • Endpoint Client VPN • Pool CoIP • Gateway del cliente • Host dedicato • Opzioni DHCP • Gateway Internet Egress-only	• "ec2:capacity-reservation" • "ec2:capacity-reservation-fleet" • "ec2:carrier-gateway" • "ec2:client-vpn-endpoint" • "ec2:coip-pool" • "ec2:customer-gateway" • "ec2:dedicated-

Tipo di risorsa

- Indirizzo IP elastico
- Finestra dell'evento
- Attività di esportazione di immagini
- Attività di esportazione dell'istanza
- Parco istanze
- Immagine
- Prenotazione host
- Immagine
- Attività di importazione dell'immagine

Tipo di risorsa

- "ec2:dhcp-options"
- "ec2:egress-only-internet-gateway"
- "ec2:elastic-ip"
- "ec2:instance-event-window"
- "ec2:export-host-image-task"
- "ec2:export-instance-task"

Servizio	Tipo di risorsa	Sintassi JSON
	• Attività di importazione di istantanee • Istanza • Endpoint Instance Connect • Internet Gateway • IP Address Manager • Token di verifica delle risorse esterne di IP Address Manager • Pool di gestione degli indirizzi IP	• "ec2:fleet" • "ec2:fpga-image" • "ec2:host-reservation" • "ec2:image" • "ec2:import-image-task" • "ec2:import-snapshot-task" • "ec2:instance" • "ec2:instance-connect-endpoint" • "ec2:internet-

Servizio | **Tipo di risorsa** | **Sintassi JSON**

- gateway"
- Individuazione delle risorse di IP Address Manager
- Associazione per la scoperta delle risorse di IP Address Manager
- Ambito di IP Address Manager
- IPv4 Piscina
- Coppia di chiavi

- "ec2:ipam"
- "ec2:ipam-external-resource-verification-token"
- "ec2:ipam-pool"
- "ec2:ipam-resource-discovery"
- "ec2:ipam-resource-discovery-association"

Servizio	Tipo di risorsa	Sintassi JSON
	• Modello di avvio • Tabella di routing del gateway locale • Associazione dei gruppi di interfacce virtuali - Local Gateway Route Table • Associazione VPC della tabella di routing del gateway locale • Gateway NAT	• "ec2:ipam-scope" • "ec2:ipv4pool-ec2" • "ec2:key-pair" • "ec2:launch-template" • "ec2:local-gateway-route-table" • "ec2:local-gateway-route-table-virtual-interface-group"

Tipo di risorsa

- Lista di controllo degli accessi di rete
- Interfaccia di rete
- Ambito di accesso a Network Insights
- Analisi dell'ambito di accesso a Network Insights
- Percorso di analisi

Tipo di risorsa

- "ec2:local-gateway-route-table"
- "ec2:vpc-association"
- "ec2:natgateway"
- "ec2:network-insights-access-scope"
- "ec2:network-insights-analysis"
- "ec2:network-insights-path"

Tipi di risorsa supportati dal servizio

- "ec2:network-insights-access-scope"
- "ec2:network-insights-analysis"
- "ec2:network-insights-path"
- "ec2:placement-group"
- "ec2:prefix-list"
- "ec2:replace-root-volume-task"

Tipo di risorsa

- Sottorete
- Prenotazione CIDR su sottorete
- Filtro di mirroring del traffico
- Sessione di mirroring del traffico
- Destinazione di mirroring del traffico
- Gateway di transito
- Allegato Transit Gateway
- Transit Gateway Connect Peer

Sintassi JSON

- …sk"
- "ec2:reserved-instances"
- "ec2:route-table"
- "ec2:security-group"
- "ec2:snapshot"
- "ec2:spot-fleet-request"
- "ec2:spot-instances-request"
- "ec2:subnet"
- "ec2:subnet-cidr-

Tipi di risorsa supportati dal servizio

- Dominio multicast Transit Gateway
- Tabella delle politiche di Transit Gateway
- Tabella di routing del gateway di transito
- Annuncio della tabella delle rotte del Transit Gateway
- Endpoint di accesso verificato
- Gruppo di

Chiavi di condizione del servizio

- "ec2:transit-gateway"
- "ec2:transit-gateway-multicast-domain"
- "ec2:transit-gateway-policy-table"
- "ec2:transit-gateway-route-table"
- "ec2:transit-gateway-route-table-announcement"
- "ec2:vpc-endpoint-service-verified-access-endpoint"
- "ec2:vpc-endpoint-service-verified-access-group"

Tipi di risorsa

- "ec2:tran sit-gatew ay-connect-peer"
- "ec2:tran sit-gatew ay-multicast-domain"
- "ec2:tran sit-gatew ay-policy-table"
- "ec2:tran sit-gatew ay-route-table"
- "ec2:tran sit-gatew ay-peering"

Tipi di risorsa

- accesso-verificato
- istanza di accesso verificato
- Provider di accesso verificato
- Volume
- Registro di flusso
- VPC
- VPC Endpoint
- VPC Servizio endpoint
- VPC Connessione di peering

Tipi di risorsa supportati dal servizio

- "ec2:route-table"
- "ec2:vpc"
- "ec2:vpn-connection"
- "ec2:vpn-gateway"
- "ec2:verified-access-endpoint"
- "ec2:verified-access-group"
- "ec2:verified-access-instance"
- "ec2:verified-access-trust-provider"
- "ec2:volume"

Tipi di risorsa supportati dal servizio

- "ec2:vpc-flow-log"
- "ec2:vpc"
- "ec2:vpc-endpoint"
- "ec2:vpc-endpoint-service"
- "ec2:vpc-peering-connection"
- "ec2:vpn-connection"
- "ec2:vpn-gateway"
- "rbin:ALL"
- "rbin:RULE"

EC2 Image Builder

- "imagebuilder:*"

Cestino Amazon

- "rbin:rule"

Servizio	Tipi di risorsa	Sintassi JSON
AWS Elastic Beanstalk	• Tutti • Applicazione • Versione dell'applicazione • Modello di configurazione • Piattaforma	• "elasticbeanstalk:ALL_SUPPORTED" • "elasticbeanstalk:application" • "elasticbeanstalk:applicationversion" • "elasticbeanstalk:configurationtemplate" • "elasticbeanstalk:platform"
Amazon Elastic Container Registry	• Tutti • Repository	• ecr:ALL_SUPPORTED • "ecr:repository"

Tipo di risorsa	Tasti supportati	Tipi di servizio supportati
Amazon Elastic Container Service	• Tutti: ALL_SUPPORTED • Fornitore di capacità • Cluster • Servizio • Definizione delle attività • Set di attività • "ecs:cluster" • "ecs:service" • "ecs:task-definition" • "ecs:task-set"	
Amazon Elastic File System	• Tutti: ALL_SUPPORTED • "elasticfilesystem:file-system"	

Servizio	Tipo di risorsa	Sintassi JSON
Amazon Elastic Kubernetes Service	• Tutto • Cluster	• "eks:ALL_SUPPORTED" • "eks:cluster"
Amazon ElasticSearch	• Tutto • Domain	• "es:ALL_SUPPORTED" • "es:domain"
Amazon EMR	• Tutto • Cluster • Editor	• "elasticmapreduce:ALL_SUPPORTED" • "elasticmapreduce:cluster" • "elasticmapreduce:editor"
Amazon EMR Serverless	Applicazioni	"emr-serverless:applications"

Servizio	Tipo di risorsa	Sintassi JSON
AWS Risoluzione dell'entità	• Tutti • Flusso di lavoro corrispondente • Mappatura dello schema	• "entityresolution:ALL_SUPPORTED" • "entityresolution:matchingworkflow" • "entityresolution:schemamapping"
Amazon ElastiCache	• Tutti • Cluster	• "elasticache:ALL_SUPPORTED" • "elasticache:cluster"
Amazon EventBridge	• Tutti • Router di eventi • Regola	• "events:ALL_SUPPORTED" • "events:event-bus" • "events:rule"

Nome servizio	Tipo di risorsa	Sintassi JSON
EventBridge Tubi	• Tutti • Pipeline	• "pipes:ALL_SUPPORTED" • "pipes:pipe"
Amazon EventBridge Scheduler	• Tutto • Gruppo di pianificazione	• "scheduler:ALL_SUPPORTED" • "scheduler:schedule-group"

Tipo di risorsa

Tipi di risorse ARN

Chiavi delle condizioni

Amazon Fraud Detector

- Tabella
- Rilevatore
- Versione del rilevatore
- Modello
- Regola
- Variabile

- "frauddetector:ALL SUPPORTED"
- "frauddetector:detector"
- "frauddetector:detector-version"
- "frauddetector:model"
- "frauddetector:rule"
- "frauddetector:variable"

Amazon Global Accelerator

- Acceleratore

- "globalaccelerator:accelerator"

Servizio	Tipo di risorsa	Sintassi JSON
Sistema di bilanciamento del carico elastico	• Listener • Regola Listener • Sistema di bilanciamento del carico (load balancer) • Gruppo di destinazione	• "elasticloadbalancing:listener" • "elasticloadbalancing:listener-rule" • "elasticloadbalancing:loadbalancer" • "elasticloadbalancing:targetgroup"
Amazon FSx	• Tutto • Backup • File system	• "fsx:ALL_SUPPORTED" • "fsx:backup" • "fsx:file-system"

Tipo di risorsa

Amazon GuardDuty

- "guardduty:detector/*"
- "guardduty:detector/filter"
- "guarddut y:detecto r/ filter"
- Set di IP
- Set di minacce
- "guarddut y:detecto r/ ipset"
- "guarddut y:detecto r/ threati ntelset"

AWS HealthLake

- "healthla ke:datast ore"

Servizio	Tipo di risorsa	Sintassi JSON
AWS HealthOmics	• Tutti • Archivio di annotazioni • Versione dell'archivio di annotazioni • Archivio di riferimenti • Documentazione di riferimento • Esecuzione • Gruppo di esecuzioni • Archivio di sequenze	• "omics:ALL_SUPPORTED" • "omics:annotationStore" • "omics:annotationStore/version" • "omics:referenceStore" • "omics:referenceStore/reference" • "omics:run" • "omics:runGroup" • "omics:sequenceStore" • "omics:sequenceStore/readSet"

Servizio	Tipo di risorsa	Sintassi JSON
	• Set di lettura • Archivio di varianti • Flusso di lavoro	• "omics:variantStore" • "omics:workflow"
Amazon Inspector	• Tutti • Filtro	• "inspector2:ALL_SUPPORTED" • "inspector2:filter"

Tipo di risorsa

- AWS Identity and Access Management
- Profilo dell'istanza
- MFA
- Provider OIDC
- Policy
- Provider SAML
- Certificato del server
- Profilo

Tipi di risorse supportati dal servizio

- "iam:ALL_SUPPORTED"
- "iam:instance-profile"
- "iam:mfa"
- "iam:oidc-provider"
- "iam:policy"
- "iam:saml-provider"
- "iam:server-certificate"

Tipo di risorsa

Tipi di risorsa supportati dal servizio

Chiavi condizione supportate

ARN

- AWS IoT Analytics Canale
- Set di dati
- Datastore
- Pipeline

- "iotanalytics:ALL_SUPPORTED"
- "iotanalytics:channel"
- "iotanalytics:dataset"
- "iotanalytics:datastore"
- "iotanalytics:pipeline"

AWS IoT Events Modello di rilevatore
Input

- "iotevents:ALL_SUPPORTED"
- "iotevents:detectorModel"
- "iotevents:input"

Tipo di risorsa

Tipi di risorsa supportati dal servizio

Chiavi condizione supportate

Esempi ARN

Applicazione Hub

- "iotfleethub:application"

Asset

- "iotsitewise:asset"

Modello di asset

- "iotsitewise:asset-model "

- AWS IoT Fleet Hub: ALL_SUPPORTED"

- AWS IoT SiteWise: ALL_SUPPORTED"

Tipo di risorsa

Tipi di risorsa supportati dal servizio

Chiavi condizione supportate

Operazioni API supportate

- AWS IoT Greengrass V2 Distribuzione
- AWS IoT Greengrass V2 componente
- AWS IoT Greengrass V2 deployment
- Definizione di connettore
- Definizione di core
- Definizione di dispositivo
- Definizione della funzione
- Definizione del logger
- Definizioni risorsa

- "greengrass:ALL_SUPPORTED"
- "greengrass:bulkDeployment"
- "greengrass:connectorDefinition"
- "greengrass:coresDefinition"
- "greengrass:deviceDefinition"
- "greengrass:functionsDefinition"
- "greengrass:loggerDefinition"
- "greengrass:resourceDefinition"
- "greengrass:subscr

Servizio	Tipo di risorsa	Sintassi JSON
	di risorsa • Definizione di sottoscrizione	optionsDefinition"
AWS Key Management Service	• Tutti • Chiave	• "kms:ALL_SUPPORTED" • "kms:key"
Amazon Kinesis	• Tutto • Applicazione	• "kinesisanalytics:ALL_SUPPORTED" • "kinesisanalytics:application"
Amazon Data Firehose	• Tutto • Flusso di consegna	• "firehose:ALL_SUPPORTED" • "firehose:deliverystream"

Servizio	Tipo di risorsa	Sintassi JSON
AWS Lambda	• Tutti • Funzione	• `"lambda:ALL_SUPPORTED"` • `"lambda:function"`
Amazon Macie	• Tutti • Identificatore dati personalizzato	• `"macie2:ALL_SUPPORTED"` • `"macie2:custom-data-identifier"`
Amazon MediaStore	• Tutti • Container	• `"mediastore:ALL_SUPPORTED"` • `"mediastore:container"`

Servizio	Tipo di risorsa	Sintassi JSON
Amazon MQ	• Tutti • Broker • Configurazione	• "mq:ALL_SUPPORTED" • "mq:broker" • "mq:configuration"

Nome servizio	Tipo di risorsa	Sintassi JSON
Amazon Network Firewall	• Tutti • Firewall • Policy firewall • Gruppo di regole stateful • Gruppo di regole stateless	"network-firewall:ALL_SUPPORTED" • "network-firewall:firewall" • "network-firewall:firewall-policy" • "network-firewall:stateful-rulegroup" • "network-firewall:stateless-rulegroup"
Amazon OpenSearch Serverless	• Tutti • Raccolta	"aoss:ALL_SUPPORTED" • "aoss:collection"

Tipo di risorsa

Tipi di risorsa supportati dal servizio

Chiavi condizione supportate

Esempi di sintassi JSON

- AWS Organizations
- Account
- Unità organizzativa
- Policy
- Root

- "organizations:ALL"
- "organizations:SUPPORTED"
- "organizations:account"
- "organizations:ou"
- "organizations:policy"
- "organizations:root"

Tipo di risorsa

Tipi di risorsa supportati dal servizio

Chiavi di condizione supportate dal servizio

Operazioni API supportate

Set di configurazione

Elenco di esclusione

Numero di telefono

Pool

ID mittente

Tutti i tipi di risorsa

Amazon Pinpoint SMS Voice V2

- sms-voice:configuration-set
- sms-voice:opt-out-list
- sms-voice:phone-number
- sms-voice:pool
- sms-voice:sender-id

Tipo di risorsa	Tasti condizione supportati	Tipi di risorsa richiesti
Amazon RDS: cluster (cluster)	aws:ResourceTag/${TagKey}	
Amazon RDS: gruppo di parametri del cluster (cluster-pg)	aws:ResourceTag/${TagKey}	
Amazon RDS: gruppo di opzioni (og)	aws:ResourceTag/${TagKey}	
Amazon RDS: endpoint del cluster (endpoint)	aws:ResourceTag/${TagKey}	
Amazon RDS: gruppo di parametri del database (pg)	aws:ResourceTag/${TagKey}	
Amazon RDS: Proxy DB	aws:ResourceTag/${TagKey}	

Tipo di risorsa

- Endpoint proxy DB
- Istanza database riservata
- Gruppo di sicurezza DB
- DB subnet group (Gruppo di sottoreti DB)
- Gruppo di destinazione

Tipo di risorsa	ARN	Chiavi di condizione
Tutti i servizi	*	
Cluster	arn:aws:redshift:*:*:cluster:*	aws:ResourceTag/${TagKey} redshift:SUPPORTED
Sottoscrizione a eventi	arn:aws:redshift:*:*:cluster:*	
Certificato client HSM	arn:aws:redshift:*:*:hsmclientcertificate:*	
Configurazione HSM	arn:aws:redshift:*:*:hsmconfiguration:*	
Gruppo di parametri	arn:aws:redshift:*:*:parametergroup:*	
Snapshot	arn:aws:redshift:*:*:snapshot:*	
Autorizzazione di copia degli snapshot	arn:aws:redshift:*:*:snapshot:*	
Pianificazione snapshot	arn:aws:redshift:*:*:snapshotschedule:*	
Subnet group	arn:aws:redshift:*:*:subnetgroup:*	
Gruppo di snapshot	arn:aws:redshift:*:*:snapshotcopygrant:*	

Nome servizio	Tipo di risorsa	Sintassi JSON
	sottoreti	ule") • "redshift:subnetgroup"
Amazon Redshift Serverless	• Tutto • Spazio dei nomi • Gruppo di lavoro	• "redshift-serverless:ALL_SUPPORTED" • "redshift-serverless:namespace" • "redshift-serverless:workgroup"
AWS Resource Access Manager	• Tutti • Condivisione delle risorse	• "ram:ALL_SUPPORTED" • "ram:resource-share"

Servizio	Tipo di risorsa	Sintassi JSON
AWS Resource Groups	• Tutti • Group (Gruppo)	• "resource-groups:ALL_SUPPORTED" • "resource-groups:group"
Amazon Route 53	• Tutti • Hosted zone	• "route53:ALL_SUPPORTED" • "route53:hostedzone"
Amazon Route 53 Resolver	• Tutti • Endpoint del risolutore • Regola del risolutore	• "route53resolver:ALL_SUPPORTED" • "route53resolver:resolver-endpoint" • "route53resolver:resolver-rule"

Tipo di risorsa

- Amazon S3 Bucket
- Storage Lens
- Storage Lens group

Tipo di risorsa

- "ALL_S3_SUPPORTED"
- "s3:bucket"
- "s3:storage-lens"
- "s3:storage-lens-group"

Tipo di risorsa	Chiavi di condizione supportate	ARN
Amazon SageMaker AI Config	aws:ResourceTag/${TagKey}	arn:${Partition}:sagemaker:${Region}:${Account}:config/${ConfigName}
Artifact	aws:ResourceTag/${TagKey}	arn:${Partition}:sagemaker:${Region}:${Account}:artifact/${ArtifactId}
Context	aws:ResourceTag/${TagKey}	arn:${Partition}:sagemaker:${Region}:${Account}:context/${ContextId}
Processo di elaborazione	aws:ResourceTag/${TagKey}	arn:${Partition}:sagemaker:${Region}:${Account}:processing-job/${ProcessingJobName}
Gruppo di pacchetti di modelli	aws:ResourceTag/${TagKey}	arn:${Partition}:sagemaker:${Region}:${Account}:model-package-group/${ModelPackageGroupName}
Url delle attività di lavoro	aws:ResourceTag/${TagKey}	arn:${Partition}:sagemaker:${Region}:${Account}:human-task-ui/${HumanTaskUiName}
Immagine	aws:ResourceTag/${TagKey}	arn:${Partition}:sagemaker:${Region}:${Account}:image/${ImageName}
Pacchetto del modello	aws:ResourceTag/${TagKey}	arn:${Partition}:sagemaker:${Region}:${Account}:model-package/${ModelPackageGroupName}/${ModelPackageVersion}
Azione	aws:ResourceTag/${TagKey}	arn:${Partition}:sagemaker:${Region}:${Account}:action/${ActionName}
Pipeline	aws:ResourceTag/${TagKey}	arn:${Partition}:sagemaker:${Region}:${Account}:pipeline/${PipelineName}
Esperimento	aws:ResourceTag/${TagKey}	arn:${Partition}:sagemaker:${Region}:${Account}:experiment/${ExperimentName}

Tipo di risorsa

Definizione di flusso

Progetto

Segreto

- "sagemaker:model-package"
- "sagemaker:action"
- "sagemaker:pipeline"
- "sagemaker:experiment"
- "sagemaker:flow-definition"
- "sagemaker:project"
- "secretsmanager:secret"

Tipo di risorsa	Nome della risorsa Amazon (ARN)	Chiavi di condizione
AWS Lake di sicurezza	• "security lake:ALL_SUPPORTED" • "security lake:data-lake" • "security lake:subscriber"	
AWS Service Catalog	• "servicecatalog:ALL_SUPPORTED" • "servicecatalog:application" • "servicecatalog:attribute-groups " • "servicecatalog:portfolio " • "servicecatalog:product "	

Servizio	Tipo di risorsa	Sintassi JSON
Amazon Simple Notification Service (SNS)	• Tutto • Argomento	• ALL_SUPPORTED • "sns:topic"
Amazon Simple Queue Service (SQS)	• Tutto • Queue	• ALL_SUPPORTED • "sqs:queue"
Amazon States Language	• Tutto • Attività • Macchina a stati	• "states:ALL_SUPPORTED" • "states:activity " • "states:stateMachine "
AWS Step Functions	• Attività	"states:activity"

Servizio	Tipo di risorsa	Sintassi JSON	Note
AWS Storage Gateway	• Gateway • Condivisione • Nastro • Volume	• "storagegateway:gateway" • "storagegateway:share" • "storagegateway:tape" • "storagegateway:gateway/volume"	

Tipo di risorsa

Tipo di servizio

Tipo di risorsa

- AWS Systems Manager
  - Esecuzione di automazione
  - Documento
  - Finestra di manutenzione
  - Istanza gestita
  - Elemento Ops
  - Base di patch
  - Gruppo di patch
  - Contatto

"ssm:ALL_SUPPORTED"

"ssm:association"

"ssm:automation-execution"

"ssm:document"

"ssm:maintenancewindow"

"ssm:managed-instance"

"ssmcontacts:contact"

Tipi di risorsa	Chiavi condizione supportate	Tipi di risorsa dipendenti
Amazon Textract Adattatore (textract:adapters)	Tutti i servizi: TAGGING_SUPPORTED textract:AdapterId textract:AdapterVersion	
AWS Transfer Family Server (transfer:server) Utente (transfer:user) Flusso di lavoro (transfer:workflow)	Tutti i servizi: TAGGING_SUPPORTED transfer:ServerProtocols transfer:UserName	
Amazon Well-Architected Carico di lavoro (wellarchitected:workload)	Tutti i servizi: TAGGING_SUPPORTED	

Nome servizio	Tipo di risorsa	Sintassi JSON
AWS Wickr	• Tutti • Rete	• "wickr:ALL_SUPPORTED" • "wickr:network"
Amazon WorkSpaces	• Tutti • Alias di connessione • Directory • WorkSpace • WorkSpaces pacchetto • WorkSpaces immagine • WorkSpaces gruppo IP	• "workspaces:ALL_SUPPORTED" • "workspaces:connectionalias" • "workspaces:directory" • "workspaces:workspace" • "workspaces:workspacebundle" • "workspaces:workspaceimage" • "workspaces:workspaceipgroup"

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",
                    "300*"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "secretsmanager:ALL_SUPPORTED"
                ]
            }
        }
    }
}
```

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. Il valore della policy distingue 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 del `CostCenter` tag sono `100200`, `e300*`.

- (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 politica dei tag di esempio specifica che il `CostCenter` tag passato a tutte le AWS Secrets Manager risorse deve essere conforme a questa politica.

  > **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, vedi Operatori di ereditarietà.

- È possibile utilizzare il carattere * jolly nei valori dei tag.
  - Puoi utilizzare solo un carattere jolly per ogni valore di tag. Ad esempio, `*@example.com` è consentito, mentre non lo è `*@*.com`.
  - È possibile utilizzare il carattere `ALL_SUPPORTED` jolly sul `enforced_for` campo con alcuni servizi per abilitare l'applicazione di tutte le risorse relative a quel 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 politica di tag simile per le chiavi dei tag che si desidera 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 politiche, inclusi esempi di come funzionano gli operatori di ereditarietà ed esempi di politiche di tag efficaci, vedere. 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"
                ]
            }
        }
    }
}
```

Esempio 3: Specificare una politica di tag per tutti i tipi di risorse supportati di un servizio specifico AWS

Per specificare una politica di tag per tutti i tipi di risorse supportati di un AWS servizio specifico, si utilizza il carattere `ALL_SUPPORTED` jolly.

Questa policy utilizza il carattere `ALL_SUPPORTED` jolly per specificare che tutte le EC2 istanze Amazon con la chiave tag `Environment` possono avere solo un valore di `Prod` tag pari o. `Non-prod` Questa jolly offre un'alternativa efficace a riga singola alla pubblicazione di ciascuna EC2 istanza Amazon singolarmente. Per un elenco di servizi e tipi di risorse che supportano i caratteri `ALL_SUPPORTED` jolly, consulta. Servizi e tipi di risorse che supportano l'applicazione

```
{
    "tags": {
        "Environment": {
            "tag_key": {
                "@@assign": "Environment",
                "@@operators_allowed_for_child_policies": ["@@none"]
            },
            "tag_value": {
                "@@assign": [
                    "Prod",
                    "Non-prod"
                ],
                "@@operators_allowed_for_child_policies": ["@@none"]
            },
            "enforced_for": {
                "@@assign": [
                    "ec2:ALL_SUPPORTED"
                ]
            }
        }
    }
}
```

Regioni supportate

Le caratteristiche delle policy di tag sono disponibili nelle seguenti regioni:

Nome della 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
Regione Asia Pacifico (Malesia)	ap-southeast-5
Asia Pacifico (Melbourne) [2]	ap-southeast-4
Asia Pacifico (Tailandia)	ap-southeast-7
Regione Canada (Centrale)	ca-central-1

Nome della Regione	Parametro della regione
Canada occidentale (Calgary) [2]	`ca-west-1`
Regione Cina (Pechino)	`cn-north-1`
Regione Cina (Ningxia)	`cn-northwest-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 Messico (Centrale)	`mx-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`
AWS GovCloud Regione (Stati Uniti orientali)	`us-gov-east-1`
AWS GovCloud Regione (Stati Uniti occidentali)	`us-gov-west-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
- 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.

Politiche relative alle applicazioni di chat

Le politiche delle applicazioni di chat ti AWS Organizations consentono di controllare l'accesso agli account della tua organizzazione da applicazioni di chat come Slack e Microsoft Teams.

Amazon Q Developer nelle applicazioni di chat è un AWS servizio che consente ai DevOps team di sviluppo software di utilizzare le chat room dei programmi di messaggistica per monitorare e rispondere agli eventi operativi nei propri ambienti Cloud AWS. Amazon Q Developer nelle applicazioni di chat elabora Servizio AWS le notifiche da Amazon Simple Notification Service (Amazon SNS) e le inoltra alle chat room in modo che i team possano analizzarle e agire di conseguenza immediatamente, indipendentemente dalla posizione.

Come funzionano le politiche delle applicazioni di chat

Utilizzando le politiche delle applicazioni di chat, l'account di gestione o l'amministratore delegato di un'organizzazione può eseguire le seguenti operazioni all'interno dell'organizzazione:

- Imponi quali applicazioni di chat supportate (Amazon Chime, Microsoft Teams e Slack) possono essere utilizzate.
- Limita l'accesso del client di chat a specifici spazi di lavoro (Slack) e team (Microsoft Teams).
- Limita la visibilità del canale Slack ai canali pubblici o privati.
- Imposta e applica impostazioni di ruolo specifiche.

Le politiche delle applicazioni di chat limitano e hanno la precedenza sulle impostazioni a livello di account, come le impostazioni dei ruoli e le politiche del guardrail del canale. Puoi accedere e modificare le policy delle applicazioni di chat da Amazon Q Developer nelle applicazioni di chat o dalla console Organizations.

Una volta allegate le policy agli account e alle unità organizzative (OU), tutte le configurazioni attuali e future di applicazioni Amazon Q Developer in chat per gli account interessati rispetteranno automaticamente le impostazioni di governance e autorizzazioni. Per ulteriori informazioni, consulta Comprendere l'ereditarietà delle politiche di gestione.

Se tenti di eseguire un'azione limitata da una politica delle applicazioni di chat, un messaggio di errore ti informerà che l'azione non è consentita a causa della politica delle applicazioni di chat con la raccomandazione di contattare l'account di gestione o l'amministratore delegato dell'organizzazione.

> **Note**
>
> Le politiche delle applicazioni di chat vengono convalidate in fase di esecuzione. Ciò significa che le risorse esistenti vengono continuamente controllate per verificarne la conformità. Non vi è alcuna sovrapposizione con le autorizzazioni IAM esistenti poiché le autorizzazioni IAM basate su runtime per l'invio di notifiche o l'interazione con Amazon Q Developer nelle applicazioni di chat non sono attualmente supportate.

Guida introduttiva alle politiche delle applicazioni di chat

Segui questi passaggi per iniziare a utilizzare le politiche delle applicazioni di chat.

1. Scopri le autorizzazioni necessarie per eseguire le attività relative alle politiche delle applicazioni di chat.
2. Abilita le politiche delle applicazioni di chat per la tua organizzazione.
3. Crea una politica per le applicazioni di chat.
4. Allega la policy relativa alle applicazioni di chat alla directory principale, all'unità organizzativa o all'account della tua organizzazione.
5. Visualizza la politica combinata sulle applicazioni di chat efficaci che si applica 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

- Scopri la sintassi delle politiche delle applicazioni di chat e guarda esempi di politiche

Sintassi ed esempi delle policy delle applicazioni di chat

Questo argomento descrive la sintassi delle politiche delle applicazioni di chat e fornisce esempi.

Sintassi per le politiche delle applicazioni di chat

Una policy per le applicazioni di chat è un file di testo semplice strutturato secondo le regole di JSON. La sintassi per le politiche delle applicazioni di chat segue la sintassi per i tipi di policy di gestione. Per una discussione completa di tale sintassi, consulta Comprendere l'ereditarietà delle policy di gestione. Questo argomento si concentra sull'applicazione di tale sintassi generale ai requisiti specifici del tipo di policy delle applicazioni di chat.

L'esempio seguente mostra la sintassi di base per una politica delle applicazioni di chat:

```
{
    "chatbot":{
       "platforms":{
          "slack":{
             "client":{
                "@@assign":"enabled" // enabled | disabled
             },
             "workspaces": { // limit 255
                   "@@assign":[
                      "Slack-Workspace-Id"
```

```
            ]
         },
         "default":{
            "supported_channel_types":{
               "@@assign":[
                  "private" // public | private
               ]
            },
            "supported_role_settings":{
               "@@assign":[
                  "user_role" // user_role | channel_role
               ]
            }
         },
         "overrides":{ // limit 255
            "Slack-Workspace-Id":{
               "supported_channel_types":{
                  "@@assign":[
                     "public" // public | private
                  ]
               },
               "supported_role_settings":{
                  "@@assign":[
                     "user_role" // user_role | channel_role
                  ]
               }
            }
         }
      },
      "microsoft_teams":{
         "client":{
            "@@assign":"enabled"
         },
         "tenants":{ // limit 36
            "Microsoft-Teams-Tenant-Id":{ // limit 36
               "@@assign":[
                  "Microsoft-Teams-Team-Id"
               ]
            }
         },
         "default":{
            "supported_role_settings":{
               "@@assign":[
                  "user_role" // user_role | channel_role
```

```
                ]
             }
          },
          "overrides":{ // limit 36
             "Microsoft-Teams-Tenant-Id":{ // limit 36
                "Microsoft-Teams-Team-Id":{
                   "supported_role_settings":{
                      "@@assign":[
                         "user_role" // user_role | channel_role
                      ]
                   }
                }
             }
          }
       },
       "chime":{
         "client":{
            "@@assign":"disabled" // enabled | disabled
         }
       }
    },
    "default":{
       "client":{
          "@@assign":"disabled" // enabled | disabled
       }
    }
 }
}
```

Questa politica per le applicazioni di chat include i seguenti elementi:

- Il nome della chiave di campo `chatbot`. Le politiche delle applicazioni di chat iniziano sempre con questo nome a chiave fissa. È la riga principale di questo esempio di policy.
- Sotto `chatbot` c'è un `platforms` blocco che contiene la configurazione per le diverse applicazioni di chat supportate: Slack, Microsoft Teams e Amazon Chime.
  - Per Slack, sono disponibili i seguenti campi:
    - `"client"`:
      - `"enabled"`: Il client Slack è abilitato. Le integrazioni con Slack sono consentite.
      - `"disabled"`: Il client Slack è disabilitato. Le integrazioni con Slack non sono consentite.

- `"workspaces"`: elenco separato da virgole degli spazi di lavoro Slack consentiti. In questo esempio, gli spazi di lavoro Slack consentiti sono e. *`Slack-Workspace-Id1`* *`Slack-Workspace-Id2`*
- `"default"`: Le impostazioni predefinite per le aree di lavoro Slack.
  - `"supported_channel_types"`:
    - `"public"`: Le aree di lavoro Slack incluse nell'ambito consentono i canali Slack pubblici per impostazione predefinita.
    - `"private"`: Le aree di lavoro Slack incluse nell'ambito consentono i canali Slack privati per impostazione predefinita.
  - `supported_role_settings`:
    - `"user_role"`: Gli spazi di lavoro Slack inclusi nell'ambito consentono i ruoli IAM a livello di utente per impostazione predefinita.
    - `"channel_role"`: Gli spazi di lavoro Slack inclusi nell'ambito consentono i ruoli IAM a livello di canale per impostazione predefinita.
- `"overrides"`: Le impostazioni di override per gli spazi di lavoro Slack.
  - *`Slack-Workspace-Id2`*: elenco separato da virgole delle aree di lavoro Slack a cui si applica l'impostazione di override. In questo esempio, l'area di lavoro di Slack è. *`Slack-Workspace-Id2`*
    - `"supported_channel_types"`:
      - `"public"`: Sostituisci l'impostazione se le aree di lavoro Slack incluse nell'ambito consentono i canali Slack pubblici.
      - `"private"`: Sostituisci l'impostazione se le aree di lavoro Slack nell'ambito consentono i canali Slack privati.
    - `supported_role_settings`:
      - `"user_role"`: Sostituisci l'impostazione se le aree di lavoro Slack nell'ambito consentono i ruoli IAM a livello di utente.
      - `"channel_role"`: Sostituisci l'impostazione se le aree di lavoro Slack nell'ambito consentono i ruoli IAM a livello di canale.
- Per Microsoft Teams, sono disponibili i seguenti campi:
  - `"client"`:
    - `"enabled"`: il client Microsoft Teams è abilitato. Le integrazioni con Microsoft Teams sono consentite.

    - `"disabled"`: il client Microsoft Teams è disabilitato. Le integrazioni con Microsoft Teams non sono consentite.
  - `"tenants"`: elenco separato da virgole dei tenant di Microsoft Teams consentiti. In questo esempio, il tenant consentito è. *`Microsoft-Teams-Tenant-Id`*
    - *`Microsoft-Teams-Tenant-Id`*: elenco separato da virgole dei team consentiti all'interno del tenant. In questo esempio, il team consentito è. *`Microsoft-Teams-Team-Id`*
  - `"default"`: Le impostazioni predefinite per i team all'interno del tenant.
    - `supported_role_settings`:
      - `"user_role"`: I team inclusi nell'ambito consentono i ruoli IAM a livello di utente per impostazione predefinita.
      - `"channel_role"`: I team inclusi nell'ambito consentono i ruoli IAM a livello di canale per impostazione predefinita.
  - `"overrides"`: le impostazioni di override per i tenant di Microsoft Teams.
    - *`Microsoft-Teams-Tenant-Id`*: elenco separato da virgole dei tenant a cui si applica l'impostazione di esclusione. In questo esempio, il tenant è. *`Microsoft-Teams-Tenant-Id`*
      - *`Microsoft-Teams-Team-Id`*: elenco separato da virgole dei team all'interno del tenant. In questo esempio, il team consentito è. *`Microsoft-Teams-Team-Id`*
        - `supported_role_settings`:
          - `"user_role"`: Sostituisci l'impostazione se i team inclusi nell'ambito consentono i ruoli IAM a livello di utente.
          - `"channel_role"`: sostituisci l'impostazione se i team inclusi nell'ambito consentono i ruoli IAM a livello di canale.
- Per Amazon Chime, sono disponibili i seguenti campi:
  - `"client"`:
    - `"enabled"`: il client Amazon Chime è abilitato. Le integrazioni con Amazon Chime sono consentite.
    - `"disabled"`: il client Amazon Chime è disabilitato. Le integrazioni con Amazon Chime non sono consentite.
- Sotto`chatbot`, c'è un `default` blocco che disabilita Amazon Q Developer nelle applicazioni di chat di tutta l'organizzazione, a meno che non venga sovrascritto a un livello inferiore. Questa impostazione predefinita disabilita anche qualsiasi nuova applicazione di chat supportata da Amazon Q Developer nelle applicazioni di chat. Ad esempio, se Amazon Q Developer nelle

applicazioni di chat supporta una nuova applicazione di chat, questa impostazione predefinita disabilita anche quella nuova applicazione di chat supportata.

> **Note**
>
> Per ulteriori informazioni sui ruoli IAM a livello di canale e sui ruoli IAM a livello di utente, consulta Understanding Amazon Q Developer in chat applications permissions nella Amazon Q Developer in chat applications Administrator Guide.

Esempi di policy per le applicazioni di chat

Le policy di esempio che seguono sono solo a scopo informativo.

Esempio 1: consenti solo i canali Slack privati in uno spazio di lavoro specifico, disabilita Microsoft Teams, sono supportate tutte le modalità di autenticazione

La seguente politica si concentra sul controllo delle configurazioni consentite per le integrazioni di chatbot di Slack e Microsoft Teams.

```
{
   "chatbot": {
      "platforms": {
         "slack": {
            "client": {
               "@@assign": "enabled"
            },
            "workspaces": {
               "@@assign": [
                  "Slack-Workspace-Id"
               ]
            },
            "default": {
               "supported_channel_types": {
                  "@@assign": [
                     "private"
                  ]
               },
               "supported_role_settings": {
                  "@@assign": [
                     "channel_role",
```

```
                    "user_role"
                ]
             }
          }
       },
       "microsoft_teams": {
          "client": {
             "@@assign": "disabled"
          }
       },
       "chime":{
          "client":{
             "@@assign":"disabled"
          }
       },
       "default":{
          "client":{
             "@@assign":"disabled"
          }
       }
    }
 }
}
```

Per Slack

- Il client Slack è abilitato.
- È consentito solo lo spazio di lavoro *`Slack-Workspace-Id`* Slack specifico.
- Le impostazioni predefinite consentono solo i canali Slack privati, i ruoli IAM a livello di canale e i ruoli IAM a livello di utente.

Per Microsoft Team

- Il client Microsoft Teams è disabilitato.

Per Amazon Chime

- Il client Amazon Chime è disabilitato.

Dettagli aggiuntivi

- Il `default` blocco in basso imposta la disattivazione del client, che disattiva Amazon Q Developer nelle applicazioni di chat in tutta l'organizzazione a meno che non venga sovrascritto a un livello inferiore. Questa impostazione predefinita disabilita anche qualsiasi nuova applicazione di chat supportata da Amazon Q Developer nelle applicazioni di chat. Ad esempio, se Amazon Q Developer nelle applicazioni di chat supporta una nuova applicazione di chat, questa impostazione predefinita disabilita anche quella nuova applicazione di chat supportata.

Esempio 2: consenti solo le integrazioni di Slack con ruoli IAM a livello di utente

La seguente policy adotta un approccio più permissivo a Slack, consentendo tutte le aree di lavoro Slack ma limitando la modalità di autenticazione ai soli ruoli IAM a livello di utente.

```
{
   "chatbot":{
      "platforms":{
         "slack":{
            "client":{
               "@@assign":"enabled"
            },
            "workspaces":
               {
                  "@@assign":[
                     "*"
                  ]
               },
            "default":{
               "supported_role_settings":{
                  "@@assign":[
                     "user_role"
                  ]
               }
            }
         },
         "microsoft_teams":{
            "client":{
               "@@assign":"disabled"
            }
         },
         "chime":{
            "client":{
               "@@assign":"disabled"
            }
```

```
         }
      },
      "default":{
         "client":{
            "@@assign":"disabled"
         }
      }
   }
}
```

Per Slack

- Il client Slack è abilitato.
- Non vengono definiti spazi di lavoro Slack specifici utilizzando il carattere jolly`"*"`, quindi tutti gli spazi di lavoro sono consentiti.
- Le impostazioni predefinite consentono solo i ruoli IAM a livello di utente.

Per Microsoft Team

- Il client Microsoft Teams è disabilitato.

Per Amazon Chime

- Il client Amazon Chime è disabilitato.

Dettagli aggiuntivi

- Il `default` blocco in basso imposta la disattivazione del client, che disattiva Amazon Q Developer nelle applicazioni di chat in tutta l'organizzazione a meno che non venga sovrascritto a un livello inferiore. Questa impostazione predefinita disabilita anche qualsiasi nuova applicazione di chat supportata da Amazon Q Developer nelle applicazioni di chat. Ad esempio, se Amazon Q Developer nelle applicazioni di chat supporta una nuova applicazione di chat, questa impostazione predefinita disabilita anche quella nuova applicazione di chat supportata.

Esempio 3: consenti solo le integrazioni di Microsoft Teams in uno specifico Tenant

La politica di esempio seguente blocca l'organizzazione per consentire solo le integrazioni di chatbot di Microsoft Teams all'interno del tenant specificato, bloccando completamente le integrazioni di Slack.

```
{
   "chatbot":{
      "platforms":{
         "slack":{
            "client": {
               "@@assign": "disabled"
            },
         },
         "microsoft_teams":{
            "client": {
               "@@assign": "enabled"
            },
            "tenants":{
               "Microsoft-Teams-Tenant-Id":{
                  "@@assign":[
                     "*"
                  ]
               }
            }
         },
         "chime": {
            "client":{
               "@@assign": "disabled"
            }
         }
      }
   }
}
```

Per Slack

- Il client Slack è disabilitato.

Per Microsoft Team

- *Microsoft-Teams-Tenant-Id*È consentito solo il tenant specifico, utilizzando la jolly "*" per consentire l'accesso a tutti i team all'interno di quel tenant.

Per Amazon Chime

- Il client Amazon Chime è disabilitato.

Dettagli aggiuntivi

- Il `default` blocco in basso imposta la disattivazione del client, che disattiva Amazon Q Developer nelle applicazioni di chat in tutta l'organizzazione a meno che non venga sovrascritto a un livello inferiore. Questa impostazione predefinita disabilita anche qualsiasi nuova applicazione di chat supportata da Amazon Q Developer nelle applicazioni di chat. Ad esempio, se Amazon Q Developer nelle applicazioni di chat supporta una nuova applicazione di chat, questa impostazione predefinita disabilita anche quella nuova applicazione di chat supportata.

Esempio 4: consente l'accesso limitato ad Amazon Q Developer nelle applicazioni di chat per le aree di lavoro Slack e un tenant di Microsoft Teams

La seguente politica consente l'accesso limitato ad Amazon Q Developer nelle applicazioni di chat per aree di lavoro Slack selezionate e un tenant Microsoft Teams.

```
{
    "chatbot":{
       "platforms":{
          "slack":{
             "client":{
                "@@assign":"enabled"
             },
             "workspaces": {
                   "@@assign":[
                      "Slack-Workspace-Id1",
                      "Slack-Workspace-Id2"
                   ]
             },
             "default":{
                "supported_channel_types":{
                   "@@assign":[
                      "private"
                   ]
```

```
            },
            "supported_role_settings":{
               "@@assign":[
                  "user_role"
               ]
            }
         },
         "overrides":{
            "Slack-Workspace-Id2":{
               "supported_channel_types":{
                  "@@assign":[
                     "public",
                     "private"
                  ]
               },
               "supported_role_settings":{
                  "@@assign":[
                     "channel_role",
                     "user_role"
                  ]
               }
            }
         }
      },
      "microsoft_teams":{
         "client":{
            "@@assign":"enabled"
         },
         "tenants":{
            "Microsoft-Teams-Tenant-Id":{
               "@@assign":[
                  "Microsoft-Teams-Team-Id"
               ]
            }
         },
         "default":{
            "supported_role_settings":{
               "@@assign":[
                  "user_role"
               ]
            }
         },
         "overrides":{
            "Microsoft-Teams-Tenant-Id":{
```

```
                  "Microsoft-Teams-Team-Id":{
                     "supported_role_settings":{
                        "@@assign":[
                           "channel_role",
                           "user_role"
                        ]
                     }
                  }
               }
            }
         }
      },
      "default":{
         "client":{
            "@@assign":"disabled"
         }
      }
   }
}
```

Per Slack

- Il client Slack è abilitato.
- Le aree di lavoro Slack consentite sono e. *Slack-Workspace-Id1* *Slack-Workspace-Id2*
- Le impostazioni predefinite per Slack consentono solo i canali privati e i ruoli IAM a livello di utente.
- Esiste un'eccezione per l'area di lavoro *Slack-Workspace-Id2* che consente sia i canali pubblici che quelli privati, nonché i ruoli IAM a livello di canale e i ruoli IAM a livello di utente.

Per Microsoft Team

- Microsoft Teams è abilitato.
- Gli inquilini autorizzati di Teams fanno *Microsoft-Teams-Tenant-Id* parte del team*Microsoft-Teams-Team-Id*.
- Le impostazioni predefinite consentono solo i ruoli IAM a livello di utente.
- Esiste un'eccezione per il tenant *Microsoft-Teams-Tenant-Id* che consente sia i ruoli IAM a livello di canale che i ruoli IAM a livello di utente per il team. *Microsoft-Teams-Team-Id*

Dettagli aggiuntivi

- Il `default` blocco in basso imposta la disattivazione del client, che disattiva Amazon Q Developer nelle applicazioni di chat in tutta l'organizzazione a meno che non venga sovrascritto a un livello inferiore. Ciò significa che Amazon Chime è disabilitato in questo esempio. Questa impostazione predefinita disabilita anche qualsiasi nuova applicazione di chat supportata da Amazon Q Developer nelle applicazioni di chat. Ad esempio, se Amazon Q Developer nelle applicazioni di chat supporta una nuova applicazione di chat, questa impostazione predefinita disabilita anche quella nuova applicazione di chat supportata.

Policy di rifiuto dei servizi di IA

AWS I servizi di intelligenza artificiale possono utilizzare e archiviare i contenuti dei clienti per il miglioramento del servizio, ad esempio la risoluzione di problemi operativi, la valutazione delle prestazioni del servizio, il debug o la formazione dei modelli. A tal fine, potremmo archiviare tali contenuti Regione AWS all'esterno del luogo in Regione AWS cui l'utente utilizza il servizio. Puoi rinunciare all'uso dei tuoi contenuti per migliorare il servizio utilizzando la politica di AWS Organizations opt-out.

Puoi creare politiche di opt-out per un singolo servizio di intelligenza artificiale o per tutti i servizi supportati dalle politiche di opt-out dei servizi di intelligenza artificiale. Puoi anche interrogare la politica efficace applicabile a ciascun account per vedere gli effetti delle tue scelte di impostazione.

Per informazioni più dettagliate, consulta AWS Machine Learning and Artificial Intelligence Services nei Termini AWS di servizio. Per un elenco dei servizi supportati dalle politiche di disattivazione dei servizi di intelligenza artificiale, consulta Elenco dei servizi di intelligenza artificiale supportati.

Argomenti

- Considerazioni sull'utilizzo delle politiche di opt-out dei servizi AI
- Guida introduttiva alle policy di rifiuto dei servizi di IA
- Disattiva tutti i servizi di AWS intelligenza artificiale supportati
- Sintassi ed esempi di policy di rifiuto dei servizi di IA

Considerazioni sull'utilizzo delle politiche di opt-out dei servizi AI

La disattivazione comporta l'eliminazione di tutti i contenuti storici associati

Quando si disattiva l'uso dei contenuti da parte di un servizio di AWS intelligenza artificiale, tale servizio elimina tutti i contenuti storici associati con cui è stato condiviso AWS prima

dell'impostazione dell'opzione. Questa eliminazione è limitata ai contenuti archiviati che non sono necessari per fornire le funzioni del servizio.

Ad esempio, quando si utilizza un servizio mentre si è attivati, tale servizio potrebbe archiviare copie dei contenuti per migliorare il servizio. Quando si effettua l'opt-out, tutte le copie archiviate dal servizio a tale scopo vengono eliminate, ma i contenuti utilizzati per fornire il servizio all'utente non vengono eliminati.

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. Ulteriori informazioni sulle autorizzazioni necessarie per eseguire attività delle policy di backup
2. Abilita le policy di rifiuto dei servizi di IA per l'organizzazione.
3. Crea una policy di rifiuto dei servizi di IA.
4. Collega la policy di rifiuto dei servizi di IA al root, all'unità organizzativa o all'account dell'organizzazione.
5. Visualizza la policy di rifiuto dei servizi di IA effettiva combinata applicabile a un account.

Per tutti questi passaggi, accedi come utente AWS Identity and Access Management (IAM), assumi un ruolo IAM o accedi come utente root (non consigliato) 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

Disattiva tutti i servizi di AWS intelligenza artificiale supportati

In questo argomento:

- Puoi disattivarlo selezionando un solo pulsante nella AWS Organizations console.
- Puoi annullare l'iscrizione allegando la politica di esempio fornita utilizzando il pulsante AWS CLI & AWS SDKs.
- Puoi visualizzare un elenco di quelle Servizi AWS supportate dalla politica di opt-out dei servizi AI.

Disattiva tutti i servizi di intelligenza artificiale supportati

Puoi impedire alla tua organizzazione di utilizzare i propri contenuti per il miglioramento del servizio creando e allegando una politica di disattivazione dei servizi di intelligenza artificiale. Questa politica si applica a tutti i servizi di AWS intelligenza artificiale supportati attuali e futuri. Gli account dei membri non possono aggiornare la politica.

AWS Management Console

Per disattivare tutti i servizi di intelligenza artificiale

1. Accedi alla AWS Organizations console . 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 delle politiche di disattivazione dei servizi AI, scegli Disattiva tutti i servizi.
3. Nella pagina di conferma dell'esclusione da tutti i servizi, scegli Rinuncia a tutti i servizi.

AWS CLI & AWS SDKs

Per disattivare tutti i servizi di intelligenza artificiale

1. Copia «Esempio 1: disattivazione di tutti i servizi di intelligenza artificiale per tutti gli account dell'organizzazione» negli esempi di disattivazione dei servizi di intelligenza artificiale.
2. Segui le istruzioni riportate in Allegare e scollegare i servizi di intelligenza artificiale (opt-out).

> **Note**
>
> Sono necessari passaggi aggiuntivi per disattivare Amazon Monitron. Per ulteriori informazioni, consultare Termini del servizio AWS.

Elenco dei servizi supportati dalla politica di esclusione dei servizi AI

Di seguito è riportato un elenco dei servizi Servizi AWS supportati dalla politica di opt-out dei servizi AI:

- Operazioni Amazon AI
- Analisi vocale dell'SDK Amazon Chime

- Amazon CloudWatch
- Amazon CodeGuru Profiler
- Amazon CodeWhisperer (ora parte di Amazon Q Developer)
- Amazon Comprehend
- Amazon Connect
- Ottimizzazione di Amazon Connect
- Lenti a contatto Amazon Connect
- AWS Servizio di migrazione del Database
- Amazon DataZone
- AWS Entity Resolution
- Amazon Fraud Detector
- AWS Glue
- Amazon GuardDuty
- Amazon Lex
- Amazon Polly
- Amazon Q
- Amazon QuickSight
- Amazon Rekognition
- Amazon Security Lake
- Catena di approvvigionamento di AWS
- Amazon Textract
- Amazon Transcribe
- Amazon Translate

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 allegare politiche per bambini a OUs o direttamente agli account per sostituire questa impostazione per qualsiasi servizio di intelligenza artificiale 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 AWS servizio di intelligenza artificiale. 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.
    - `aiops`
    - `awssupplychain`
    - `chimesdkvoiceanalytics`
    - `cloudwatch`

- codeguruprofiler
- codewhisperer
- comprehend
- connectamd
- connectoptimization
- contactlens
- datazone
- dms
- entityresolution
- frauddetector
- glue
- 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 politica efficace che ne risulta Account AWS è che l'account opti solo per Amazon Lex e rinunci a tutti gli altri servizi di AWS intelligenza artificiale a causa dell'impostazione di `default` opt-out ereditata dalla politica principale.

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 coperti da questa politica, ma potrebbero essere influenzati dalle politiche relative ai minori in altri account. OUs

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

Politiche del Security Hub

AWS Security Hub le politiche forniscono ai team addetti alla sicurezza un approccio centralizzato alla gestione delle configurazioni di sicurezza in tutti i loro ambienti. AWS Organizations Sfruttando queste politiche, è possibile stabilire e mantenere controlli di sicurezza coerenti attraverso un meccanismo di configurazione centrale. Questa integrazione consente di colmare le lacune nella copertura di sicurezza creando politiche in linea con i requisiti di sicurezza dell'organizzazione e applicandole centralmente a tutti gli account e le unità organizzative (). OUs

Le policy di Security Hub sono completamente integrate e consentono agli account di gestione o agli amministratori delegati di definire e applicare le configurazioni di sicurezza. AWS Organizations Quando gli account entrano a far parte dell'organizzazione, ereditano automaticamente le politiche applicabili in base alla loro posizione nella gerarchia organizzativa. Ciò garantisce che gli standard di sicurezza vengano applicati in modo coerente man mano che l'organizzazione cresce. Le politiche rispettano le strutture organizzative esistenti e offrono flessibilità nel modo in cui le configurazioni di

sicurezza vengono distribuite, pur mantenendo il controllo centrale sulle impostazioni di sicurezza critiche.

Caratteristiche e vantaggi principali

Le policy di Security Hub forniscono un set completo di funzionalità che aiutano a gestire e applicare le configurazioni di sicurezza in tutta l'organizzazione AWS . Queste funzionalità semplificano la gestione della sicurezza garantendo al contempo un controllo costante sull'ambiente multi-account.

- Attiva centralmente Security Hub su tutti gli account e le regioni della tua organizzazione
- Crea politiche di sicurezza che definiscano la configurazione di sicurezza tra account e OUs
- Applica automaticamente le configurazioni di sicurezza ai nuovi account quando entrano a far parte della tua organizzazione
- Garantisci impostazioni di sicurezza coerenti in tutta l'organizzazione
- Impedisci agli account dei membri di modificare le configurazioni di sicurezza a livello di organizzazione

Cosa sono le politiche del Security Hub?

Le policy di Security Hub sono AWS Organizations policy che forniscono il controllo centralizzato sulle configurazioni di sicurezza tra gli account dell'organizzazione. Queste policy si integrano perfettamente AWS Organizations per aiutarti a stabilire e mantenere standard di sicurezza coerenti in tutto l'ambiente con più account.

Quando si implementano le policy di Security Hub, si ottiene la possibilità di definire configurazioni di sicurezza specifiche che si propagano automaticamente all'interno dell'organizzazione. Ciò garantisce che tutti gli account, compresi quelli appena creati, siano in linea con i requisiti di sicurezza e le migliori pratiche dell'organizzazione.

Queste politiche aiutano anche a mantenere la conformità applicando controlli di sicurezza coerenti e impedendo ai singoli account di modificare le impostazioni di sicurezza a livello di organizzazione. Questo approccio centralizzato riduce in modo significativo il sovraccarico amministrativo legato alla gestione delle configurazioni di sicurezza in ambienti complessi e di grandi dimensioni. AWS

Come funzionano le policy di Security Hub

Quando alleghi una policy di Security Hub alla tua organizzazione o unità organizzativa, valuta AWS Organizations automaticamente la policy e la applica in base all'ambito definito. Il processo di applicazione delle policy segue regole specifiche per la risoluzione dei conflitti:

Quando le regioni compaiono sia negli elenchi di attivazione che in quelli di disabilitazione, la configurazione di disabilitazione ha la precedenza. Ad esempio, se una regione è elencata sia nelle configurazioni di attivazione che di disabilitazione, Security Hub verrà disabilitato in quella regione.

Quando `ALL_SUPPORTED` viene specificata l'abilitazione, Security Hub è abilitato in tutte le regioni attuali e future a meno che non sia disabilitato esplicitamente. Ciò consente di mantenere una copertura di sicurezza completa man mano che AWS si espande in nuove regioni.

Le politiche per i figli possono modificare le impostazioni delle politiche principali utilizzando operatori di ereditarietà, consentendo un controllo granulare a diversi livelli organizzativi. Questo approccio gerarchico garantisce che unità organizzative specifiche possano personalizzare le proprie impostazioni di sicurezza mantenendo i controlli di base.

Terminologia

In questo argomento vengono utilizzati i seguenti termini per discutere delle politiche di Security Hub.

Terminologia delle policy di Security Hub

Termine	Definizione
Policy operativa	La politica finale che si applica a un account dopo aver combinato tutte le politiche ereditate.
Ereditarietà delle policy	Processo mediante il quale gli account ereditano le politiche dalle unità organizzative principali.
Amministratore delegato	Un account designato per gestire le politiche del Security Hub per conto dell'organizzazione.
Ruolo collegato al servizio	Un ruolo IAM che consente a Security Hub di interagire con altri AWS servizi.

Casi d'uso per le policy di Security Hub

Le policy di Security Hub risolvono le sfide più comuni di gestione della sicurezza in ambienti con più account. I seguenti casi d'uso dimostrano come le organizzazioni in genere implementano queste politiche per migliorare il proprio livello di sicurezza.

Caso d'uso di esempio: requisiti di conformità regionali

Una multinazionale necessita di diverse configurazioni di Security Hub per diverse aree geografiche. Creano una politica principale che abilita Security Hub in tutte le regioni utilizzando`ALL_SUPPORTED`, quindi utilizzano politiche secondarie per disabilitare aree specifiche in cui sono richiesti controlli di sicurezza diversi. Ciò consente loro di mantenere la conformità alle normative regionali garantendo al contempo una copertura di sicurezza completa.

Caso d'uso di esempio: standard di sicurezza del team di sviluppo

Un'organizzazione di sviluppo software implementa le politiche del Security Hub che consentono il monitoraggio nelle aree di produzione mantenendo le aree di sviluppo non gestite. Nelle proprie politiche utilizzano elenchi di regioni espliciti anziché `ALL_SUPPORTED` mantenere un controllo preciso sulla copertura del monitoraggio della sicurezza. Questo approccio consente loro di applicare controlli di sicurezza più rigorosi negli ambienti di produzione, mantenendo al contempo la flessibilità nelle aree di sviluppo.

Ereditarietà e applicazione delle politiche

Comprendere come le politiche vengono ereditate e applicate è fondamentale per una gestione efficace della sicurezza in tutta l'organizzazione. Il modello di ereditarietà segue la AWS Organizations gerarchia, garantendo un'applicazione delle policy prevedibile e coerente.

- Le politiche allegate a livello principale si applicano a tutti gli account
- Gli account ereditano le politiche dalle unità organizzative principali
- È possibile applicare più politiche a un singolo account
- Le politiche più specifiche (più vicine all'account nella gerarchia) hanno la precedenza

Convalida di policy

Quando si creano le policy di Security Hub, si verificano le seguenti convalide:

- I nomi delle regioni devono essere identificatori di AWS regione validi

- Le aree devono essere supportate da Security Hub
- La struttura delle politiche deve seguire le AWS Organizations regole di sintassi delle politiche
- Entrambi `enable_in_regions` gli `disable_in_regions` elenchi devono essere presenti, sebbene possano essere vuoti

Considerazioni regionali e regioni supportate

Le policy di Security Hub operano in più regioni e richiedono un'attenta considerazione dei requisiti di sicurezza globali. La comprensione del comportamento regionale consente di implementare controlli di sicurezza efficaci in tutta la presenza globale dell'organizzazione.

- L'applicazione delle politiche avviene in ogni regione in modo indipendente
- Puoi specificare quali regioni includere o escludere nelle tue politiche
- Le nuove regioni vengono incluse automaticamente quando si utilizza l'`ALL_SUPPORTED`opzione
- Le politiche si applicano solo alle regioni in cui è disponibile Security Hub

Passaggi successivi

Per iniziare a usare le policy di Security Hub:

1. Consulta i prerequisiti nella Guida introduttiva alle politiche di Security Hub
2. Pianifica la tua strategia politica utilizzando la nostra guida alle migliori pratiche
3. Scopri la sintassi delle policy e visualizza esempi di policy

Guida introduttiva alle policy di Security Hub

Prima di configurare le policy di Security Hub, assicurati di aver compreso i prerequisiti e i requisiti di implementazione. Questo argomento ti guida attraverso il processo di configurazione e gestione di queste politiche nella tua organizzazione.

Prima di iniziare

Esamina i seguenti requisiti prima di implementare le politiche del Security Hub:

- Il tuo account deve far parte di un' AWS Organizations organizzazione
- Devi aver effettuato l'accesso in uno dei seguenti modi:

  - L'account di gestione dell'organizzazione
  - Un account amministratore delegato con autorizzazioni per gestire le politiche del Security Hub
- È necessario abilitare l'accesso affidabile per Security Hub nella propria organizzazione
- È necessario abilitare il tipo di policy Security Hub nella radice dell'organizzazione

Inoltre, verifica che:

- Security Hub è supportato nelle regioni in cui si desidera applicare le politiche
- Il ruolo `AWSServiceRoleForSecurityHubV2` collegato al servizio è configurato nel tuo account di gestione. Per verificare l'esistenza di questo ruolo, esegui. `aws iam get-role --role-name AWSServiceRoleForSecurityHubV2` Se devi creare questo ruolo, puoi eseguirlo `aws securityhub enable-security-hub-v2` in qualsiasi regione dal tuo account di gestione o crearlo direttamente eseguendo`aws iam create-service-linked-role --aws-service-name securityhubv2.amazonaws.com`.

Passaggi dell'implementazione

Per implementare le politiche del Security Hub in modo efficace, segui questi passaggi in sequenza. Ogni passaggio garantisce una configurazione corretta e aiuta a prevenire problemi comuni durante la configurazione. L'account di gestione o l'amministratore delegato può eseguire questi passaggi tramite la AWS Organizations console, l'interfaccia a riga di AWS comando (AWS CLI) o. AWS SDKs

1. Abilita l'accesso affidabile per Security Hub.
2. Abilita le politiche di Security Hub per la tua organizzazione.
3. Crea una policy Security Hub.
4. Allega la policy Security Hub alla directory principale, all'unità organizzativa o all'account della tua organizzazione.
5. Visualizza la politica combinata efficace di Security Hub che si applica a un account.

Per tutti questi passaggi, accedi come utente AWS Identity and Access Management (IAM), assumi un ruolo IAM o accedi come utente root (non consigliato) nell'account di gestione dell'organizzazione.

Altre informazioni

- Scopri la sintassi delle policy per le policy di Security Hub e guarda gli esempi di policy

Le migliori pratiche per l'utilizzo delle policy di Security Hub

Quando si implementano le policy di Security Hub in tutta l'organizzazione, seguire le best practice consolidate aiuta a garantire l'implementazione e la manutenzione di successo delle configurazioni di sicurezza. Queste linee guida riguardano specificamente gli aspetti unici della gestione e dell'applicazione delle policy di Security Hub all'interno AWS Organizations.

Principi di progettazione delle politiche

Prima di creare le policy di Security Hub, stabilisci principi chiari per la struttura delle policy. Mantieni le policy semplici ed evita complesse regole combinate tra attributi o annidate che rendono difficile la determinazione del risultato finale. Inizia con politiche generali a livello di organizzazione e perfezionale attraverso politiche secondarie, se necessario.

Prendi in considerazione l'utilizzo strategico di elenchi di regioni vuoti. Puoi lasciarlo `enable_in_regions` vuoto quando devi disabilitare Security Hub solo in aree specifiche o lasciare `disable_in_regions` vuoto per evitare che le aree non siano gestite dalle policy. Questa flessibilità ti aiuta a mantenere un controllo preciso sulla copertura del monitoraggio della sicurezza.

Strategie di gestione delle regioni

Quando gestisci le aree tramite le policy del Security Hub, prendi in considerazione questi approcci collaudati. `ALL_SUPPORTED`Utilizzalo quando desideri includere automaticamente le regioni future nella tua copertura di sicurezza. Per un controllo più granulare, elenca in modo esplicito le regioni anziché fare affidamento su di esse`ALL_SUPPORTED`, soprattutto quando aree diverse richiedono configurazioni di sicurezza diverse.

Documenta i requisiti specifici della tua regione, in particolare per:

- Regioni soggette a obblighi di conformità che richiedono configurazioni specifiche
- Differenze tra ambiente di sviluppo e ambiente di produzione
- Regioni che prevedono l'adesione con considerazioni particolari
- Regioni in cui il Security Hub deve rimanere disabilitato

Pianificazione dell'ereditarietà delle politiche

Pianificate attentamente la struttura di ereditarietà delle polizze per mantenere un controllo di sicurezza efficace, garantendo al contempo la flessibilità necessaria. Documenta quali unità organizzative possono modificare le politiche ereditate e quali modifiche sono consentite. Prendi

in considerazione la possibilità di limitare gli operatori di ereditarietà (@ @assign, @ @append, @ @remove) ai livelli principali quando devi applicare controlli di sicurezza rigorosi.

Monitoraggio e convalida

Implementa pratiche di monitoraggio regolari per garantire che le tue politiche rimangano efficaci. Rivedi periodicamente gli allegati delle politiche, soprattutto dopo i cambiamenti organizzativi. Verifica che le configurazioni delle aree corrispondano alla copertura di sicurezza prevista, in particolare quando utilizzi `ALL_SUPPORTED` o gestisci più elenchi di aree.

Strategie di risoluzione

Durante la risoluzione dei problemi relativi alle policy di Security Hub, concentrati innanzitutto sulla priorità e sull'ereditarietà delle policy. Ricorda che le configurazioni di disabilitazione hanno la precedenza sull'attivazione delle configurazioni quando le regioni compaiono in entrambi gli elenchi. Controlla le catene di ereditarietà delle politiche per capire come le politiche relative ai genitori e ai figli si combinano per creare la politica efficace per ogni account.

Sintassi ed esempi delle policy di Security Hub

Le policy di Security Hub seguono una sintassi JSON standardizzata che definisce il modo in cui Security Hub è abilitato e configurato all'interno dell'organizzazione. La comprensione della struttura delle politiche consente di creare politiche efficaci per i requisiti di sicurezza.

Considerazioni

Prima di creare le policy di Security Hub, comprendi questi punti chiave sulla sintassi delle policy:

- Entrambi `enable_in_regions` gli `disable_in_regions` elenchi sono obbligatori nella policy, sebbene possano essere vuoti
- Nell'elaborazione di politiche efficaci, ha la `disable_in_regions` precedenza su `enable_in_regions`
- Le politiche secondarie possono modificare le politiche principali utilizzando operatori di ereditarietà, a meno che non siano esplicitamente limitate
- La `ALL_SUPPORTED` designazione include regioni attuali e future
- I nomi delle aree devono essere validi e disponibili in Security Hub

Struttura politica di base

Una policy Security Hub utilizza questa struttura di base:

```
{
   "securityhub":{
      "enable_in_regions":[
         "us-east-1",
         "us-west-2"
      ],
      "disable_in_regions":[
         "eu-central-1"
      ]
   }
}
```

Componenti della politica

Le policy di Security Hub contengono questi componenti chiave:

`securityhub`

Il contenitore di primo livello per le impostazioni delle politiche

Obbligatorio per tutte le policy di Security Hub

`enable_in_regions`

Elenco delle regioni in cui deve essere abilitato Security Hub

Può contenere nomi di regioni specifici o `ALL_SUPPORTED`

Campo obbligatorio ma può essere vuoto

In caso di utilizzo`ALL_SUPPORTED`, include le regioni future

`disable_in_regions`

Elenco delle regioni in cui il Security Hub deve essere disabilitato

Può contenere nomi di regioni specifici o `ALL_SUPPORTED`

Campo obbligatorio ma può essere vuoto

Ha la precedenza su `enable_in_regions` quando le regioni appaiono in entrambi gli elenchi

Operatori di ereditarietà

@ @assign - Sovrascrive i valori ereditati

@ @append - Aggiunge nuovi valori a quelli esistenti

@ @remove - Rimuove valori specifici dalle impostazioni ereditate

Esempi di policy di Security Hub

Gli esempi seguenti mostrano configurazioni comuni delle policy di Security Hub.

L'esempio seguente abilita Security Hub in tutte le regioni attuali e future. Inserendola `ALL_SUPPORTED` nell'`enable_in_regions`elenco e lasciandola `disable_in_regions` vuota, questa politica garantisce una copertura di sicurezza completa man mano che nuove regioni diventano disponibili.

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@assign":[
            "ALL_SUPPORTED"
         ]
      },
      "disable_in_regions":{
         "@@assign":[

         ]
      }
   }
}
```

Questo esempio disabilita Security Hub in tutte le regioni, comprese le aree future, poiché l'`disable_in_regions`elenco ha la precedenza su. `enable_in_regions`

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@assign":[
            "us-east-1",
            "us-west-2"
         ]
      },
      "disable_in_regions":{
         "@@assign":[
            "ALL_SUPPORTED"
```

```
         ]
      }
   }
}
```

L'esempio seguente dimostra come le politiche secondarie possono modificare le impostazioni delle politiche principali utilizzando operatori di ereditarietà. Questo approccio consente un controllo granulare mantenendo al contempo la struttura generale delle politiche. La politica per i bambini aggiunge una nuova regione `enable_in_regions` e ne rimuove una da`disable_in_regions`.

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@append":[
            "eu-central-1"
         ]
      },
      "disable_in_regions":{
         "@@remove":[
            "us-west-2"
         ]
      }
   }
}
```

Questo esempio mostra come abilitare Security Hub in più aree specifiche senza utilizzarlo`ALL_SUPPORTED`. Ciò fornisce un controllo preciso su quali aree hanno il Security Hub abilitato, lasciando le aree non specificate non gestite dalla policy.

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@assign":[
            "us-east-1",
            "us-west-2",
            "eu-west-1",
            "ap-southeast-1"
         ]
      },
      "disable_in_regions":{
         "@@assign":[
```

```
         ]
      }
   }
}
```

L'esempio seguente dimostra come gestire i requisiti di conformità regionali abilitando Security Hub nella maggior parte delle regioni e disabilitandolo esplicitamente in posizioni specifiche. L'`disable_in_regions`elenco ha la precedenza, garantendo che Security Hub rimanga disabilitato in quelle aree indipendentemente dalle altre impostazioni dei criteri.

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@assign":[
            "ALL_SUPPORTED"
         ]
      },
      "disable_in_regions":{
         "@@assign":[
            "ap-east-1",
            "me-south-1"
         ]
      }
   }
}
```

Amministratore delegato per AWS Organizations

Ti consigliamo di utilizzare l'account di AWS Organizations gestione e i relativi utenti e ruoli solo per le attività che devono essere eseguite da quell'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 Organizations service control policies (SCPs) 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.

Ad esempio, politiche di delega basate sulle risorse, vedi. Esempi di policy basate sulle risorse per AWS Organizations

Argomenti

Crea una politica di delega basata sulle risorse con AWS Organizations

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

Autorizzazioni minime

Per creare la politica di delega basata sulle risorse, sono necessarie le autorizzazioni per eseguire le seguenti azioni:

- `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 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:

- Politica JSON: incolla e personalizza un esempio di politica di delega basata sulle risorse da utilizzare nel tuo account oppure 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.

Usa l'editor di policy JSON per creare una politica di delega

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. Seleziona Impostazioni.
3. Nella sezione Amministratore delegato per AWS Organizations, scegli Delega per creare la policy di delega di Organizations.
4. Specificare un documento della 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.

Usa l'editor visivo per creare una politica di delega

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. Seleziona Impostazioni.
3. Nella sezione Amministratore delegato per AWS Organizations, scegli Delega per creare la policy di delega di Organizations.
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.
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 membro delegato può allegare politiche alla radice o alle unità organizzative dell'organizzazione (OUs), impostaResources. Dovrai inoltre selezionare `policy` come tipo di risorsa. 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 le risorse ARNs manualmente nell'editor. Per ulteriori informazioni sulla sintassi ARN, consulta Amazon Resource Name (ARN) nella General Reference Guide. AWS Per

informazioni sull'utilizzo ARNs dell'elemento risorsa di una policy, consulta IAM JSON policy elements: Resource.

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`**. 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

Crea una politica di delega

È possibile utilizzare il seguente comando per creare una politica di delega:

- AWS CLI: put-resource-policy

  L'esempio seguente crea una politica 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"
                    ]
                }
            }
        }
    ]
}
```

- AWS SDK: 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

Chiavi di condizione supportate

Solo le chiavi condizionali supportate da AWS Organizations possono essere utilizzate per la politica di delega. Per ulteriori informazioni, vedere Condition keys for AWS Organizations nel Service Authorization Reference.

Aggiorna una politica di delega basata sulle risorse con AWS Organizations

Dall'account di gestione, aggiorna una politica di delega basata sulle risorse per la tua organizzazione e aggiungi una dichiarazione che specifichi quali account membri possono eseguire azioni sulle

politiche. Puoi aggiungere più istruzioni nella policy per indicare un diverso set di autorizzazioni per gli account membri.

Autorizzazioni minime

Per aggiornare la politica di delega basata sulle risorse, sono necessarie le autorizzazioni per eseguire le seguenti azioni:

- `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 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:

- Politica JSON: incolla e personalizza un esempio di politica di delega basata sulle risorse da utilizzare nel tuo account oppure 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.

Utilizza l'editor di policy JSON per aggiornare una politica di delega

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. Seleziona Impostazioni.
3. Nella AWS Organizations sezione Amministratore delegato per, scegli Modifica per aggiornare la politica di delega di Organizations.
4. Specificare un documento della 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 politiche, quindi scegli Crea politica.

Usa l'editor visivo per aggiornare una politica di delega

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. Seleziona Impostazioni.
3. Nella AWS Organizations sezione Amministratore delegato per, scegli Modifica per aggiornare la politica di delega di Organizations.
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.
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 membro delegato può allegare politiche alle unità principali o organizzative dell'organizzazione (OUs), imposta. `Resources` Dovrai inoltre selezionare `policy` come tipo di risorsa. 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 le risorse ARNs manualmente nell'editor. Per ulteriori informazioni sulla sintassi ARN, consulta Amazon Resource Name (ARN) nella General Reference Guide. AWS Per informazioni sull'utilizzo ARNs dell'elemento risorsa di una policy, consulta IAM JSON policy elements: Resource.
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`**. 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 della policy, quindi scegli Salva policy.

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"
                    ]
                }
            }
        }
    ]
}
```

- AWS SDK: 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`

Chiavi di condizione supportate

Solo le chiavi condizionali supportate da AWS Organizations possono essere utilizzate per la politica di delega. Per ulteriori informazioni, vedere Condition keys for AWS Organizations nel Service Authorization Reference.

Visualizza una politica di delega basata sulle risorse con AWS Organizations

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. 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. 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
  ```

- AWS SDK: DescribeResourcePolicy

Elimina una politica di delega basata sulle risorse con AWS Organizations

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. 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. 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
  ```

- AWS SDK: DeleteResourcePolicy

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 o da un account membro designato come amministratore delegato.

> **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 politica, scegli Abilita. ***policy type***

   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`.

- AWS SDKs: 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. È possibile disabilitare un tipo di policy solo dall'account di gestione dell'organizzazione o da un account membro designato come amministratore delegato.

Considerazioni

Le politiche disabilitate vengono scollegate da tutte le entità ma non eliminate

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 il tipo di policy di controllo del servizio) Tutte le entità nella radice vengono inizialmente collegate solo all'SCP predefinito **`FullAWSAccess`**

(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. Gli allegati delle SCPs entità vengono persi quando

SCPs vengono disabilitati nell'organizzazione. Se in seguito desideri riattivarli SCPs, devi ricollegarli alla radice e agli account dell'organizzazione OUs, a seconda dei casi.

Disabilita un tipo di policy

Autorizzazioni minime

Per disabilitarlo SCPs, è necessaria l'autorizzazione per eseguire le seguenti azioni:

- `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 Disabilita ***policy type***.
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.

- AWS SDKs: DisablePolicyType

Creazione di politiche organizzative con AWS Organizations

Dopo aver abilitato le politiche per l'organizzazione, puoi creare una politica.

Questo argomento descrive come creare politiche con AWS Organizations. Una politica definisce i controlli che si desidera applicare a un gruppo di Account AWS.

Argomenti

- Creare una policy di controllo del servizio (SCP)
- Creare una politica di controllo delle risorse (RCP)
- Crea una politica dichiarativa
- Crea una policy di backup
- Crea una politica di tag
- Crea una politica per le applicazioni di chat
- Crea una politica di disattivazione dei servizi AI
- Creare una policy Security Hub

Creare una policy di controllo del servizio (SCP)

Autorizzazioni minime

Per creare SCPs, è necessaria l'autorizzazione per eseguire la seguente azione:

- `organizations:CreatePolicy`

AWS Management Console

Per creare una policy di controllo dei servizi

1. Accedi alla AWS Organizations console . 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 Taggare le 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. Se si utilizzano `Deny` le istruzioni, si dispone di un controllo aggiuntivo in quanto è possibile limitare l'accesso a risorse specifiche, definire le condizioni relative all' SCPs entrata

in vigore e utilizzare l'NotActionelemento. Per informazioni dettagliate sulla sintassi, consulta Sintassi delle SCP.

Per aggiungere un'istruzione che nega l'accesso:

a. Nel riquadro Modifica istruzioni a destra dell'editor, in Aggiungi azioni, scegli un AWS servizio.

   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 è possibile scegliere qualsiasi chiave di condizione disponibile per tutti i AWS servizi (ad esempio,`aws:SourceIp`) o una chiave specifica del servizio solo per uno dei servizi selezionati per questa istruzione.
- Qualificatore: (Facoltativo) Quando la richiesta contiene più di un valore per una chiave di contesto multivalore, è possibile specificare un qualificatore per testare le richieste rispetto ai valori. Per ulteriori informazioni, consulta Chiavi di contesto a valore singolo e chiavi di contesto multivalore nella IAM User Guide. Per verificare se una richiesta può avere più valori, consulta la sezione Azioni, risorse e chiavi di condizione nel Service Authorization Reference. Servizi AWS
  - 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 tranne il `Null` test, puoi scegliere l'IfExistsopzione.

- Valore - (Facoltativo) Specifica uno o più valori per i quali desideri testare la richiesta.

Scegliere 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.

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. Ora puoi collegare il tuo SCP alla radice o agli account. OUs

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\":[\"*\"]}]}"
    }
}
```

- AWS SDKs: CreatePolicy

> **Note**
>
> SCPs non hanno effetto sull'account di gestione e in alcune altre situazioni. Per ulteriori informazioni, consulta Attività ed entità non limitate da SCPs.

Creare una politica di controllo delle risorse (RCP)

> **Autorizzazioni minime**
>
> Per creare RCPs, è necessaria l'autorizzazione per eseguire la seguente azione:
>
> - `organizations:CreatePolicy`

AWS Management Console

Per creare una politica di controllo delle risorse

1. Accedi alla AWS Organizations console . 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 Politica di controllo delle risorse, scegli Crea politica.
3. Nella pagina Crea una nuova politica di controllo delle risorse, inserisci un nome di politica e una descrizione facoltativa della politica.
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 Taggare le 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 aggiungere una dichiarazione:

   a. Nel riquadro Modifica istruzione a destra dell'editor, in Aggiungi azioni, scegli un AWS servizio.

      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.
- Completa l'Amazon Resource Name (ARN) in Resource ARN per identificare la risorsa specifica a 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. Consulta la documentazione relativa a un tipo di risorsa specifico per informazioni su dove puoi usare le wild card.
- 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 è possibile scegliere qualsiasi chiave di condizione disponibile per tutti i AWS servizi (ad esempio,`aws:SourceIp`) o una chiave specifica del servizio solo per uno dei servizi selezionati per questa istruzione.
- Qualificatore: (Facoltativo) Quando la richiesta contiene più di un valore per una chiave di contesto multivalore, è possibile specificare un qualificatore per testare le richieste rispetto ai valori. Per ulteriori informazioni, consulta Chiavi di contesto a valore singolo e chiavi di contesto multivalore nella IAM User Guide. Per verificare se una richiesta può avere più valori, consulta la sezione Azioni, risorse e chiavi di condizione nel Service Authorization Reference. Servizi AWS
  - 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 tranne il `Null` test, puoi scegliere l'IfExistsopzione.

- Valore - (Facoltativo) Specifica uno o più valori per i quali desideri testare la richiesta.

Scegliere 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 IAM JSON Policy Elements: NotAction nella IAM User Guide.

6. (Facoltativo) Per aggiungere un'altra istruzione alla policy, scegli Add statement (Aggiungi istruzione) e utilizza l'editor visivo per creare l'istruzione successiva.
7. Quando hai finito di aggiungere le istruzioni, scegli Crea policy per salvare l'RCP completato.

Il tuo nuovo RCP viene visualizzato nell'elenco delle politiche dell'organizzazione. Ora puoi collegare il tuo RCP alla radice o agli OUs account.

AWS CLI & AWS SDKs

Per creare una politica di controllo delle risorse

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

- 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 quel file per creare una nuova politica di controllo delle risorse.

```
$ aws organizations create-policy \
    --content file://Deny-IAM.json \
    --description "Deny all IAM actions" \
    --name DenyIAMRCP \
    --type RESOURCE_CONTROL_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
resource_control_policy/p-i9j8k7l6m5",
            "Name": "DenyIAMRCP",
            "Description": "Deny all IAM actions",
            "Type": "RESOURCE_CONTROL_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

- AWS SDKs: CreatePolicy

> **Note**
>
> RCPs non hanno effetto sull'account di gestione e in alcune altre situazioni. Per ulteriori informazioni, consulta Risorse ed entità non limitate da RCPs.

Crea una politica dichiarativa

Autorizzazioni minime

Per creare una politica dichiarativa, è necessaria l'autorizzazione per eseguire la seguente azione:

- `organizations:CreatePolicy`

AWS Management Console

Per creare una politica dichiarativa

1. Accedi alla AWS Organizations console . 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 Politiche dichiarative, scegli Crea politica.
3. Nella EC2pagina Crea nuova politica dichiarativa per, inserisci un nome di politica e una descrizione facoltativa della politica.
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, consulta Taggare le 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 delle politiche dichiarative, vedere. Sintassi ed esempi delle politiche dichiarative

   Se scegli di utilizzare l'editor visivo, seleziona l'attributo di servizio che desideri includere nella tua politica dichiarativa. Per ulteriori informazioni, consulta Supportato Servizi AWS e attributi.
6. Scegli Aggiungi attributo di servizio e configura l'attributo in base alle tue specifiche. Per informazioni più dettagliate su ciascun effetto, consultaSintassi ed esempi delle politiche dichiarative.
7. 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 politica dichiarativa

È possibile utilizzare uno dei seguenti metodi per creare una politica dichiarativa:

- AWS CLI: create-policy

1. Create una politica dichiarativa come la seguente e memorizzatela in un file di testo.

```
{
    "ec2_attributes": {
        "image_block_public_access": {
            "state": {
                "@@assign": "block_new_sharing"
            }
        }
    }
}
```

Questa politica dichiarativa specifica che tutti gli account interessati dalla policy devono essere configurati in modo che le nuove Amazon Machine Images (AMIs) non siano condivisibili pubblicamente. Per informazioni sulla sintassi delle politiche dichiarative, consulta. Sintassi ed esempi delle politiche dichiarative

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 DECLARATIVE_POLICY_EC2 \
    --name "MyTestPolicy" \
    --description "My test policy" \
    --content file://policy.json
{
    "Policy": {
        "Content": "{"ec2_attributes":{"image_block_public_access":{"state":
{"@@assign":"block_new_sharing"}}}}".
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5"
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/
declarative_policy_ec2/p-i9j8k7l6m5",
            "Description": "My test policy",
            "Name": "MyTestPolicy",
```

```
            "Type": "DECLARATIVE_POLICY_EC2"
        }
    }
}
```

- AWS SDKs: CreatePolicy

Cosa fare in seguito

Dopo aver creato una politica dichiarativa, valuta lo stato di preparazione utilizzando il rapporto sullo stato dell'account. È quindi possibile applicare le configurazioni di base. A tale scopo, è possibile collegare la policy alla radice dell'organizzazione, alle unità organizzative (OUs), Account AWS all'interno dell'organizzazione o a una combinazione di tutti questi elementi.

Crea 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

È possibile creare una policy di backup 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. Accedi alla AWS Organizations console . 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 sull'assegnazione di tag, consulta Taggare le 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. Crea il vault utilizzando la AWS Backup console o AWS CLI i comandi.

- (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 le coppie di tag AWS Backup utilizzate 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" ] }
                    }
                }
            }
        }
    }
}
```

Questo piano di backup specifica che AWS Backup deve eseguire il backup di tutte le risorse dell'area interessata Account AWS che si trovano nel campo specificato Regioni AWS e che hanno il tag `dataType` con un valore di`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...",
    }
```

```
}
```

- AWS SDKs: CreatePolicy

Crea una politica di tag

> **Autorizzazioni minime**
>
> Per creare le policy di tag, è necessaria l'autorizzazione per la seguente operazione:
>
> - `organizations:CreatePolicy`

Puoi creare una politica sui tag 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

È possibile creare una politica sui tag 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 tag

1. Accedi alla AWS Organizations console . 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 Taggare le 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.

   Se scegli di utilizzare l'editor visivo, specifica quanto segue:
6. Per New tag key 1 (Nuova chiave di tag 1), specifica il nome di una chiave di tag da aggiungere.
7. Per le opzioni di conformità, puoi selezionare le seguenti opzioni:

   a. Utilizzate le lettere maiuscole che avete specificato sopra per la chiave del tag: lasciate questa opzione deselezionata (impostazione predefinita) per specificare che la politica del tag principale ereditata, se esiste, deve definire il trattamento tra maiuscole e minuscole per la chiave del 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 allegare politiche di tag aggiuntive ai nostri account per OUs creare regole di tagging aggiuntive.

b. Specificate i valori consentiti per questa chiave di tag: attivate questa opzione se desiderate aggiungere i valori consentiti per questa chiave di tag a qualsiasi valore ereditato da una politica principale.

   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 applicare i tipi di risorsa, puoi selezionare Impedisci operazioni non conformi per questo tag.

   Ti consigliamo di lasciare deselezionata questa opzione (impostazione predefinita) a meno che tu non abbia esperienza nell'uso delle politiche relative ai 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 politica come questa significa che una risorsa a cui è associato il CostCenter tag con o senza un 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"
    }
}
```

- AWS SDKs: CreatePolicy

Crea una politica per le applicazioni di chat

> **Autorizzazioni minime**
>
> Per creare una politica per le applicazioni di chat, è necessaria l'autorizzazione per eseguire la seguente azione:

- `organizations:CreatePolicy`

AWS Management Console

È possibile creare una politica per le applicazioni di chat 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 politica per le applicazioni di chat

1. Accedi alla AWS Organizations console . 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 delle politiche del Chatbot, scegli Crea policy.
3. Nella pagina Crea nuove applicazioni di chat, inserisci un nome per la politica e una descrizione facoltativa della politica.
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, consulta Taggare le 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 delle policy delle applicazioni di chat, consultaSintassi ed esempi delle policy delle applicazioni di chat.

Se scegli di utilizzare l'editor visivo, configura la politica delle applicazioni di chat specificando i controlli di accesso per i client di chat.

a. Scegli una delle seguenti opzioni per impostare l'accesso al client di chat Amazon Chime
   - Nega l'accesso a chime.
   - Consenti l'accesso a Chime.

b. Scegli quanto segue per Impostare l'accesso al client di chat di Microsoft Teams
   - Nega l'accesso a tutti i team
   - Consenti l'accesso a tutti i team
   - Limita l'accesso a team denominati

c. Scegli una delle seguenti opzioni per impostare l'accesso al client di chat Slack
   - Nega l'accesso a tutte le aree di lavoro Slack
   - Consenti l'accesso a tutte le aree di lavoro Slack
   - Limita l'accesso agli spazi di lavoro Slack denominati

> **Note**
>
> Inoltre, puoi selezionare Limita l'utilizzo di Amazon Q Developer nelle applicazioni di chat ai soli canali Slack privati.

d. Seleziona le seguenti opzioni per Imposta i tipi di autorizzazioni IAM
   - Abilita il ruolo IAM a livello di canale: tutti i membri del canale condividono le autorizzazioni del ruolo IAM per eseguire attività in un canale. Un ruolo di canale è appropriato se i membri del canale richiedono le stesse autorizzazioni.
   - Abilita il ruolo IAM a livello di utente: i membri del canale devono scegliere un ruolo utente IAM per eseguire le azioni (richiede l'accesso alla console per scegliere i ruoli). I ruoli utente sono appropriati se i membri del canale richiedono autorizzazioni diverse e possono scegliere i propri ruoli utente.

6. Al termine della creazione della policy, scegli Create policy (Crea policy). La politica viene visualizzata nell'elenco delle politiche di backup dei chatbot.

AWS CLI & AWS SDKs

Per creare una politica per le applicazioni di chat

È possibile utilizzare una delle seguenti opzioni per creare una politica per le applicazioni di chat:

- AWS CLI: create-policy

  Puoi utilizzare qualsiasi editor di testo per creare una politica per le applicazioni di chat. Usa la sintassi JSON e salva la politica delle applicazioni di chat come file con qualsiasi nome ed estensione in una posizione a tua scelta. Le politiche delle applicazioni di chat possono avere un massimo di? caratteri, spazi inclusi. Per informazioni sulla sintassi delle policy di tag, consulta Sintassi ed esempi delle policy delle applicazioni di chat.

  Per creare una politica per le applicazioni di chat

  1. Crea una politica per le applicazioni di chat in un file di testo simile al seguente:

     Contenuto di `testpolicy.json`.

```
{
   "chatbot": {
      "platforms": {
         "slack": {
            "client": {
               "@@assign": "enabled"
            },
            "workspaces": {
               "@@assign": [
                  "Slack-Workspace-Id"
               ]
            },
            "default": {
               "supported_channel_types": {
                  "@@assign": [
                     "private"
                  ]
               }
            }
         },
         "microsoft_teams": {
            "client": {
               "@@assign": "disabled"
            }
         }
      }
   }
```

```
}
```

Questa politica sulle applicazioni di chat consente solo canali Slack privati in un'area di lavoro specifica, disabilita Microsoft Teams e supporta tutte le impostazioni dei ruoli.

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 "MyTestChatbotPolicy" \
    --description "My Test policy" \
    --content file://testpolicy.json \
    --type CHATBOT_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-a1b2c3d4e5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
chatbot_policy/p-a1b2c3d4e5",
            "Name": "MyTestChatApplicationsPolicy",
            "Description": "My Test policy",
            "Type": "CHATBOT_POLICY",
            "AwsManaged": false
        },
        "Content": "{"chatbot":{"platforms":{"slack":{"client":
{"@@assign":"enabled"},"workspaces":{"@@assign":["Slack-Workspace-
Id"]},"supported_channel_types":{"@@assign":["private"]}},"microsoft_teams":
{"client":{"@@assign":"disabled"}}}}}"
    }
}
```

- AWS SDKs: CreatePolicy

Crea una politica di disattivazione dei servizi AI

> **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. Accedi alla AWS Organizations console . 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, consulta Taggare le 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"
        }
    }
}
```

- AWS SDKs: CreatePolicy

Creare una policy Security Hub

> **Autorizzazioni minime**
>
> Per creare una policy di Security Hub, è necessaria l'autorizzazione per eseguire la seguente azione:
>
> - `organizations:CreatePolicy`

AWS Management Console

Per creare una policy Security Hub

1. Accedi alla AWS Organizations console . 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 delle politiche di Security Hub, scegli Crea policy.
3. Nella pagina Crea un nuovo criterio di Security Hub, inserisci un nome di policy e una descrizione facoltativa della 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, consulta Taggare le risorse AWS Organizations.
5. Inserisci o incolla il testo della policy nella casella del codice JSON. Per informazioni sulla sintassi delle policy di Security Hub, vedereSintassi ed esempi delle policy di Security Hub. Per esempi di policy che puoi utilizzare come punto di partenza, consulta Esempi di policy di Security Hub.
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 Security Hub

È possibile utilizzare uno dei seguenti metodi per creare una policy di Security Hub:

- AWS CLI: create-policy

Esempio: creare una policy che abiliti Security Hub in tutte le regioni supportate

L'esempio seguente presuppone l'esistenza di un file denominato `testPolicy_enableAllSupportedRegions.json` con il testo della policy JSON al suo interno. Utilizza quel file per creare una nuova politica del Security Hub.

```
$ aws organizations create-policy \
    --content file://./testPolicy_enableAllSupportedRegions.json \
    --name "testPolicy_enableAllSupportedRegions" \
    --description "Test policy to enable securityhub in ALL_SUPPORTED Regions" \
    --type SECURITYHUB_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-66ev7hgcvj",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66ev7hgcvj",
            "Name": "testPolicy_enableAllSupportedRegions",
            "Description": "Test policy to enable securityhub in ALL_SUPPORTED
 Regions",
            "Type": "SECURITYHUB_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
 {\n      \"@@assign\":[\n        \"ALL_SUPPORTED\"\n      ]\n    },\n
 \"disable_in_regions\": {\n      \"@@assign\":[]\n    }\n  }\n}\n"
    }
}
```

Esempio: creare una policy che abiliti Security Hub in tutte le regioni supportate ma la disabiliti nella regione us-east-1

L'esempio seguente presuppone l'esistenza di un file denominato `testPolicy_enableAllSupportedRegions_Disable_us-east-1.json` con il testo della policy JSON al suo interno. Utilizza quel file per creare una nuova politica del Security Hub.

```
$ aws organizations create-policy \
    --content file://./testPolicy_enableAllSupportedRegions_Disable_us-east-1.json
 \
    --name "testPolicy_enableAllSupportedRegions_Disable_us-east-1" \
```

```
    --description "Test policy to enable securityhub in ALL_SUPPORTED Regions but
 disable in us-east-1 Region" \
    --type SECURITYHUB_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-66217dwpos",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66217dwpos",
            "Name": "testPolicy_enableAllSupportedRegions_Disable_us-east-1",
            "Description": "Test policy to enable securityhub in ALL_SUPPORTED
 Regions but disable in us-east-1 Region",
            "Type": "SECURITYHUB_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
 {\n      \"@@assign\":[\n        \"ALL_SUPPORTED\"\n      ]\n    },\n
 \"disable_in_regions\": {\n      \"@@assign\":[\n        \"us-east-1\"\n      ]\n
    }\n  }\n}\n"
    }
}
```

- AWS SDKs: CreatePolicy

Aggiornamento delle politiche dell'organizzazione con AWS Organizations

Quando i requisiti della tua politica cambiano, puoi aggiornare una politica esistente.

Questo argomento descrive come aggiornare le politiche con AWS Organizations. Una policy definisce i controlli che si desidera applicare a un gruppo di Account AWS.

Argomenti

- Aggiornare una policy di controllo del servizio (SCP)
- Aggiornare una politica di controllo delle risorse (RCP)
- Aggiornare una politica dichiarativa
- Aggiornare una politica di backup
- Aggiornare una politica sui tag
- Aggiorna una politica sulle applicazioni di chat

- Aggiorna una politica di disattivazione dei servizi AI
- Aggiornare una policy di Security Hub

Aggiornare una policy di controllo del servizio (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 AWS Organizations console . 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, scegli 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\":[\"*
\"]}]}"
    }
}
```

- AWS SDKs: UpdatePolicy

Aggiornare una politica di controllo delle risorse (RCP)

Quando effettui l'accesso all'account di gestione della tua organizzazione, puoi rinominare o modificare i contenuti di una policy. La modifica del contenuto di un RCP influisce immediatamente su tutte le risorse in tutti gli account collegati.

Autorizzazioni minime

Per aggiornare un RCP, è necessaria l'autorizzazione per eseguire le seguenti azioni:

- `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 AWS Organizations console . 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 Politica di controllo delle risorse, scegli il nome della politica 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, vedere la procedura Creazione di un RCP riportata più avanti in questo argomento.
5. Al termine, scegli 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\":[\"*\"]}]}"
    }
}
```

L'esempio seguente aggiunge o modifica la descrizione di una politica di controllo delle risorse.

```
$ 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\":[\"*\"]}]}"
    }
}
```

L'esempio seguente modifica il documento di policy dell'RCP specificando un file che contiene 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\":[\"*
\"]}]}"
    }
}
```

- AWS SDKs: UpdatePolicy

Aggiornare una politica dichiarativa

> **Autorizzazioni minime**
>
> Per aggiornare una politica dichiarativa, è necessario disporre dell'autorizzazione per eseguire le seguenti azioni:
>
> - `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 politica dichiarativa

1. Accedi alla AWS Organizations console . 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 Politiche dichiarative, scegli il nome della politica che desideri 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 delle politiche dichiarative, consulta. Sintassi ed esempi delle politiche dichiarative
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

L'esempio seguente rinomina una politica dichiarativa.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
declarative_policy_ec2/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "DECLARATIVE_POLICY_EC2",
```

```
            "AwsManaged": false
        },
        "Content": "{"ec2-configuration":{"ec2_attributes":
{"image_block_public_access":{"state":{"@@assign":"block_new_sharing"}}}}".
    }
}
```

L'esempio seguente aggiunge o modifica la descrizione di una politica dichiarativa.

```
$ 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/
declarative_policy_ec2/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "DECLARATIVE_POLICY_EC2",
            "AwsManaged": false
        },
        "Content": "{"ec2_attributes":{"image_block_public_access":{"state":
{"@@assign":"block_new_sharing"}}}}".
    }
}
```

- AWS SDKs: UpdatePolicy

Aggiornare una politica 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. Accedi alla AWS Organizations console . 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" },
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" },
                                "opt_in_to_archive_for_supported_resources":
 {"@@assign": false}
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$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\"]}}}}}}"
}
```

- AWS SDKs: UpdatePolicy

Aggiornare una politica sui 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 AWS Organizations console . 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\"]}}}}"
}
```

- AWS SDKs: UpdatePolicy

Aggiorna una politica sulle applicazioni di chat

> **Autorizzazioni minime**
>
> Per aggiornare una politica delle applicazioni di chat, devi disporre dell'autorizzazione per eseguire le seguenti azioni:
>
> - `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 politica sulle applicazioni di chat

1. Accedi alla AWS Organizations console . 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 delle politiche dei Chatbot, scegli la politica delle applicazioni di chat 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

  L'esempio seguente rinomina una policy per le applicazioni di chat.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed chat applications policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
chatbot_policy/p-i9j8k7l6m5",
            "Name": "Renamed chat applications policy",
            "Type": "CHATBOT_POLICY",
            "AwsManaged": false
        },
        "Content": "{"chatbot":{"platforms":{"slack":{"client":
{"@@assign":"enabled"},"workspaces":{"@@assign":["Slack-Workspace-Id"]},"default":
{"supported_channel_types":{"@@assign":["private"]}}},"microsoft_teams":{"client":
{"@@assign":"disabled"}}}}}"
    }
}
```

- AWS SDKs: UpdatePolicy

Aggiorna una politica di disattivazione dei servizi AI

> **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. Accedi alla AWS Organizations console . 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"}
}
```

- AWS SDKs: UpdatePolicy

Aggiornare una policy di Security Hub

Autorizzazioni minime

Per aggiornare una policy di Security Hub, è necessario disporre dell'autorizzazione per eseguire le seguenti azioni:

- `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 Security Hub

1. Accedi alla AWS Organizations console . 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 delle politiche di Security Hub, scegli il nome della politica che desideri 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 delle policy di Security Hub, vedereSintassi ed esempi delle policy di Security Hub. Per esempi di policy che puoi utilizzare come punto di partenza, consulta Esempi di policy di Security Hub.
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

L'esempio seguente rinomina una politica di Security Hub.

```
$ aws organizations update-policy \
    --policy-id p-66ev7hgcvj \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-66ev7hgcvj",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66ev7hgcvj",
            "Name": "Renamed policy",
            "Type": "SECURITYHUB_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
 {\n      \"@@assign\":[\n        \"ALL_SUPPORTED\"\n      ]\n    },\n
 \"disable_in_regions\": {\n      \"@@assign\":[]\n    }\n  }\n}\n"
    }
}
```

L'esempio seguente aggiunge o modifica la descrizione di una policy di Security Hub.

```
$ aws organizations update-policy \
    --policy-id p-66ev7hgcvj \
    --name "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-66ev7hgcvj",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66ev7hgcvj",
            "Name": "My new description",
            "Type": "SECURITYHUB_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
 {\n      \"@@assign\":[\n        \"ALL_SUPPORTED\"\n      ]\n    },\n
 \"disable_in_regions\": {\n      \"@@assign\":[]\n    }\n  }\n}\n"
    }
}
```

- AWS SDKs: UpdatePolicy

Modifica dei tag allegati alle politiche dell'organizzazione con AWS Organizations

Questo argomento descrive come modificare le politiche relative ai tag allegati con AWS Organizations. Una politica definisce i controlli che si desidera applicare a un gruppo di Account AWS.

Argomenti

Modifica i tag allegati a una policy di controllo del servizio (SCP)

Quando effettui l'accesso all'account di gestione dell'organizzazione, puoi aggiungere o rimuovere i tag collegati a una SCP. Per ulteriori informazioni sull'assegnazione di tag, consulta Taggare le risorse AWS Organizations.

Autorizzazioni minime

Per modificare i tag associati a una SCP nella tua organizzazione , 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 AWS Organizations console . 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, scegli 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
- AWS SDKs: TagResource e UntagResource

Modifica i tag allegati a una politica di controllo delle risorse (RCP)

Quando accedi all'account di gestione della tua organizzazione, puoi aggiungere o rimuovere i tag allegati a un RCP. Per ulteriori informazioni sull'assegnazione di tag, consulta Taggare le risorse AWS Organizations.

Autorizzazioni minime

Per modificare i tag allegati a un RCP nell' AWS organizzazione, 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 allegati a un RCP

1. Accedi alla AWS Organizations console . 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 della politica di controllo delle risorse, scegli il nome della politica con i tag che desideri modificare.
3. Nella pagina dei dettagli della politica, scegli la scheda Tag, quindi scegli 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, scegli Salva le modifiche.

AWS CLI & AWS SDKs

Per modificare i tag allegati a un RCP

È possibile utilizzare uno dei seguenti comandi per modificare i tag allegati a un RCP:

- AWS CLI: tag-resource e untag-resource
- AWS SDKs: TagResource e UntagResource

Modifica i tag allegati a una politica dichiarativa

Quando accedi all'account di gestione della tua organizzazione, puoi aggiungere o rimuovere i tag allegati a una politica dichiarativa. Per ulteriori informazioni sull'assegnazione di tag, consulta Taggare le risorse AWS Organizations.

Autorizzazioni minime

Per modificare i tag allegati a una politica dichiarativa nell' AWS organizzazione, devi 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 allegati a una politica dichiarativa

1. Accedi alla AWS Organizations console . 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 Politiche dichiarative, scegli il nome della politica con i tag che desideri 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 allegati a una politica dichiarativa

È possibile utilizzare uno dei seguenti comandi per modificare i tag allegati a una politica dichiarativa:

- AWS CLI: tag-resource e untag-resource
- AWS SDKs: TagResource e UntagResource

Modifica i tag allegati a una politica 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 sull'assegnazione di tag, consulta Taggare le risorse AWS Organizations.

Autorizzazioni minime

Per modificare i tag associati a una policy di backup nella tua organizzazione , 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. Accedi alla AWS Organizations console . 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 Tag scegliere 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
- AWS SDKs: TagResource e UntagResource

Modifica i tag allegati a una politica sui 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 , 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 tag

1. Accedi alla AWS Organizations console . 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
- AWS SDKs: TagResource e UntagResource

Modifica i tag allegati a una politica delle applicazioni di chat

Quando accedi all'account di gestione della tua organizzazione, puoi aggiungere o rimuovere i tag allegati a una politica per le applicazioni di chat. Per farlo, completa le seguenti fasi.

> **Autorizzazioni minime**
>
> Per modificare i tag allegati a una politica delle applicazioni di chat nella tua organizzazione, devi 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 allegati a una politica delle applicazioni di chat

1. Accedi alla AWS Organizations console . 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 delle politiche del Chatbot, scegli il nome della politica con i tag che desideri 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 allegati a una politica delle applicazioni di chat

Puoi utilizzare uno dei seguenti comandi per modificare i tag allegati a una politica delle applicazioni di chat:

- AWS CLI: tag-resource e untag-resource
- AWS SDKs: TagResource e UntagResource

Modifica i tag allegati a una politica di disattivazione dei servizi AI

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 sull'assegnazione di tag, consulta Taggare le risorse AWS Organizations.

Autorizzazioni minime

Per modificare i tag associati a una policy di rifiuto dei servizi di IA nella tua organizzazione , 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. Accedi alla AWS Organizations console . 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
- AWS SDKs: TagResource e UntagResource

Modificare i tag allegati a una policy di Security Hub

Quando accedi all'account di gestione della tua organizzazione, puoi aggiungere o rimuovere i tag allegati a una policy di Security Hub. Per ulteriori informazioni sull'assegnazione di tag, consulta Taggare le risorse AWS Organizations.

Autorizzazioni minime

Per modificare i tag allegati a una politica di Security Hub nella propria organizzazione, 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 allegati a una politica del Security Hub

1. Accedi alla AWS Organizations console . 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 delle politiche di Security Hub, scegli il nome della politica con i tag che desideri 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 allegati a una politica del Security Hub

È possibile utilizzare uno dei seguenti comandi per modificare i tag allegati a una policy di Security Hub:

- AWS CLI: tag-resource e untag-resource
- AWS SDKs: TagResource e UntagResource

Allegare le politiche organizzative con AWS Organizations

Questo argomento descrive come allegare le politiche con AWS Organizations. Una politica definisce i controlli che si desidera applicare a un gruppo di Account AWS.

Argomenti

Allega le politiche con AWS Organizations

Autorizzazioni minime

Per allegare le politiche, è necessario disporre dell'autorizzazione per eseguire la seguente azione:

- `organizations:AttachPolicy`

Autorizzazioni minime

Per allegare una politica di autorizzazione (SCP o RCP) a una root, un'unità organizzativa o un account, è necessaria l'autorizzazione per eseguire la seguente azione:

- `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

Service control policies (SCPs)

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 AWS Organizations console . 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 OUs (scegliere l'opzione
per trovare l'unità organizzativa 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 degli SCPs allegati nella scheda Politiche 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 AWS Organizations console . 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 OUs (scegliere il) per trovare l'unità organizzativa o l'account desiderato.
5. Scegli Collega policy.

   L'elenco degli SCPs allegati nella scheda Obiettivi 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.

Resource control policies (RCPs)

È possibile allegare un RCP accedendo alla policy o alla root, all'unità organizzativa o all'account a cui si desidera allegare la policy.

Per collegare un RCP accedendo alla directory principale, all'unità organizzativa o all'account

1. Accedi alla AWS Organizations console . 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, accedi e seleziona la casella di controllo accanto alla radice, all'unità organizzativa o all'account a cui desideri collegare un RCP. Potrebbe essere necessario espandere OUs (scegliere il) per trovare l'unità organizzativa o l'account desiderato.
3. Nella scheda Politiche, nella voce Politiche di controllo delle risorse, scegli Allega.
4. Individua la policy desiderata e scegli Attach policy (Collega policy).

   L'elenco degli RCPs allegati nella scheda Politiche viene aggiornato per includere la nuova aggiunta. La modifica della politica ha effetto immediato e influisce sulle autorizzazioni delle risorse nell'account collegato o su tutti gli account nell'unità principale o nell'unità organizzativa allegata.

Per allegare un RCP accedendo alla policy

1. Accedi alla AWS Organizations console . 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 della politica di controllo delle risorse, scegli il nome della politica che desideri allegare.
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 OUs (scegliere l'opzione per trovare l'unità organizzativa o l'account desiderato.
5. Scegli Collega policy.

   L'elenco degli RCPs allegati nella scheda Obiettivi viene aggiornato per includere la nuova aggiunta. La modifica della politica ha effetto immediato e influisce sulle autorizzazioni delle risorse nell'account collegato o su tutti gli account nell'unità principale o nell'unità organizzativa allegata.

Declarative policies

È possibile allegare una politica dichiarativa accedendo alla policy o alla radice, all'unità organizzativa o all'account a cui si desidera allegare la politica.

Per allegare una politica dichiarativa accedendo alla directory principale, all'unità organizzativa o all'account

1. Accedi alla AWS Organizations console . 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 OUs (scegliere il) per trovare l'unità organizzativa o l'account desiderato.
3. Nella scheda Politiche, nella voce Politiche dichiarative, scegli Allega.
4. Individua la policy desiderata e scegli Attach policy (Collega policy).

   L'elenco delle politiche dichiarative allegate nella scheda Politiche viene aggiornato per includere la nuova aggiunta. La modifica della policy diventa immediatamente effettiva.

Per allegare una politica dichiarativa accedendo alla politica

1. Accedi alla AWS Organizations console . 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 Politiche dichiarative, scegli il nome della politica che desideri allegare.
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 OUs (scegliere il) per trovare l'unità organizzativa o l'account che desideri.
5. Scegli Collega policy.

   L'elenco delle politiche dichiarative allegate nella scheda Target viene aggiornato per includere la nuova aggiunta. La modifica della policy diventa immediatamente effettiva.

Backup policies

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. Accedi alla AWS Organizations console . 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 OUs (scegliere il) per trovare l'unità organizzativa 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. Accedi alla AWS Organizations console . 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 OUs (scegliere il) per trovare l'unità organizzativa o l'account desiderato.
5. Scegli 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.

Tag policies

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 AWS Organizations console . 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 OUs (scegliere il) per trovare l'unità organizzativa 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 AWS Organizations console . 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 OUs (scegliere il) per trovare l'unità organizzativa o l'account desiderato.

5. Scegli 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.

Chat applications policies

È possibile allegare una policy per le applicazioni di chat accedendo alla policy o alla directory principale, all'unità organizzativa o all'account a cui si desidera allegare la policy.

Per allegare una policy relativa alle applicazioni di chat accedendo alla directory principale, all'unità organizzativa o all'account

1. Accedi alla AWS Organizations console . 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 OUs (scegliere l'opzione
   per trovare l'unità organizzativa o l'account desiderato.
3. Nella scheda Politiche, nella voce Politiche delle applicazioni di chat, scegli Allega.
4. Individua la policy desiderata e scegli Attach policy (Collega policy).

   L'elenco delle politiche delle applicazioni di chat allegate nella scheda Politiche viene aggiornato per includere la nuova aggiunta. La modifica della policy diventa immediatamente effettiva.

Per allegare una policy relativa alle applicazioni di chat accedendo alla policy

1. Accedi alla AWS Organizations console . 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 delle politiche del Chatbot, scegli il nome della politica che desideri allegare.
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 OUs (scegliere

l'opzione
per trovare l'unità organizzativa o l'account che desideri.

5. Scegli Collega policy.

   L'elenco delle politiche delle applicazioni di chat allegate nella scheda Target viene aggiornato per includere la nuova aggiunta. La modifica della policy diventa immediatamente effettiva.

AI services opt-out policies

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 AWS Organizations console . 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 OUs (scegliere l'opzione
   per trovare l'unità organizzativa 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 AWS Organizations console . 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 OUs (scegliere il) per trovare l'unità organizzativa o l'account desiderato.
5. Scegli 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.

Security Hub policies

È possibile allegare una policy di Security Hub accedendo alla policy o alla root, all'unità organizzativa o all'account a cui si desidera allegare la policy.

Per allegare una policy di Security Hub accedendo alla directory principale, all'unità organizzativa o all'account

1. Accedi alla AWS Organizations console . 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 OUs (scegliere il) per trovare l'unità organizzativa o l'account desiderato.
3. Nella scheda Criteri, nella voce relativa alle politiche di Security Hub, scegli Allega.
4. Individua la policy desiderata e scegli Attach policy (Collega policy).

   L'elenco dei criteri di Security Hub allegati nella scheda Politiche viene aggiornato per includere la nuova aggiunta. La modifica della policy diventa immediatamente effettiva.

Per allegare una policy di Security Hub accedendo alla policy

1. Accedi alla AWS Organizations console . 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 delle politiche di Security Hub, scegli il nome della politica che desideri allegare.
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 OUs (scegliere il) per trovare l'unità organizzativa o l'account che desideri.
5. Scegli Collega policy.

   L'elenco delle politiche del Security Hub allegate nella scheda Target viene aggiornato per includere la nuova aggiunta. La modifica della policy diventa immediatamente effettiva.

AWS CLI & AWS SDKs

Per allegare una politica

Gli esempi di codice seguenti mostrano come utilizzare `AttachPolicy`.

.NET

SDK per .NET

> **Note**
>
> C'è altro da fare GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
```

```
    /// Shows how to attach an AWS Organizations policy to an organization,
    /// an organizational unit, or an account.
    /// </summary>
    public class AttachPolicy
    {
        /// <summary>
        /// Initializes the Organizations client object and then calls the
        /// AttachPolicyAsync method to attach the policy to the root
        /// organization.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var policyId = "p-00000000";
            var targetId = "r-0000";

            var request = new AttachPolicyRequest
            {
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.AttachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully attached Policy ID {policyId} to
Target ID: {targetId}.");
            }
            else
            {
                Console.WriteLine("Was not successful in attaching the policy.");
            }
        }
    }
```

- Per i dettagli sull'API, consulta la AttachPolicysezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Per allegare una policy a una root, a un'unità organizzativa o a un account

Esempio 1

L'esempio seguente mostra come collegare una policy di controllo del servizio (SCP) a un'unità organizzativa:

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id ou-examplerootid111-exampleouid111
```

Esempio 2

L'esempio seguente mostra come allegare una politica di controllo del servizio direttamente a un account:

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id 333333333333
```

- Per i dettagli sull'API, consulta AttachPolicy AWS CLICommand Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
def attach_policy(policy_id, target_id, orgs_client):
    """
    Attaches a policy to a target. The target is an organization root, account,
 or
    organizational unit.
```

```
    :param policy_id: The ID of the policy to attach.
    :param target_id: The ID of the resources to attach the policy to.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.attach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Attached policy %s to target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't attach policy %s to target %s.", policy_id, target_id
        )
        raise
```

- Per i dettagli sull'API, consulta AttachPolicy AWSSDK for Python (Boto3) API Reference.

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

Separazione delle politiche organizzative con AWS Organizations

Questo argomento descrive come scollegare le politiche con. AWS Organizations Una policy definisce i controlli che si desidera applicare a un gruppo di Account AWS.

Argomenti

- Scollega le politiche con AWS Organizations

Scollega le politiche con AWS Organizations

> **Autorizzazioni minime**
>
> Per scollegare una policy dalla radice, dall'unità organizzativa o dall'account dell'organizzazione, è necessario disporre dell'autorizzazione per eseguire la seguente azione:
>
> - `organizations:DetachPolicy`

> **Note**
>
> Non è possibile scollegare l'ultima politica di autorizzazione (SCP o RCP) da una radice, un'unità organizzativa o un account. È necessario che sia sempre associato almeno un SCP e un RCP a ogni radice, unità organizzativa e account.

AWS Management Console

Service control policies (SCPs)

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 AWS Organizations console . 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 OUs (scegliere il ▶) per trovare l'unità organizzativa 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 degli allegati SCPs è 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 AWS Organizations console . 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 OUs (scegliere l'opzione ▶ per trovare l'unità organizzativa o l'account desiderato.
4. Seleziona Scollega.
5. Nella finestra di dialogo di conferma, scegli Detach (Scollega).

   L'elenco degli allegati SCPs è 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.

Resource control policies (RCPs)

È possibile scollegare un RCP accedendo alla policy o alla directory principale, all'unità organizzativa o all'account da cui si desidera scollegare la policy. Dopo aver scollegato un RCP da un'entità, tale RCP non si applica più alle risorse interessate dall'entità ora distaccata.

> **Note**
>
> Non è possibile scollegare la policy **`RCPFullAWSAccess`**
> La `RCPFullAWSAccess` policy viene allegata automaticamente alla directory principale, a ogni unità organizzativa e a ogni account dell'organizzazione. Non è possibile scollegare questa politica.

Per scollegare un RCP accedendo alla directory principale, all'unità organizzativa o all'account a cui è collegato

1. Accedi alla AWS Organizations console . 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 OUs (scegliere l'opzione
   per trovare l'unità organizzativa o l'account desiderato. Scegli il nome del root, dell'unità organizzativa o dell'account.
3. Nella scheda Politiche, scegli il pulsante di opzione accanto all'RCP che desideri scollegare, quindi scegli Scollega.
4. Nella finestra di dialogo di conferma, scegli Detach policy (Scollega policy).

   L'elenco degli allegati RCPs viene aggiornato. La modifica della politica causata dal distacco dell'RCP ha effetto immediato. Ad esempio, il distacco di un RCP influisce immediatamente sulle autorizzazioni degli utenti e dei ruoli IAM nell'account o negli account precedentemente collegati all'organizzazione principale o all'unità organizzativa precedentemente collegata.

Per scollegare un RCP accedendo alla policy

1. Accedi alla AWS Organizations console . 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 della politica di controllo delle risorse, scegli il nome della politica che desideri scollegare da una root, un'unità organizzativa 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 OUs (scegliere l'opzione
   per trovare l'unità organizzativa o l'account desiderato.
4. Seleziona Scollega.
5. Nella finestra di dialogo di conferma, scegli Detach (Scollega).

L'elenco degli allegati RCPs è aggiornato. La modifica della politica causata dal distacco dell'RCP ha effetto immediato. Ad esempio, il distacco di un RCP influisce immediatamente sulle autorizzazioni degli utenti e dei ruoli IAM nell'account o negli account precedentemente collegati all'organizzazione principale o all'unità organizzativa precedentemente collegata.

Declarative policies

È possibile scollegare una policy dichiarativa accedendo alla policy o alla directory principale, all'unità organizzativa o all'account da cui si desidera scollegare la policy.

Per scollegare una politica dichiarativa accedendo alla radice, all'unità organizzativa o all'account a cui è associata

1. Accedi alla AWS Organizations console . 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 OUs (scegliere l'opzione
per trovare l'unità organizzativa o l'account desiderato. Scegli il nome del root, dell'unità organizzativa o dell'account.
3. Nella scheda Politiche, scegli il pulsante di opzione accanto alla politica dichiarativa che desideri scollegare, quindi scegli Scollega.
4. Nella finestra di dialogo di conferma, scegli Detach policy (Scollega policy).

   L'elenco delle politiche dichiarative allegate viene aggiornato. La modifica della policy diventa immediatamente effettiva.

Per scollegare una politica dichiarativa accedendo alla politica

1. Accedi alla AWS Organizations console . 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 Politiche dichiarative, scegli il nome della politica che desideri scollegare da una radice, un'unità organizzativa 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 OUs (scegliere l'opzione
per trovare l'unità organizzativa o l'account desiderato.
4. Seleziona Scollega.
5. Nella finestra di dialogo di conferma, scegli Detach (Scollega).

   L'elenco delle politiche dichiarative allegate viene aggiornato. La modifica della policy diventa immediatamente effettiva.

Backup policies

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. Accedi alla AWS Organizations console . 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 OUs (scegliere l'opzione
per trovare l'unità organizzativa 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. Accedi alla AWS Organizations console . 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 OUs (scegliere il) per trovare l'unità organizzativa o l'account desiderato.
4. Seleziona 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.

Tag policies

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 AWS Organizations console . 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 OUs (scegliere il) per trovare l'unità organizzativa 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 AWS Organizations console . 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 OUs (scegliere il) per trovare l'unità organizzativa o l'account desiderato.
4. Seleziona 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.

Chat applications policies

Puoi scollegare una policy per le applicazioni di chat accedendo alla policy o alla directory principale, all'unità organizzativa o all'account da cui desideri scollegare la policy.

Per scollegare una policy per le applicazioni di chat accedendo alla directory principale, all'unità organizzativa o all'account a cui è associata

1. Accedi alla AWS Organizations console . 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 OUs (scegliere l'opzione

per trovare l'unità organizzativa o l'account desiderato. Scegli il nome del root, dell'unità organizzativa o dell'account.

3. Nella scheda Politiche, scegli il pulsante di opzione accanto alla politica delle applicazioni di chat che desideri scollegare, quindi scegli Scollega.
4. Nella finestra di dialogo di conferma, scegli Detach policy (Scollega policy).

   L'elenco delle politiche relative alle applicazioni di chat allegate viene aggiornato. La modifica della policy diventa immediatamente effettiva.

Per scollegare una policy per le applicazioni di chat accedendo alla policy

1. Accedi alla AWS Organizations console . 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 delle politiche del Chatbot, scegli il nome della politica che desideri scollegare da una root, un'unità organizzativa 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 OUs (scegliere l'opzione per trovare l'unità organizzativa o l'account che desideri.
4. Seleziona Scollega.
5. Nella finestra di dialogo di conferma, scegli Detach (Scollega).

   L'elenco delle politiche relative alle applicazioni di chat allegate è aggiornato. La modifica della policy diventa immediatamente effettiva.

AI services opt-out policies

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 AWS Organizations console . 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 OUs (scegliere l'opzione
   per trovare l'unità organizzativa 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 AWS Organizations console . 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 OUs (scegliere il)
   per trovare l'unità organizzativa o l'account desiderato.
4. Seleziona 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.

Security Hub policies

È possibile scollegare una policy di Security Hub accedendo alla policy o alla root, all'unità organizzativa o all'account da cui si desidera scollegare la policy.

Per scollegare una policy di Security Hub accedendo alla directory principale, all'unità organizzativa o all'account a cui è collegata

1. Accedi alla AWS Organizations console . 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 OUs (scegliere l'opzione
   per trovare l'unità organizzativa o l'account desiderato. Scegli il nome del root, dell'unità organizzativa o dell'account.
3. Nella scheda Politiche, scegli il pulsante di opzione accanto alla politica di Security Hub che desideri scollegare, quindi scegli Scollega.
4. Nella finestra di dialogo di conferma, scegli Detach policy (Scollega policy).

   L'elenco delle politiche del Security Hub allegate viene aggiornato. La modifica della policy diventa immediatamente effettiva.

Per scollegare una policy di Security Hub accedendo alla policy

1. Accedi alla AWS Organizations console . 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 delle politiche di Security Hub, scegli il nome della policy che desideri scollegare da una root, un'unità organizzativa 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 OUs (scegliere l'opzione
   per trovare l'unità organizzativa o l'account desiderato.
4. Seleziona Scollega.
5. Nella finestra di dialogo di conferma, scegli Detach (Scollega).

L'elenco delle politiche del Security Hub allegate viene aggiornato. La modifica della policy diventa immediatamente effettiva.

AWS CLI & AWS SDKs

Per allegare una politica

Gli esempi di codice seguenti mostrano come utilizzare `DetachPolicy`.

.NET

SDK per .NET

> **Note**
>
> C'è altro da fare GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to detach a policy from an AWS Organizations organization,
/// organizational unit, or account.
/// </summary>
public class DetachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and uses it to call
    /// DetachPolicyAsync to detach the policy.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-00000000";
        var targetId = "r-0000";
```

```
            var request = new DetachPolicyRequest
            {
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.DetachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully detached policy with Policy Id:
{policyId}.");
            }
            else
            {
                Console.WriteLine("Could not detach the policy.");
            }
        }
    }
```

- Per i dettagli sull'API, consulta la DetachPolicysezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Per scollegare una policy da una root, un'unità organizzativa o un account

L'esempio seguente mostra come scollegare una policy da un'unità organizzativa:

```
aws organizations  detach-policy  --target-id ou-examplerootid111-exampleouid111
 --policy-id p-examplepolicyid111
```

- Per i dettagli sull'API, vedere DetachPolicyin AWS CLI Command Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
def detach_policy(policy_id, target_id, orgs_client):
    """
    Detaches a policy from a target.

    :param policy_id: The ID of the policy to detach.
    :param target_id: The ID of the resource where the policy is currently
 attached.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.detach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Detached policy %s from target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't detach policy %s from target %s.", policy_id, target_id
        )
        raise
```

- Per i dettagli sull'API, consulta DetachPolicy AWSSDK for Python (Boto3) API Reference.

La modifica della policy ha effetto immediato e incide sulle autorizzazioni degli utenti, dei ruoli e delle risorse IAM, se applicabile, nell'account collegato o su tutti gli account sotto l'unità principale o l'unità organizzativa allegata.

Ottenere informazioni sulle policy dell'organizzazione

Questo argomento descrive vari modi per ottenere dettagli sulle politiche dell'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.

Argomenti

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 politiche della propria organizzazione in AWS Management Console o utilizzando un comando AWS Command Line Interface (AWS CLI) o un'operazione AWS SDK.

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

Gli esempi di codice seguenti mostrano come utilizzare `ListPolicies`.

.NET

SDK per .NET

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to list the AWS Organizations policies associated with an
/// organization.
/// </summary>
public class ListPolicies
{
    /// <summary>
    /// Initializes an Organizations client object, and then calls its
    /// ListPoliciesAsync method.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        // The value for the Filter parameter is required and must must be
        // one of the following:
        //     AISERVICES_OPT_OUT_POLICY
        //     BACKUP_POLICY
        //     SERVICE_CONTROL_POLICY
        //     TAG_POLICY
```

```
            var request = new ListPoliciesRequest
            {
                Filter = "SERVICE_CONTROL_POLICY",
                MaxResults = 5,
            };

            var response = new ListPoliciesResponse();
            try
            {
                do
                {
                    response = await client.ListPoliciesAsync(request);
                    response.Policies.ForEach(p => DisplayPolicies(p));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (AWSOrganizationsNotInUseException ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about the Organizations policies associated
        /// with an organization.
        /// </summary>
        /// <param name="policy">An Organizations policy summary to display
        /// information on the console.</param>
        private static void DisplayPolicies(PolicySummary policy)
        {
            string policyInfo = $"{policy.Id}
{policy.Name}\t{policy.Description}";

            Console.WriteLine(policyInfo);
        }
    }
```

- Per i dettagli sull'API, consulta la ListPoliciessezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Per recuperare un elenco di tutte le politiche in un'organizzazione di un determinato tipo

L'esempio seguente mostra come ottenere un elenco di SCPs, come specificato dal parametro filter:

```
aws organizations list-policies --filter SERVICE_CONTROL_POLICY
```

L'output include un elenco di politiche con informazioni di riepilogo:

```
{
        "Policies": [
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllS3Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid111",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Enables account admins to delegate
 permissions for any S3 actions to users and roles in their accounts."
                },
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllEC2Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid222",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid222",
                        "Description": "Enables account admins to delegate
 permissions for any EC2 actions to users and roles in their accounts."
                },
                {
                        "AwsManaged": true,
                        "Description": "Allows access to every operation",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-FullAWSAccess",
                        "Arn": "arn:aws:organizations::aws:policy/
service_control_policy/p-FullAWSAccess",
                        "Name": "FullAWSAccess"
```

```
                }
        ]
}
```

- Per i dettagli sull'API, vedere ListPoliciesin AWS CLI Command Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
def list_policies(policy_filter, orgs_client):
    """
    Lists the policies for the account, limited to the specified filter.

    :param policy_filter: The kind of policies to return.
    :param orgs_client: The Boto3 Organizations client.
    :return: The list of policies found.
    """
    try:
        response = orgs_client.list_policies(Filter=policy_filter)
        policies = response["Policies"]
        logger.info("Found %s %s policies.", len(policies), policy_filter)
    except ClientError:
        logger.exception("Couldn't get %s policies.", policy_filter)
        raise
    else:
        return policies
```

- Per i dettagli sull'API, consulta ListPolicies AWSSDK for Python (Boto3) API Reference.

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 OUs (scegliere la) per trovare l'unità organizzativa 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
        }
    ]
}
```

- AWS SDKs: ListPoliciesForTarget

Elenca tutte OUs le radici e gli account a cui è associata una politica

> **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 tutte le radici e OUs gli account a cui è allegata una politica specificata

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 tutte le radici e OUs gli account a cui è allegata una politica specificata

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

- AWS CLI: list-targets-for-policy

  L'esempio seguente mostra tutti gli allegati a root e OUs gli account per la politica 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"
```

```
        }
    ]
}
```

- AWS SDKs: 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 Target mostra un elenco delle radici e degli account a cui è associata la politica. OUs
   - 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

Gli esempi di codice seguenti mostrano come utilizzare `DescribePolicy`.

CLI

AWS CLI

Per ottenere informazioni su una politica

L'esempio seguente mostra come richiedere informazioni su una politica:

```
aws organizations describe-policy --policy-id p-examplepolicyid111
```

L'output include un oggetto politico che contiene dettagli sulla politica:

```
{
        "Policy": {
                "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement
\": [\n    {\n      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n
 \"Resource\": \"*\"\n    }\n  ]\n}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::111111111111:policy/o-
exampleorgid/service_control_policy/p-examplepolicyid111",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-examplepolicyid111",
                        "AwsManaged": false,
                        "Name": "AllowAllS3Actions",
                        "Description": "Enables admins to delegate S3
 permissions"
                }
        }
}
```

- Per i dettagli sull'API, vedere DescribePolicyin AWS CLI Command Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
def describe_policy(policy_id, orgs_client):
    """
    Describes a policy.

    :param policy_id: The ID of the policy to describe.
    :param orgs_client: The Boto3 Organizations client.
    :return: The description of the policy.
    """
    try:
        response = orgs_client.describe_policy(PolicyId=policy_id)
        policy = response["Policy"]
        logger.info("Got policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't get policy %s.", policy_id)
        raise
    else:
        return policy
```

- Per i dettagli sull'API, consulta DescribePolicy AWSSDK for Python (Boto3) API Reference.

Eliminazione delle politiche organizzative con AWS Organizations

Quando non hai più bisogno di una politica e dopo averla scollegata da tutte le unità organizzative (OUs) e dagli account, puoi eliminarla.

Questo argomento descrive come eliminare le politiche con AWS Organizations. Una politica definisce i controlli che si desidera applicare a un gruppo di Account AWS.

Argomenti

Elimina le politiche con AWS Organizations

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.

> **Note**
>
> - Non è possibile eliminare alcun SCP AWS gestito, ad esempio l'SCP denominato. `FullAWSAccess`
> - Non è possibile eliminare alcun RCP AWS gestito come l'RCP denominato. `RCPFullAWSAccess`

> **Autorizzazioni minime**
>
> Per eliminare una politica, è necessaria l'autorizzazione per eseguire la seguente azione:
>
> - `organizations:DeletePolicy`

AWS Management Console

Service control policies (SCPs)

Per eliminare una SCP

1. Accedi alla AWS Organizations console . 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 innanzitutto necessario scollegare la politica che si desidera eliminare da tutte le radici e OUs 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).

Resource control policies (RCPs)

Per eliminare un RCP

1. Accedi alla AWS Organizations console . 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 Politiche di controllo delle risorse, scegli il nome dell'RCP che desideri eliminare.
3. È innanzitutto necessario scollegare la politica che si desidera eliminare da tutte le radici e OUs 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).

Declarative policies

Per eliminare una politica dichiarativa

1. Accedi alla AWS Organizations console . 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 Politiche dichiarative, scegli il nome della politica che desideri eliminare.
3. È innanzitutto necessario scollegare la politica che si desidera eliminare da tutte le radici e OUs 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).

Backup policies

Per eliminare una policy di backup

1. Accedi alla AWS Organizations console . 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 innanzitutto necessario scollegare la politica di backup che si desidera eliminare da tutte le radici e OUs 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).

Tag policies

Per eliminare una policy di tag

1. Accedi alla AWS Organizations console . 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 delle politiche relative ai tag, scegli la politica che desideri eliminare.
3. Devi prima scollegare la politica che desideri eliminare da tutte le radici e OUs 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).

Chat applications policies

Per eliminare una politica relativa alle applicazioni di chat

1. Accedi alla AWS Organizations console . 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 delle politiche del Chatbot, scegli il nome della politica che desideri eliminare.
3. Devi prima scollegare la politica che desideri eliminare da tutte le radici e OUs 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).

AI services opt-out policies

Per eliminare una policy di rifiuto dei servizi di IA

1. Accedi alla AWS Organizations console . 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 innanzitutto necessario scollegare la politica che si desidera eliminare da tutte le radici e OUs 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).

Security Hub policies

Per eliminare una politica del Security Hub

1. Accedi alla AWS Organizations console . 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 delle politiche di Security Hub, scegli il nome della politica che desideri eliminare.
3. È innanzitutto necessario scollegare la politica che si desidera eliminare da tutte le radici e OUs 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 politica pubblicitaria

Gli esempi di codice seguenti mostrano come utilizzare `DeletePolicy`.

.NET

SDK per .NET

> **Note**
>
> C'è altro da fare GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
```

```
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Deletes an existing AWS Organizations policy.
/// </summary>
public class DeletePolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// delete the policy with the specified policyId.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-00000000";

        var request = new DeletePolicyRequest
        {
            PolicyId = policyId,
        };

        var response = await client.DeletePolicyAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
            Console.WriteLine($"Successfully deleted Policy: {policyId}.");
        }
        else
        {
            Console.WriteLine($"Could not delete Policy: {policyId}.");
        }
    }
}
```

- Per i dettagli sull'API, consulta la DeletePolicysezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Per eliminare una politica

L'esempio seguente mostra come eliminare una politica da un'organizzazione. L'esempio presuppone che in precedenza sia stata scollegata la politica da tutte le entità:

```
aws organizations delete-policy --policy-id p-examplepolicyid111
```

- Per i dettagli sull'API, consulta AWS CLI Command DeletePolicyReference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
def delete_policy(policy_id, orgs_client):
    """
    Deletes a policy.

    :param policy_id: The ID of the policy to delete.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.delete_policy(PolicyId=policy_id)
        logger.info("Deleted policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't delete policy %s.", policy_id)
        raise
```

- Per i dettagli sull'API, consulta DeletePolicy AWSSDK for Python (Boto3) API Reference.

Taggare le risorse AWS Organizations

Un tag è un'etichetta di attributo personalizzata che si aggiunge a una AWS risorsa 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 Practices for Tagging AWS Resources.

> **Tip**
>
> Puoi utilizzare le policy di tag per standardizzare i tag tra le risorse degli account dell'organizzazione.

Argomenti

Considerazioni

AWS Organizations supporta le seguenti operazioni di tagging quando si accede all'account di gestione:

È possibile aggiungere tag alle seguenti risorse dell'organizzazione

- Account AWS
- Unità organizzative
- Il root dell'organizzazione
- Policy

È possibile aggiungere tag nei seguenti orari

- 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`.

Altre considerazioni

È possibile visualizzare i tag su qualsiasi risorsa taggabile utilizzando la console o chiamando l'`ListTagsForResource`operazione. AWS Organizations

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 controllo dei servizi
  - Politica di controllo delle risorse
  - Politica dichiarativa
  - Policy di backup
  - Policy di tag
  - Politica sulle applicazioni di chat
  - Policy di rifiuto dei servizi di IA

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 AWS Organizations console . 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. Scegli Save changes (Salva 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
- AWS SDKs: TagResource

Per eliminare tag da una risorsa nell'organizzazione

Per eliminare i tag, puoi utilizzare uno dei seguenti comandi:

- AWS CLI: untag-resource
- AWS SDKs: UntagResource

Approvazione multipartitica per AWS Organizations

L'approvazione multipartitica è una funzionalità AWS Organizationsche consente di proteggere un elenco predefinito di operazioni attraverso un processo di approvazione distribuito. Utilizza l'approvazione multipartitica per stabilire flussi di lavoro di approvazione e trasformare i processi di sicurezza in decisioni basate sul team.

Quando utilizzare l'approvazione multipartitica:

- È necessario allinearsi al principio Zero Trust secondo cui «mai fidarsi, verificare sempre»
- Devi assicurarti che le persone giuste abbiano accesso alle cose giuste nel modo giusto
- È necessario un processo decisionale distribuito per operazioni sensibili o critiche
- È necessario proteggersi da operazioni indesiderate su risorse sensibili o critiche
- Sono necessarie revisioni e approvazioni formali per motivi di controllo o conformità

Per ulteriori informazioni, consulta Cos'è l'approvazione multipartitica nella Guida per l'utente all'approvazione multipartitica.

Utilizzo AWS Organizations con altri Servizi AWS

È possibile utilizzare l'accesso affidabile per consentire a un AWS servizio supportato specificato dall'utente, denominato servizio affidabile, di eseguire attività all'interno dell'organizzazione e dei relativi account per conto dell'utente. 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

Ti consigliamo vivamente, quando l'opzione è disponibile, di abilitare e disabilitare l'accesso affidabile utilizzando solo la console del servizio affidabile o gli equivalenti operativi della AWS CLI stessa o dell'API. 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 Servizi AWS che puoi usare 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 affidabile richiede le autorizzazioni per due servizi: AWS Organizations e il servizio affidabile. Per abilitare l'accesso sicuro, scegli uno dei seguenti scenari:

- Se disponi di credenziali con autorizzazioni per entrambi AWS Organizations e per il servizio affidabile, abilita l'accesso utilizzando gli strumenti (console o AWS CLI) forniti dal servizio affidabile. Ciò consente al servizio di abilitare l'accesso affidabile per conto dell'utente e di creare tutte le risorse necessarie affinché il servizio funzioni all'interno dell'organizzazione. AWS Organizations

  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`— Obbligatorio se si utilizza la AWS Organizations console.
  - Le autorizzazioni minime necessarie per il servizio sicuro dipende dal servizio. Per ulteriori informazioni, consulta la documentazione del servizio sicuro.

- Se una persona dispone di credenziali con autorizzazioni AWS Organizations ma qualcun altro possiede credenziali con autorizzazioni nel servizio affidabile, esegui questi passaggi nell'ordine seguente:

  1. La persona che dispone di credenziali con autorizzazioni AWS Organizations deve utilizzare la AWS Organizations console, l'SDK o un AWS SDK per abilitare l' AWS CLI accesso affidabile per il servizio affidabile. Ciò autorizza l'altro servizio a eseguire la configurazione richiesta nell'organizzazione quando viene eseguito il seguente passaggio (passaggio 2).

     Le AWS Organizations autorizzazioni minime sono le seguenti:

     - `organizations:EnableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization`— Richiesto solo se si utilizza la console AWS Organizations

     Per i passaggi per abilitare l'accesso affidabile in AWS Organizations, vediCome 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 Servizi AWS che puoi usare 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 impedire completamente a utenti e ruoli di accedere a un AWS servizio, puoi rimuovere le autorizzazioni IAM che concedono tale accesso oppure puoi utilizzare le policy di controllo del servizio (SCPs) in AWS Organizations.

Puoi candidarti solo SCPs agli account dei membri. SCPs non si applicano all'account di gestione. Ti consigliamo di non eseguire servizi nell'account di gestione. Eseguili invece negli account dei membri in cui puoi controllare la sicurezza utilizzando SCPs.

- Se disponi di credenziali con autorizzazioni AWS Organizations sia per il servizio affidabile che per il servizio affidabile, disabilita l'accesso utilizzando gli strumenti (console o AWS CLI) disponibili per il servizio affidabile. 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`— Obbligatorio se si utilizza la AWS Organizations console.
  - Le autorizzazioni minime necessarie per il servizio sicuro dipendono dal servizio. Per ulteriori informazioni, consulta la documentazione del servizio sicuro.
- Se le credenziali con autorizzazioni AWS Organizations non sono le credenziali con autorizzazioni nel servizio affidabile, esegui questi passaggi nell'ordine seguente:

  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 Servizi AWS che puoi usare con AWS Organizations.
  2. La persona con le autorizzazioni AWS Organizations può quindi utilizzare la AWS Organizations console o un AWS SDK per disabilitare l'accesso al servizio affidabile. AWS CLI Ciò rimuove le autorizzazioni per il servizio sicuro dall'organizzazione e dal relativo account.

     Le AWS Organizations autorizzazioni minime sono le seguenti:

     - `organizations:DisableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization`— Richiesto solo se si utilizza la console AWS Organizations

     Per i passaggi per disabilitare l'accesso affidabile in AWS Organizations, vedereCome abilitare o disabilitare l'accesso sicuro.

Come abilitare o disabilitare l'accesso sicuro

Se disponi solo delle autorizzazioni AWS Organizations e desideri abilitare o disabilitare l'accesso affidabile alla tua organizzazione per conto dell'amministratore dell'altro AWS servizio, utilizza la procedura seguente.

Important

Ti consigliamo vivamente, quando l'opzione è disponibile, di abilitare e disabilitare l'accesso affidabile utilizzando solo la console del servizio affidabile o gli equivalenti operativi della AWS CLI stessa o dell'API. 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 Servizi AWS che puoi usare 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 AWS servizio.

AWS Management Console

Per abilitare l'accesso al servizio attendibile

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 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, comunica all'amministratore dell'altro AWS servizio che ora può abilitare l'utilizzo dell'altro servizio AWS Organizations.

Per disabilitare l'accesso al servizio attendibile

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 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 AWS CLI comandi o operazioni API per abilitare o disabilitare l'accesso affidabile ai servizi:

- AWS CLI: AWS organizzazioni enable-aws-service-access
- AWS CLI: AWS organizzazioni disable-aws-service-access
- AWS API: Abilita AWSService l'accesso
- AWS API: disabilita AWSService l'accesso

AWS Organizations e ruoli collegati ai servizi

AWS Organizations utilizza ruoli collegati ai servizi IAM per consentire ai servizi affidabili di eseguire attività per tuo conto negli account dei membri della tua 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 AWS Organizations servizio stesso può assumere questo ruolo. Il ruolo dispone di autorizzazioni che consentono di AWS Organizations creare ruoli collegati al servizio 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 al servizio 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**
>
> AWS Organizations SCPs non influiscono mai sui ruoli collegati ai servizi. Questi ruoli sono esenti da qualsiasi restrizione SCP.

Utilizzo del ruolo AWSService RoleForDeclarativePolicies EC2 Report collegato al servizio

Il ruolo `AWSServiceRoleForDeclarativePoliciesEC2Report` collegato al servizio viene utilizzato da Organizations per descrivere gli stati degli attributi degli account per gli account dei membri per creare report Declarative Policies. Le autorizzazioni del ruolo sono definite in. AWS politica gestita: DeclarativePoliciesEC2Report

Servizi AWS che puoi usare con AWS Organizations

Con AWS Organizations puoi eseguire attività di gestione degli account a larga scala, consolidando più Account AWS in un'unica organizzazione. Il consolidamento degli account semplifica il modo in cui utilizzi gli altri. Servizi AWS Puoi sfruttare i servizi di gestione multi-account disponibili in

AWS Organizations select Servizi AWS per eseguire attività su tutti gli account membri della tua organizzazione.

La tabella seguente elenca i servizi Servizi AWS che è possibile utilizzare e AWS Organizations i vantaggi derivanti dall'utilizzo di ciascun servizio a livello di organizzazione.

Accesso attendibile - Puoi abilitare un AWS servizio compatibile per eseguire operazioni su tutti Account AWS gli dell'organizzazione. Per ulteriori informazioni, consulta Utilizzo AWS Organizations con altri Servizi AWS.

Amministratore delegato per Servizi AWS - Un AWS servizio compatibile può registrare un account AWS membro nell'organizzazione come amministratore per gli account dell'organizzazione in tale servizio. Per ulteriori informazioni, consulta Amministratore delegato per Servizi AWS quel lavoro con Organizations.

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
Gestione dell'account AWS Gestisci i dettagli e i metadati per tutti gli Account AWS per la tua organizzazione.	Gestisci i dettagli dell'account, i contatti alternativi e le regioni per tutti i membri della tua 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 Application Migration Service AWS Application Migration Service consente alle aziende di lift-and-shift accedere a AWS un gran numero di server fisici, virtuali o cloud senza problemi di compatibilità, interruzioni delle prestazioni o lunghe finestre di conversione.	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	
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	 No	

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 AWS l'utilizzo di in più account nell'organizzazione e per semplificare le modalità di valutazione dei rischi 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 (OUs). 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
AWS Billing and Cost Management Fornisce una panoramica dei dati di gestione finanziaria del AWS cloud e consente di prendere decisioni più rapide e informate.	Consente la suddivisione dei dati di allocazione dei costi per recuperare AWS Organizations informazioni, se applicabile, e raccogliere dati di telemetria per i servizi di dati di allocazione dei costi suddivisa che hai scelto.	 Sì Ulteriori informazioni	 No

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	Per ulteriori informazioni, consulta Cos'è? AWS Billing and Cost Management nella guida per l'utente di Billing and Cost Management.			

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	
Amazon CloudWatch Monitora in tempo reale le AWS risorse e le applicazioni AWS in esecuzione su. Puoi utilizzare lo CloudWatch per raccogliere e tenere traccia dei parametri, che sono delle variabili che si possono misurare per le risorse e le applicazioni.	L'integrazione con Organizations ha due vantaggi in CloudWatch. Innanzitutto, grazie CloudWatch all'integrazione con Organizations, puoi scoprire e comprendere lo stato della configurazione di telemetria per AWS le tue risorse da una vista centrale	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	nella console. CloudWatch In secondo luogo, quando è possibile utilizzare Network Flow Monitor CloudWatch per ottenere visibilità sulle metriche delle prestazioni di rete, mediante l'integrazione con Organizations, è possibile visualizz			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	are le informazioni sulle prestazioni di rete per le risorse in più account anziché in un solo account.			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
AWS Compute Optimizer Ottieni consigli per l' AWS ottimizzazione dell'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 le regole e i pacchetti di conformità per tutti gli	 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	
	Account AWS nell'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 Organizat			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	ions. Per ulteriori 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 impostare una zona di destinazione, un ambiente con più account per tutte le AWS risorse. Questo ambiente include un'organizzazione e le entità dell'organizzazione. Puoi utilizzare questo ambiente per applicare le normative di	 Sì Ulteriori informazioni	 No	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	conformità su 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	 Sì Ulteriori informazioni	

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.	È possibile integrare Amazon Detective con AWS Organizations per garantire che il grafico del comportamento di Amazon Detective fornisca visibilità sull'attività per tutti gli 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	
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 ricevono una notifica quando DevOps Guru rileva un problema operativo o un rischio.	È possibile eseguire l'integrazione con AWS Organizations per gestire le informazioni dettagliate da tutti gli account dell'intera organizzazione. È possibile delegare un amministratore per visualizzare, ordinare e filtrare le informazioni da	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	tutti gli account per ottenere lo stato di 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 in tempo reale le AWS risorse e le applicazioni AWS in esecuzione su.	Puoi abilitare la condivisione di tutti EventBridge gli eventi Amazon, precedentemente CloudWatch Eventi Amazon su tutti gli account dell'organizzazione. Per ulteriori informazioni, consulta Invio e ricezione di EventBridge eventi	 No	 No	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	Amazon tra due Account AWS nella Amazon EventBridge User Guide.			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
Amazon Elastic Compute Cloud Amazon VPC Address Manager (IPAM) fornisce capacità di calcolo scalabile on demand nel cloud. AWS	Consenti all'amministratore di Organizations di creare un rapporto sulla configurazione esistente per gli account dell'organizzazione e quando utilizzi la funzionalità delle politiche dichiarative.	 Sì Ulteriori informazioni	 No	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato
Amazon Elastic Kubernetes Service La dashboard di Amazon EKS offre visibilità e gestione aggregate dei cluster Kubernetes nel cloud. AWS	Consenti all'amministratore di Organizations di visualizzare i dati consolidati del dashboard sulle risorse del cluster, tra cui la distribuzione delle versioni, lo stato di integrità e i requisiti di aggiornamento all'interno 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 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 in modo centralizzato AWS WAF regole su tutti gli account nella 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 origini 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 GuardDuty affinché visualizzi e gestisca tutti gli account dell'organizzazione. L'aggiunta di account membri abilita GuardDuty automaticamente tali account nella selezionata 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 per i nuovi account aggiunti all'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 per Servizi AWS.	Puoi aggregare AWS Health gli eventi tra 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 Identity and Access Management Controlla in modo sicuro l'accesso alle AWS risorse.	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. Puoi utilizzare questi dati per creare e aggiornare le policy di controllo dei servizi (SCPs) che	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	limitano l'accesso esclusivamente ai AWS servizi 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	
	La gestione degli accessi root di IAM consente di gestire centralmente le credenziali dell'utente root e completare attività con privilegi sugli account membri.			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
IAM Access Analyzer Analizza le policy basate su risorse nell'AWS ambiente per identificare eventuali policy che consentano l'accesso a un'entità esterna all'area di attendibilità.	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 Eseguire una scansione automatica AWS dei carichi di lavoro alla ricerca di vulnerabilità per scoprire le EC2 istanze di Amazon e le immagini dei container che risiedono in Amazon ECR per vulnerabilità software e esposizione non intenzionale 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	
AWS Managed Services (AMS) Self-Service Reporting (SSR) Raccoglie dati da vari AWS servizi nativi e fornisce l'accesso ai report sulle principali offerte AMS. SSR fornisce le informazioni che è possibile utilizzare per supportare le operazioni, la gestione della configurazione, la gestione delle risorse, la gestione della sicurezza e la conformità.	È possibile abilitare Aggregated SSR, una funzionalità che consente ai clienti di visualizzare report self-service consolidati in tutta l'organizzazione tramite il proprio account di gestione o un account amministratore delegato.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

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 gli Marketplace AWS abbonamenti e gli acquisti negli account nell'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 uno o più o più account dell'organizzazione e OUs, ciascuno con il proprio set di prodotti approvati. AWS Gli amministratori possono anche applicare	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	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	
Marketplace AWS dashboard di approfondimenti sugli acquisti Ti consente di visualizzare i dati sugli accordi e sull'analisi dei costi per tutti gli Marketplace AWS acquisti tra gli AWS account della tua organizzazione.	Marketplace AWS La dashboard di Procurement Insights ascolta le modifiche organizzative, ad esempio l'ingresso di un account nell'organizzazione, e aggrega i dati relativi ai contratti corrispondenti per creare dashboard.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
AWS Network Manager Ti consente di gestire centralmente la tua rete core WAN di AWS Cloud e la tua rete di AWS Transit Gateway su AWS account, regioni e posizioni on-premise.	Puoi gestire e monitorare centralmente le reti globali con gateway di transito e le relative risorse collegate in più AWS account all'interno dell'organizzazione.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato
Amazon Q Developer Amazon Q Developer è un assistente conversazionale basato sull'IA generativa che permette di comprendere, creare, estendere e utilizzare al meglio le applicazioni. AWS	La versione in abbonamento a pagamento di Amazon Q Developer richiede l'integrazione di Organizations.	 Sì Ulteriori informazioni	 No

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 Amazon EC2 User Guide o la Amazon EC2 User Guide. Per un elenco delle risorse condivisibili, consulta Risorse condivisibili nella Guida per l'utente			

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	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 lo stato di sicurezza in AWS e controlla l'ambiente rispetto agli standard di sicurezza e alle best practice del settore.	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	
AWS Risposta agli incidenti di sicurezza AWS servizio di sicurezza che fornisce supporto in tempo reale, 24 ore su 24, 7 giorni su 7, in caso di incidenti di sicurezza con assistenza umana, per aiutare i clienti a rispondere rapidamente agli incidenti di sicurezza informatica come il furto di credenziali e gli attacchi ransomware.	Copertura di sicurezza per l'intera 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.	Puoi condividere portafogli e copiare prodotti su più account più facilmente, senza condividere il portafoglio IDs.	 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 nel loro account di gestione o membro assegnato.	 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 AWS risorse.	Puoi sincronizzare i dati delle operazioni tra tutti gli Account AWS dell'organizzazione utilizzando Systems Manager Explorer. Ora puoi gestire modelli di modifica, approvazioni e report per tutti gli account membri dell'organizzazione da un	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

AWS servizio	Vantaggi dell'utilizzo con AWS Organizations	Supporta l'accesso attendibile	Supporta l'amministratore delegato	
	account di amministratore delegato utilizzando Systems Manager Change Manager.			
Notifiche all'utente AWS Una posizione centrale per le AWS notifiche.	Puoi configurare e visualizzare le notifiche centralmente su 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	
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 analizza AWS l'ambiente 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.	Esegui i Trusted Advisor controlli per tutti gli Account AWS 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 Well-Architected Tool Lo AWS Well-Architected Tool aiuta a documentare lo stato dei carichi di lavoro e a confrontarli con quelli più recenti best practice AWS architettoniche di.	Consente ai clienti dello AWS WA Tool e di Organizations di semplificare il processo di condivisione AWS WA Tool delle risorse dello con altri membri della loro 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 caratteristica del VPC che semplifica la pianificazione, il tracciamento 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 (). VPCs	Tieni traccia dei percorsi tra gli account delle tue organizzazioni.	 Sì Ulteriori informazioni	 Sì Ulteriori informazioni	

Gestione dell'account AWS e AWS Organizations

Gestione dell'account AWS ti aiuta a gestire le informazioni e i metadati dell'account per tutti i membri Account AWS della 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 Gestione dell'account AWS nell'organizzazione nella Gestione dell'account AWS Guida per l'utente.

Utilizza le seguenti informazioni per semplificare l'integrazione Gestione dell'account AWS 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.

Account Management richiede un accesso affidabile AWS Organizations prima di poter designare un account membro come amministratore delegato di questo servizio per l'organizzazione.

Puoi abilitare l'accesso affidabile solo utilizzando gli strumenti Organizations.

È possibile abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in uno dei AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli Gestione dell'account AWSnell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di Gestione dell'account AWS dialogo Abilita accesso affidabile per, digita enable per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore Gestione dell'account AWS che ora può abilitare il funzionamento del servizio AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitarlo Gestione dell'account AWS come servizio affidabile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: Abilita AWSService l'accesso

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 dell'account di AWS Organizations gestione può disabilitare l'accesso affidabile con Gestione dell'account AWS.

Puoi disabilitare l'accesso affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli Gestione dell'account AWSnell'elenco dei servizi.
4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Nella finestra di Gestione dell'account AWS dialogo Disabilita l'accesso affidabile per, digita disabilita per confermare, quindi scegli Disabilita accesso affidabile.

6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore Gestione dell'account AWS che ora può disabilitare il funzionamento di quel servizio AWS Organizations utilizzando la console o gli strumenti di servizio.

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

  Esegui il comando seguente per disabilitarlo Gestione dell'account AWS come servizio affidabile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: disabilita AWSService l'accesso

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 Crea una politica di delega basata sulle risorse con AWS Organizations.

AWS CLI, AWS API

Se desideri configurare un account amministratore delegato utilizzando la AWS CLI o uno dei seguenti, puoi utilizzare AWS SDKs i seguenti comandi:

- AWS CLI:

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

AWS Application Migration Service (Servizio di migrazione delle applicazioni) e AWS Organizations

AWS Application Migration Service semplifica, accelera e riduce i costi di 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 la guida per l'utente di Configuration up your AWS Organizations in the Application Migration Service.

Utilizza le seguenti informazioni per semplificare l'integrazione AWS Application Migration Service 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 Application Migration Service 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 Application Migration Service e Organizations o se si rimuove l'account membro dall'organizzazione.

- `AWSServiceRoleForApplicationMigrationService`

Principali del servizio utilizzati da Application Migration Service

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 Application Migration Service garantiscono l'accesso ai seguenti principali di servizio:

- `mgn.amazonaws.com`

Abilitazione dell'accesso affidabile con Application Migration Service

Quando abiliti l'accesso affidabile con Application Migration Service, puoi utilizzare la funzionalità di visualizzazione globale, che consente di gestire migrazioni su larga scala su più account. La visualizzazione globale offre visibilità e la possibilità di eseguire azioni specifiche su server di origine, app e wave in diversi AWS account. Per ulteriori informazioni, consulta Setting up your AWS Organizations nella guida AWS Application Migration Service per l'utente.

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

È possibile abilitare l'accesso affidabile utilizzando la AWS Application Migration Service console o la AWS Organizations console.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS Application Migration Service console o gli strumenti per abilitare l'integrazione con Organizations. Ciò consente di AWS Application Migration Service eseguire qualsiasi configurazione richiesta, ad esempio la creazione delle risorse necessarie al servizio. Procedi con questi passaggi solo se non è possibile abilitare l'integrazione utilizzando gli strumenti forniti da AWS Application Migration Service. Per ulteriori informazioni, consulta questa nota.
> Se abiliti l'accesso affidabile utilizzando la AWS Application Migration Service console o gli strumenti, non è necessario completare questi passaggi.

Puoi abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in uno dei AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Application Migration Servicenell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di AWS Application Migration Service dialogo Abilita accesso affidabile per, digita enable per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS Application Migration Service che ora può abilitare il funzionamento del servizio AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitarlo AWS Application Migration Service come servizio affidabile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: Abilita AWSService l'accesso

Disabilitazione dell'accesso affidabile con Application Migration Service

Solo un amministratore dell'account di gestione Organizations può disabilitare l'accesso affidabile con Application Migration Service.

È possibile disabilitare l'accesso affidabile utilizzando gli AWS Organizations strumenti AWS Application Migration Service o.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS Application Migration Service console o gli strumenti per disabilitare l'integrazione con Organizations. Ciò consente di AWS Application Migration Service eseguire tutte le operazioni di pulizia necessarie, ad esempio l'eliminazione di risorse o l'accesso a ruoli che non sono più necessari al servizio. Procedi con questi passaggi solo se non è possibile disabilitare l'integrazione utilizzando gli strumenti forniti da AWS Application Migration Service.
> Se disabiliti l'accesso affidabile utilizzando la AWS Application Migration Service console o gli strumenti, non è necessario completare questi passaggi.

È possibile disabilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Application Migration Servicenell'elenco dei servizi.
4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Nella finestra di AWS Application Migration Service dialogo Disabilita l'accesso affidabile per, digita disabilita per confermare, quindi scegli Disabilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS Application Migration Service che ora può disabilitare il funzionamento di quel servizio AWS Organizations utilizzando la console o gli strumenti di servizio.

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

  Esegui il comando seguente per disabilitarlo AWS Application Migration Service come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal mgn.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: disabilita AWSService l'accesso

Abilitazione di un account amministratore delegato per Application Migration Service

Quando si designa un account membro come amministratore delegato dell'organizzazione, gli utenti e i ruoli di tale account possono eseguire azioni amministrative per Application Migration Service che altrimenti possono essere eseguite solo da utenti o ruoli nell'account di gestione dell'organizzazione. Ciò consente di separare la gestione dell'organizzazione dalla gestione di Application Migration Service. Per ulteriori informazioni, consulta la guida utente di Configurazione dell'applicazione AWS Organizations all'interno dell'Application Migration Service.

> **Autorizzazioni minime**
>
> Solo un utente o un ruolo nell'account di gestione Organizations può configurare un account membro come amministratore delegato per Application Migration Service nell'organizzazione.

AWS CLI, AWS API

Se desideri configurare un account amministratore delegato utilizzando la AWS CLI o uno dei seguenti, puoi utilizzare AWS SDKs i seguenti comandi:

- AWS CLI:

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

- AWS SDK: richiama l'`RegisterDelegatedAdministrator`operazione Organizations e il numero ID dell'account membro e identifica il servizio dell'account `mgn.amazonaws.com` come parametri.

Disabilitazione di un amministratore delegato per Application Migration Service

Solo un amministratore dell'account di gestione Organizations può rimuovere un amministratore delegato per Application Migration Service. 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 report AWS sulla conformità alla sicurezza come report ISO e PCI. Utilizzando AWS Artifact, un utente dell'account di gestione dell'organizzazione può accettare automaticamente gli accordi per conto di tutti gli account membri di un'organizzazione, anche quando vengono aggiunti nuovi report e account. Glu utenti degli account membri possono visualizzare e scaricare gli accordi. Per ulteriori informazioni, consulta Gestire un contratto per più account in AWS Artifact nella AWS Artifact Guida per l'utente.

Utilizza le seguenti informazioni per aiutarti a eseguire l'integrazione 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. Questo ruolo consente di AWS Artifact 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 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 di 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 affidabile solo utilizzando gli strumenti Organizations.

È possibile abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in uno dei AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Artifactnell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di AWS Artifact dialogo Abilita accesso affidabile per, digita enable per confermare, quindi scegli Abilita accesso affidabile.

6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS Artifact che ora può abilitare il funzionamento del servizio AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitarlo AWS Artifact come servizio affidabile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: Abilita AWSService l'accesso

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 dell'account di AWS Organizations gestione può disabilitare l'accesso affidabile con AWS Artifact.

Puoi disabilitare l'accesso affidabile solo utilizzando gli strumenti Organizations.

AWS Artifact richiede un accesso affidabile con AWS Organizations per lavorare con gli accordi organizzativi. Se si disabilita l'accesso attendibile AWS Organizations mentre si utilizza AWS Artifact per gli accordi organizzativi, smette di funzionare perché non può accedere all'organizzazione. Tutti gli accordi organizzativi che accetti AWS Artifact rimangono, ma non sono accessibili AWS Artifact. Il AWS Artifact ruolo che AWS Artifact crea 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 affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Artifactnell'elenco dei servizi.
4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Nella finestra di AWS Artifact dialogo Disabilita l'accesso affidabile per, digita disabilita per confermare, quindi scegli Disabilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS Artifact che ora può disabilitare il funzionamento di quel servizio AWS Organizations utilizzando la console o gli strumenti di servizio.

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

  Esegui il comando seguente per disabilitarlo AWS Artifact come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal artifact.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita AWSService l'accesso

AWS Audit Manager e AWS Organizations

AWS Audit Manager ti aiuta a controllare continuamente AWS l'utilizzo per semplificare la valutazione del rischio 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 prove Account AWS provenienti dalla tua organizzazione nell'ambito delle tue valutazioni.

Per ulteriori informazioni, consulta Enable AWS Organizations nella Audit Manager User Guide.

Utilizza le seguenti informazioni per aiutarti a eseguire l'integrazione 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 un accesso affidabile AWS Organizations prima di poter designare un account membro come amministratore delegato dell'organizzazione.

È possibile abilitare l'accesso affidabile utilizzando la AWS Audit Manager console o la AWS Organizations console.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS Audit Manager console o gli strumenti per abilitare l'integrazione con Organizations. Ciò consente di AWS Audit Manager eseguire qualsiasi configurazione richiesta, ad esempio la creazione delle 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 affidabile utilizzando la AWS Audit Manager console o gli strumenti, 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 configuri un amministratore delegato utilizzando la AWS Audit Manager console, abilita AWS Audit Manager automaticamente l'accesso affidabile per te.

È possibile abilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile ai servizi:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitarlo AWS Audit Manager come servizio affidabile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: Abilita AWSService l'accesso

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 dell'account di AWS Organizations gestione può disabilitare l'accesso affidabile con AWS Audit Manager.

Puoi disabilitare l'accesso affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  Esegui il comando seguente per disabilitarlo AWS Audit Manager come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal auditmanager.amazonaws.com
  ```

Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita AWSService l'accesso

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 configuri un amministratore delegato utilizzando la AWS Audit Manager console, Audit Manager abilita automaticamente l'accesso affidabile per te.

AWS CLI, AWS API

Se desideri configurare un account amministratore delegato utilizzando la AWS CLI o uno dei seguenti, puoi utilizzare AWS SDKs i seguenti comandi:

- AWS CLI:

```
$  aws audit-manager register-account \
    --delegated-admin-account 123456789012
```

- AWS SDK: richiama l'`RegisterAccount`operazione 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 AWS Backup lavori all'interno dell'organizzazione. Utilizzando AWS Backup, se si accede come utente all'account di gestione dell'organizzazione, è possibile abilitare la protezione e il monitoraggio dei backup a livello dell'organizzazione. Ti aiuta a raggiungere la conformità utilizzando politiche di backup per applicare centralmente AWS Backup i piani alle risorse di tutti gli account dell'organizzazione. Se li usi entrambi AWS Backup e AWS Organizations insieme, puoi 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 directory principale o agli account dell'organizzazione. OUs Una politica di backup combina un AWS Backup piano con gli altri dettagli necessari per applicare automaticamente il piano agli account. Le politiche collegate direttamente a un account vengono unite alle politiche ereditate dalla radice dell'organizzazione e da qualsiasi genitore OUs per creare una politica efficace applicabile all'account. La policy include l'ID di un ruolo IAM che dispone delle autorizzazioni per l'esecuzione AWS Backup sulle risorse dei tuoi 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 sicuro AWS 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 in merito AWS Backup, consulta la Guida per AWS Backup gli sviluppatori.

Utilizza le seguenti informazioni per semplificare l'integrazione 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 affidabile utilizzando la AWS Backup console o la AWS Organizations console.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS Backup console o gli strumenti per abilitare l'integrazione con Organizations. Ciò consente di AWS Backup eseguire qualsiasi configurazione richiesta, ad esempio la creazione delle 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 affidabile utilizzando la AWS Backup console o gli strumenti, non è necessario completare questi passaggi.

Per abilitare l'utilizzo dell'accesso affidabile AWS Backup, consulta Enabling backup in multiple Account AWS nella AWS Backup Developer Guide.

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 un accesso affidabile AWS Organizations per consentire il monitoraggio dei processi di backup, ripristino e copia tra gli account dell'organizzazione. Se disabiliti l'accesso affidabile AWS Backup, perdi la possibilità di visualizzare i lavori al di fuori dell'account corrente. Il AWS Backup ruolo che AWS Backup crea rimane. Se successivamente riattivi l'accesso affidabile, AWS Backup continua a funzionare come prima, senza la necessità di riconfigurare il servizio.

Puoi disabilitare l'accesso affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

Esegui il comando seguente per disabilitarlo AWS Backup come servizio affidabile con Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal backup.amazonaws.com
```

Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita AWSService l'accesso

Abilitazione di un account amministratore delegato per AWS Backup

Vedi la sezione Amministratore delegato nella Guida per gli sviluppatori di AWS Backup .

AWS Billing and Cost Management e AWS Organizations

AWS Billing and Cost Management offre una suite di funzionalità per aiutarti a configurare la fatturazione, recuperare e pagare le fatture e analizzare, organizzare, pianificare e ottimizzare i costi. Quando utilizzi Billing and Cost Management AWS Organizations with, consenti ai dati di allocazione dei costi suddivisi per AWS Organizations recuperare informazioni, se applicabile, e raccogliere dati di telemetria per i servizi di dati di allocazione dei costi suddivisi per i quali hai aderito.

Utilizza le seguenti informazioni per semplificare l'integrazione con. AWS Billing and Cost Management 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 Billing and Cost Management di eseguire le 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 Billing and Cost Management e Organizations o se rimuovi l'account membro dall'organizzazione.

Per ulteriori informazioni, consulta Autorizzazioni di ruolo collegate ai servizi per Billing and Cost Management nella Billing and Cost Management User Guide.

- `AWSServiceRoleForSplitCostAllocationData`

Principali dei servizi utilizzati da Billing and Cost Management

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 Billing and Cost Management garantiscono l'accesso ai seguenti principali di servizio:

Billing and Cost Management utilizza `billing-cost-management.amazonaws.com` il service principal.

Consentire un accesso affidabile con Billing and Cost Management

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Con l'accesso affidabile abilitato tramite l'account di gestione, i clienti possono sfruttare la funzionalità di suddivisione dei dati di allocazione dei costi in Billing and Cost Management. Quando i clienti abilitano i dati di allocazione dei costi suddivisi per Amazon Elastic Kubernetes Service con Amazon Managed Service for Prometheus, viene richiamato l'accesso affidabile per creare ruoli collegati ai servizi per tutti gli account membri all'interno dell'organizzazione. Ciò consente di suddividere i dati di allocazione dei costi per raccogliere dati di telemetria dagli spazi di lavoro Amazon Managed Service for Prometheus dei clienti ed eseguire l'allocazione dei costi in base a tali metriche.

Puoi abilitare l'accesso affidabile solo utilizzando gli strumenti Organizations.

È possibile abilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile ai servizi:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitarlo AWS Billing and Cost Management come servizio affidabile con Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal  billing-cost-management.amazonaws.com
```

Questo comando non produce alcun output se ha esito positivo.

- AWS API: Abilita AWSService l'accesso

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 affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  Esegui il comando seguente per disabilitarlo AWS Billing and Cost Management come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal  billing-cost-management.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: disabilita AWSService l'accesso

AWS CloudFormation StackSets e AWS Organizations

AWS CloudFormation StackSets consente di creare, aggiornare o eliminare pile su più Account AWS pile Regioni AWS con un'unica operazione. StackSets l'integrazione con AWS Organizations consente di creare set di stack con autorizzazioni gestite dal servizio, utilizzando un ruolo collegato al servizio che dispone dell'autorizzazione pertinente in ciascun account membro. Ciò consente di implementare istanze dello stack a tutti gli account membri dell'organizzazione. Non è necessario

creare i AWS Identity and Access Management ruoli 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.

Con l'accesso affidabile tra StackSets e Organizations abilitato, 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 degli amministratori delegati per la distribuzione su specifici set di stack OUs o per eseguire operazioni specifiche su set di stack.

Per ulteriori informazioni sull'integrazione StackSets con Organizations, consulta Working with AWS CloudFormation StackSets nella AWS CloudFormation User Guide.

Utilizza le seguenti informazioni per semplificare l'integrazione 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. Questo ruolo consente a AWS CloudFormation Stacksets 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 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 maggiori dettagli sulla creazione di set di stack, consulta Working with AWS CloudFormation StackSets nella Guida per l'AWS CloudFormation utente.

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 di servizio:

- Account di gestione: `stacksets.cloudformation.amazonaws.com`

  È possibile modificare o eliminare questo ruolo solo se è stato disabilitato l'accesso affidabile tra StackSets e Organizations.
- Account membri: `member.org.stacksets.cloudformation.amazonaws.com`

  È possibile modificare o eliminare questo ruolo da un account solo se si disabilita prima l'accesso affidabile tra StackSets e Organizations o se si rimuove prima l'account dall'organizzazione o dall'unità organizzativa (OU) 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 dell'account di gestione Organizations dispone delle autorizzazioni per abilitare l'accesso affidabile con un altro AWS servizio. Puoi abilitare l'accesso attendibile utilizzando la console AWS CloudFormation o la console Organizations.

È possibile abilitare l'accesso attendibile solo utilizzando AWS CloudFormation StackSets.

Per abilitare l'accesso affidabile utilizzando la console AWS CloudFormation Stacksets, consulta Enable Trusted Access with AWS Organizations nella Guida per l' AWS CloudFormation utente.

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 l'amministratore di un account di gestione Organizations dispone delle autorizzazioni per disabilitare l'accesso affidabile con un altro AWS servizio. Puoi disabilitare l'accesso attendibile utilizzando solo la console Organizations. Se disabiliti l'accesso affidabile con Organizations durante l'utilizzo 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 affidabile utilizzando la AWS CloudFormation console o la console Organizations.

> **Important**
>
> Se disabiliti l'accesso affidabile a livello di codice (ad esempio con AWS CLI o con un'API), tieni presente che ciò rimuoverà l'autorizzazione. È meglio disabilitare l'accesso affidabile con la console. AWS CloudFormation

È possibile disabilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS CloudFormation StackSetsnell'elenco dei servizi.

4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Nella finestra di AWS CloudFormation StackSets dialogo Disabilita l'accesso attendibile per, digita disabilita per confermare, quindi scegli Disabilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS CloudFormation StackSets che ora può disabilitare il funzionamento di quel servizio AWS Organizations utilizzando la console o gli strumenti di servizio.

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

  Esegui il comando seguente per disabilitarlo AWS CloudFormation StackSets come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal stacksets.cloudformation.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: disabilita AWSService l'accesso

Abilitazione di un account amministratore delegato per Stacksets AWS CloudFormation

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 degli Stackset. AWS CloudFormation

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 di AWS CloudTrail .

Utilizza le seguenti informazioni per aiutarti a eseguire 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 Organizations nella 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.

È possibile abilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile ai servizi:

- AWS CLI: enable-aws-service-access

  Esegui 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 AWSService l'accesso

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 un percorso, esegui update-trailcomando e includi il `--is-organization-trail` parametro.
  - Per aggiornare un archivio dati di eventi, esegui 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. È possibile 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 dei. AWS SDKs

È possibile disabilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS CloudTrailnell'elenco dei servizi.
4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Nella finestra di AWS CloudTrail dialogo Disabilita l'accesso attendibile per, digita disabilita per confermare, quindi scegli Disabilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS CloudTrail che ora può disabilitare il funzionamento di quel servizio AWS Organizations utilizzando la console o gli strumenti di servizio.

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

  Esegui 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 AWSService l'accesso

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

Amazon CloudWatch e AWS Organizations

Puoi utilizzarlo AWS Organizations per Amazon CloudWatch per i seguenti casi d'uso:

- Scopri e comprendi lo stato della configurazione di telemetria per AWS le tue risorse da una vista centralizzata nella console. CloudWatch Ciò semplifica il processo di verifica delle configurazioni della raccolta di telemetria per diversi tipi di risorse all'interno dell'organizzazione o dell'account. AWS È necessario attivare l'accesso affidabile per utilizzare la configurazione di telemetria in tutta l'organizzazione.

  Per ulteriori informazioni, consulta la sezione Controllo delle configurazioni di CloudWatch telemetria nella Amazon User Guide. CloudWatch

- Lavora con più account in Network Flow Monitor, una funzionalità di Amazon CloudWatch Network Monitoring. Network Flow Monitor offre una visibilità quasi in tempo reale sulle prestazioni di rete per il traffico tra EC2 istanze Amazon. Dopo aver attivato l'accesso affidabile per l'integrazione con Organizations, puoi creare un monitor per visualizzare i dettagli delle prestazioni di rete su più account.

  Per ulteriori informazioni, consulta Initialize Network Flow Monitor per il monitoraggio di più account nella Amazon CloudWatch User Guide.

Utilizza le seguenti informazioni per facilitare l'integrazione di Amazon CloudWatch con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

Crea il seguente ruolo legato al servizio nell'account di gestione della tua organizzazione. Il ruolo collegato ai servizi viene creato automaticamente negli account dei membri quando abiliti l'accesso attendibile. Tale ruolo consente CloudWatch a di eseguire le operazioni supportate all'interno degli account dell'organizzazione. Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso attendibile tra CloudWatch e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForObservabilityAdmin`

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 CloudWatch concedono l'accesso ai seguenti principali del servizio:

- `observabilityadmin.amazonaws.com`
- `networkflowmonitor.amazonaws.com`
- `topology.networkflowmonitor.amazonaws.com`

Abilitazione dell'accesso attendibile con CloudWatch

Per informazioni sulle autorizzazioni di cui hai bisogno per attivare l'accesso attendibile, consultaAutorizzazioni necessarie per abilitare l'accesso sicuro.

Puoi abilitare l'accesso attendibile utilizzando la CloudWatch console Amazon o la AWS Organizations console.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la CloudWatch console o gli strumenti Amazon per abilitare l'integrazione con Organizations. Ciò consente ad Amazon di CloudWatch 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 CloudWatch. Per ulteriori informazioni, consulta questa nota.
> Se abiliti l'accesso attendibile utilizzando la CloudWatch console o gli strumenti Amazon, non è necessario completare questi passaggi.

Per abilitare l'accesso attendibile tramite la CloudWatch console

Consulta Attivazione del controllo CloudWatch telemetrico nella Amazon User Guide. CloudWatch

Quando attivi l'accesso affidabile in CloudWatch, abiliti il controllo telemetrico e puoi lavorare con più account in Network Flow Monitor.

È possibile abilitare l'accesso attendibile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando oppure chiamando un'operazione API in una delle AWS SDKs.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

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

6. Se sei l'amministratore di AWS Organizations, comunica all'amministratore di Amazon CloudWatch che ora è possibile abilitare tale servizio per il funzionamento con AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizzare i seguenti AWS CLI comandi oppure operazioni API per abilitare l'accesso al servizio attendibile:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitare Amazon CloudWatch come servizio attendibile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: Abilita AWSService l'accesso

Disattiva l'accesso affidabile con CloudWatch

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Puoi disabilitare l'accesso attendibile utilizzando Amazon CloudWatch o gli AWS Organizations strumenti.

> **Important**
>
> Consigliamo vivamente di utilizzare, quando possibile, la CloudWatch console o gli strumenti Amazon per disabilitare l'integrazione con Organizations. Ciò consente ad Amazon di CloudWatch 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 Amazon CloudWatch.

Se disabiliti l'accesso attendibile utilizzando la CloudWatch console o gli strumenti Amazon, non è necessario completare questi passaggi.

Per abilitare l'accesso attendibile tramite la CloudWatch console

Consulta la sezione Disattivazione del controllo CloudWatch telemetrico nella Amazon User Guide CloudWatch

Quando disattivi l'accesso affidabile in CloudWatch, il controllo telemetrico non è più attivo e non puoi più lavorare con più account in Network Flow Monitor.

È possibile disabilitare l'accesso attendibile eseguendo AWS CLI il comando di Organizations oppure chiamando un'operazione API Organizations in una delle AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizzare i seguenti AWS CLI comandi oppure operazioni API per disabilitare l'accesso al servizio attendibile:

- AWS CLI: disable-aws-service-access

  Esegui il comando seguente per disabilitare Amazon CloudWatch come servizio attendibile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal observabilityadmin.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: disabilita AWSService l'accesso

Registrazione di un account di amministratore delegato per CloudWatch

Quando si registra un account membro come account di amministratore delegato per l'organizzazione, gli utenti e i ruoli di tale account possono eseguire operazioni amministrative CloudWatch che altrimenti possono essere eseguiti solo da utenti o ruoli collegati con l'account di gestione dell'organizzazione. L'utilizzo di un account di amministratore delegato consente di separare la gestione dell'organizzazione dalla gestione delle funzionalità in CloudWatch.

> **Autorizzazioni minime**
>
> Solo un amministratore nell'account di gestione di Organizations può registrare un account membro come account amministratore delegato per CloudWatch nell'organizzazione.

Puoi registrare l'account di un amministratore delegato tramite la CloudWatch console oppure utilizzando l'operazione `RegisterDelegatedAdministrator` API Organizations con AWS Command Line Interface o un SDK.

Per informazioni su come registrare un account amministratore delegato utilizzando la CloudWatch console, consulta Turning on CloudWatch telemetry auditing nella Amazon User Guide. CloudWatch

Quando registri un account amministratore delegato in CloudWatch, puoi utilizzare l'account per le operazioni di gestione con il controllo della telemetria e con Network Flow Monitor.

Annullare la registrazione di un amministratore delegato per CloudWatch

> **Autorizzazioni minime**
>
> Solo un amministratore che ha effettuato l'accesso con l'account di gestione di Organizations può annullare la registrazione di un account amministratore delegato per CloudWatch nell'organizzazione.

Puoi annullare la registrazione dell'account di amministratore delegato utilizzando la CloudWatch console oppure utilizzando l'operazione `DeregisterDelegatedAdministrator` API Organizations con AWS Command Line Interface o un SDK. Per ulteriori informazioni, consulta Annullamento della registrazione di un account amministratore delegato nella Amazon CloudWatch User Guide.

Quando annulli la registrazione di un account amministratore delegato in CloudWatch, non puoi più utilizzare l'account per operazioni di gestione con il controllo della telemetria e con Network Flow Monitor.

AWS Compute Optimizer e AWS Organizations

AWS Compute Optimizer è un servizio che analizza le metriche di configurazione e utilizzo delle risorse. AWS Gli esempi di risorse includono le istanze Amazon Elastic Compute Cloud (Amazon

EC2) e i gruppi di 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 aiutarti a eseguire l'integrazione con. AWS Compute Optimizer 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 affidabile utilizzando la AWS Compute Optimizer console o la AWS Organizations console.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS Compute Optimizer console o gli strumenti per abilitare l'integrazione con Organizations. Ciò consente di AWS

Compute Optimizer eseguire qualsiasi configurazione richiesta, ad esempio la creazione delle 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 affidabile utilizzando la AWS Compute Optimizer console o gli strumenti, 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 .

Puoi abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in uno dei AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Compute Optimizernell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di AWS Compute Optimizer dialogo Abilita accesso affidabile per, digita enable per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS Compute Optimizer che ora può abilitare il funzionamento del servizio AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitarlo AWS Compute Optimizer come servizio affidabile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: Abilita AWSService l'accesso

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 dell'account di AWS Organizations gestione può disabilitare l'accesso affidabile con AWS Compute Optimizer.

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  Esegui il comando seguente per disabilitarlo AWS Compute Optimizer come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal compute-optimizer.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita AWSService l'accesso

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 amministratore delegato utilizzando la AWS CLI o uno dei seguenti, puoi utilizzare AWS SDKs i seguenti comandi:

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal compute-optimizer.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.

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 il AWS AWS CLI, consulta la sezione AWS AWS CLI Command deregister-delegated-administratorReference.

AWS Config e AWS Organizations

L'aggregazione di dati su più account e più regioni AWS Config consente di aggregare AWS Config i dati di più account 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 AWS Config che raccoglie AWS Config dati da più account e regioni di origine. Crea un aggregatore nella regione in cui desideri visualizzare i dati aggregati. AWS Config Durante la creazione di un aggregatore, puoi scegliere di aggiungere un account individuale IDs o la tua organizzazione. Per ulteriori informazioni in merito AWS Config, consulta la Guida per gli AWS Config sviluppatori.

Puoi anche AWS Config APIsutilizzarlo per gestire AWS Config le regole Account AWS in tutta l'organizzazione. Per ulteriori informazioni, consulta Abilitazione AWS Config delle regole per tutti gli account dell'organizzazione nella Guida per gli AWS Config sviluppatori.

Utilizza le seguenti informazioni per aiutarti a eseguire l'integrazione AWS Config con AWS Organizations.

Ruoli collegati ai servizi

Il seguente ruolo collegato al servizio consente di AWS Config eseguire operazioni supportate all'interno degli account dell'organizzazione.

- `AWSServiceRoleForConfig`

Scopri di più sulla creazione di questo ruolo in Autorizzazioni per il ruolo IAM assegnato a AWS Config nella Guida per gli sviluppatori AWS Config

Scopri di più su come utilizzare i ruoli collegati ai servizi in AWS Config Using Service-Linked Roles for nella Developer Guide AWS ConfigAWS Config

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.

Puoi abilitare l'accesso affidabile utilizzando la console o la AWS Config console. AWS Organizations

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS Config console o gli strumenti per abilitare l'integrazione con Organizations. Ciò consente di AWS Config eseguire qualsiasi configurazione richiesta, ad esempio la creazione delle 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 affidabile utilizzando la AWS Config console o gli strumenti, non è necessario completare questi passaggi.

Per abilitare l'accesso affidabile tramite la AWS Config console

Per abilitare l'accesso affidabile all' AWS Organizations utilizzo AWS Config, crea un aggregatore multi-account e aggiungi l'organizzazione. Per informazioni su come configurare un aggregatore multi-account, consulta Creating Aggregators nella Developer Guide.AWS Config

È possibile abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in uno dei. AWS SDKs

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Configgnell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).

5. Nella finestra di AWS Config dialogo Abilita accesso affidabile per, digita enable per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS Config che ora può abilitare il funzionamento del servizio AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitarlo AWS Config come servizio affidabile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: Abilita AWSService l'accesso

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 affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  Esegui il comando seguente per disabilitarlo AWS Config come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal config.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita AWSService l'accesso

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.

È possibile abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in uno dei AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli Centrale ottimizzazione costi AWSnell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di Centrale ottimizzazione costi AWS dialogo Abilita accesso affidabile per, digita enable per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore Centrale ottimizzazione costi AWS che ora può abilitare il funzionamento del servizio AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  Esegui 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 AWSService l'accesso

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 affidabile solo utilizzando gli strumenti 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.

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

Esegui 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 AWSService l'accesso

Abilitazione di un account amministratore delegato per Cost Optimization Hub

Quando si designa un account membro come amministratore delegato dell'organizzazione, l'account designato può recuperare i consigli di Cost Optimization Hub per tutti gli account dell'organizzazione e gestire le preferenze del Cost Optimization Hub, offrendo una maggiore flessibilità nell'identificare centralmente le opportunità di ottimizzazione delle risorse.

> **Autorizzazioni minime**
>
> Solo un utente o un ruolo nell'account di gestione Organizations con la seguente autorizzazione può configurare un account membro come amministratore delegato per Cost Optimization Hub nell'organizzazione:

Per istruzioni sull'attivazione di un account amministratore delegato per Cost Optimization Hub, consulta Delegare un account amministratore nella Guida per l'AWS Cost Management utente.

Disabilitazione di un amministratore delegato per Cost Optimization Hub

Solo un amministratore dell'account di gestione Organizations può rimuovere un amministratore delegato per Cost Optimization Hub.

Per disabilitare l'account amministratore delegato Cost Optimization Hub utilizzando la console Cost Optimization Hub, consulta Delegare un account amministratore nella Guida per l'AWS Cost Management utente.

Per rimuovere un amministratore delegato utilizzando la AWS CLI, `deregister-delegated-administrator`consulta il riferimento alla AWS Config CLI.

AWS Control Tower e AWS Organizations

AWS Control Tower offre un modo semplice per configurare e gestire un ambiente AWS multi-account, seguendo le migliori pratiche prescrittive. AWS Control Tower l'orchestrazione estende le funzionalità di. AWS Organizations AWS Control Tower applica controlli preventivi e investigativi (guardrail) per evitare che le organizzazioni e i conti divergano dalle migliori pratiche (deriva).

AWS Control Tower l'orchestrazione estende le funzionalità di. AWS Organizations

Per ulteriori informazioni, consulta la guida per l'AWS Control Tower utente.

Utilizza le seguenti informazioni per facilitare l'integrazione AWS Control Tower con AWS Organizations.

Ruoli necessari per l'integrazione

Il ruolo `AWSControlTowerExecution` deve essere presente in tutti gli account registrati. Consente di AWS Control Tower gestire i singoli account e di riportare le informazioni su di essi agli account Audit e Log Archive.

Per ulteriori informazioni sui ruoli utilizzati da AWS Control Tower, consulta How AWS Control Tower works with roles to create and manage account e Using Identity-Based Policies (IAM Policies) per. AWS Control Tower

Principali di servizio utilizzati da AWS Control Tower

AWS Control Tower utilizza il `controltower.amazonaws.com` service principal.

Abilitazione dell'accesso attendibile con AWS Control Tower

AWS Control Tower utilizza un accesso affidabile per rilevare la deriva a fini di controlli preventivi e per tenere traccia delle modifiche all'account e all'unità organizzativa che causano la deriva.

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Puoi abilitare l'accesso affidabile solo utilizzando gli strumenti Organizations.

Per abilitare l'accesso attendibile dalla console Organizations, scegli **`Enable access`** accanto a AWS Control Tower.

È possibile abilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile ai servizi:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitarlo AWS Control Tower come servizio affidabile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: Abilita AWSService l'accesso

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 affidabile solo utilizzando gli strumenti Organizations.

> **Important**
>
> La disabilitazione AWS Control Tower dell'accesso affidabile causa un cambiamento nella tua AWS Control Tower Landing Zone. 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 .

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  Esegui il comando seguente per disabilitarlo AWS Control Tower come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal controltower.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita AWSService l'accesso

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'utilizzo ti AWS Organizations consente di garantire che il grafico del comportamento del Detective fornisca visibilità sull'attività di tutti gli account della tua 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.

Utilizza le seguenti informazioni per aiutarti a integrare 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 un accesso affidabile AWS Organizations prima di poter designare un account membro come amministratore delegato di questo servizio per l'organizzazione.

Puoi abilitare l'accesso affidabile solo utilizzando gli strumenti Organizations.

È possibile abilitare l'accesso affidabile utilizzando la AWS Organizations console.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli Amazon Detective nell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di dialogo Abilita accesso affidabile per Amazon Detective, digita enable per confermarlo, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore di Amazon Detective che ora può abilitare il funzionamento di quel servizio AWS Organizations dalla console di servizio.

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 dell'account di AWS Organizations gestione può disabilitare l'accesso affidabile con Amazon Detective.

Puoi disabilitare l'accesso affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile utilizzando la AWS Organizations console.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli Amazon Detective nell'elenco dei servizi.
4. Scegli Disable trusted access (Disabilita accesso attendibile).

5. Nella finestra di dialogo Disabilita l'accesso affidabile per Amazon Detective, digita disable per confermare, quindi scegli Disabilita accesso affidabile.
6. Se sei l'amministratore di only AWS Organizations, comunica all'amministratore di Amazon Detective che ora può disabilitare il funzionamento di quel servizio AWS Organizations utilizzando la console o gli strumenti del servizio;.

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 amministratore delegato utilizzando la AWS CLI o uno dei seguenti, puoi utilizzare AWS SDKs i seguenti comandi:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal detective.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 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 le metriche e gli eventi delle applicazioni per identificare comportamenti che si discostano dai normali modelli operativi. Gli utenti vengono avvisati quando DevOps Guru rileva un problema o un rischio operativo.

L'utilizzo di DevOps Guru consente il supporto multiaccount con AWS Organizations, quindi puoi designare un account membro per gestire le informazioni 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, consulta Monitora gli account della tua organizzazione nella Amazon DevOps Guru User Guide.

Utilizza le seguenti informazioni per aiutarti a integrare 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. Questo ruolo consente a DevOps Guru di eseguire le operazioni supportate all'interno degli account della tua organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso affidabile tra DevOps Guru e Organizations o se rimuovi 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 garantiscono l'accesso ai seguenti principali di servizio:

- `devops-guru.amazonaws.com`

Per ulteriori informazioni, consulta Using service-linked roles for DevOps Guru nella Amazon Guru User DevOps Guide.

Per abilitare l'accesso affidabile con Guru DevOps

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, Guru abilita automaticamente l'accesso affidabile per DevOps Guru per la propria organizzazione DevOps.
> DevOpsGuru richiede un accesso affidabile AWS Organizations prima di poter designare un account membro come amministratore delegato di questo servizio per la tua organizzazione.

> **Important**
>
> Ti 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 delle risorse necessarie al servizio. Procedi con questi passaggi solo se non riesci ad

abilitare l'integrazione utilizzando gli strumenti forniti da Amazon DevOps Guru. Per ulteriori informazioni, consulta questa nota.

Puoi abilitare l'accesso affidabile utilizzando la AWS Organizations console o la console DevOps Guru.

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 Servizi, trova la riga per Amazon DevOps Guru, 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 Amazon DevOps Guru che ora può abilitare quel servizio utilizzando la sua console con AWS Organizations cui lavorare.

DevOps Guru console

Per abilitare l'accesso affidabile al servizio utilizzando la console DevOps Guru

1. Accedi come amministratore nell'account di gestione e apri la console DevOps Guru: Amazon DevOps Guru console
2. Scegliere Enable trusted access (Abilita accesso sicuro).

Per disabilitare l'accesso affidabile con Guru DevOps

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Solo un amministratore dell'account di AWS Organizations gestione può disabilitare l'accesso affidabile con Amazon DevOps Guru.

Puoi disabilitare l'accesso affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile utilizzando la AWS Organizations console.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli Amazon DevOps Guru nell'elenco dei servizi.
4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Nella finestra di dialogo Disabilita accesso affidabile per Amazon DevOps Guru, digita disable per confermare, quindi scegli Disabilita accesso affidabile.
6. Se sei l'amministratore di only AWS Organizations, comunica all'amministratore di Amazon DevOps Guru che ora può disabilitare il funzionamento di quel servizio AWS Organizations utilizzando la console o gli strumenti di servizio;.

Attivazione di un account amministratore delegato per Guru DevOps

L'account amministratore delegato di DevOps Guru può visualizzare i dati di approfondimento di tutti gli account dei membri che vengono aggiunti a Guru dall'organizzazione. DevOps Per informazioni su come un amministratore delegato gestisce gli account dell'organizzazione, consulta Monitora gli account della tua organizzazione nella Amazon DevOps Guru User Guide.

Solo un amministratore dell'account di gestione dell'organizzazione può configurare un amministratore delegato per Guru. DevOps

È possibile specificare un account amministratore delegato dalla console DevOps Guru o utilizzando l'operazione Organizations `RegisterDelegatedAdministrator` CLI o SDK.

> **Autorizzazioni minime**
>
> Solo un utente o un ruolo nell'account di gestione Organizations può configurare un account membro come amministratore delegato per DevOps Guru nell'organizzazione.

DevOps Guru console

Per configurare un amministratore delegato nella console Guru DevOps

1. Accedi come amministratore nell'account di gestione e apri la console DevOps Guru: Amazon DevOps Guru console
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 amministratore delegato utilizzando la AWS CLI o uno dei seguenti, puoi utilizzare AWS SDKs i seguenti comandi:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal devops-guru.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 Guru DevOps

È possibile rimuovere l'amministratore delegato utilizzando la console DevOps Guru o utilizzando l'operazione Organizations `DeregisterDelegatedAdministrator` CLI o SDK. Per informazioni su come rimuovere un amministratore delegato utilizzando la console DevOps Guru, consulta Monitora gli account della tua organizzazione nella Amazon DevOps Guru User Guide.

AWS Directory Service e AWS Organizations

AWS Directory Service per Microsoft Active Directory oppure AWS Managed Microsoft AD consente di eseguire Microsoft Active Directory (AD) come servizio gestito. AWS Directory Service semplifica la configurazione e l'esecuzione di directory nel AWS cloud o la connessione AWS delle risorse a un Microsoft Active Directory locale esistente. AWS Managed Microsoft AD si integra perfettamente anche con AWS Organizations per consentire la condivisione di directory senza interruzioni tra più

Account AWS VPC in una regione. Per ulteriori informazioni, consulta la Guida di amministrazione di AWS Directory Service.

Per condividerne una all' AWS Directory Service interno di un'organizzazione, l'organizzazione deve avere tutte le funzionalità abilitate e la directory deve trovarsi nell'account di gestione dell'organizzazione.

Utilizza le seguenti informazioni per semplificare l'integrazione 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 affidabile utilizzando la AWS Directory Service console o la AWS Organizations console.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS Directory Service console o gli strumenti per abilitare l'integrazione con Organizations. Ciò consente di AWS Directory Service eseguire qualsiasi configurazione richiesta, ad esempio la creazione delle 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 affidabile utilizzando la AWS Directory Service console o gli strumenti, non è necessario completare questi passaggi.

Per abilitare l'accesso affidabile tramite la AWS Directory Service console

Per condividere una directory che abilita automaticamente l'accesso attendibile, consulta Condivisione della directory nella Guida per l'amministratore di AWS Directory Service . Per step-by-step istruzioni, vedi Tutorial: Condivisione della directory AWS gestita di Microsoft AD.

È possibile abilitare l'accesso affidabile utilizzando la AWS Organizations console.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Directory Servicenell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di AWS Directory Service dialogo Abilita accesso affidabile per, digita enable per confermarlo, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS Directory Service che ora può abilitare il funzionamento del servizio AWS Organizations dalla console di servizio.

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 affidabile utilizzando AWS Organizations mentre stai utilizzando AWS Directory Service, tutte le directory precedentemente condivise continueranno 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 affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile utilizzando la AWS Organizations console.

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. Nel riquadro di navigazione, scegli Servizi.

3. Scegli AWS Directory Servicenell'elenco dei servizi.
4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Nella finestra di AWS Directory Service dialogo Disabilita l'accesso affidabile per, digita disabilita per confermare, quindi scegli Disabilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS Directory Service che ora può disabilitare il funzionamento di quel servizio AWS Organizations utilizzando la console o gli strumenti di servizio;.

Amazon Elastic Compute Cloud e AWS Organizations

Amazon Elastic Compute Cloud fornisce capacità di elaborazione scalabile su richiesta nel cloud. AWS Quando utilizzi Amazon EC2 with Organizations, consenti all'amministratore dell'organizzazione di creare un report sulla configurazione esistente per gli account dell'organizzazione dopo aver utilizzato la funzione Declarative EC2 Policies di Amazon.

Utilizza le seguenti informazioni per aiutarti a integrare Amazon Elastic Compute Cloud 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 EC2 ad Amazon di eseguire operazioni supportate all'interno degli account della tua organizzazione.

Puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso affidabile tra Amazon EC2 e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForDeclarativePoliciesEC2Report`

Principali di servizio utilizzati da Amazon EC2

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 EC2 concedono l'accesso ai seguenti principali di servizio:

- `ec2.amazonaws.com`

Abilitare l'accesso affidabile con Amazon EC2

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Per consentire all'amministratore di Organizations di creare un rapporto sulla configurazione esistente per gli account all'interno dell'organizzazione, devi abilitare l'accesso affidabile.

Puoi abilitare l'accesso affidabile solo utilizzando gli strumenti Organizations.

È possibile abilitare l'accesso attendibile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in uno dei AWS SDKs.

AWS Management Console

Per abilitare l'accesso al servizio attendibile tramite la console Organizations

1. Accedi alla AWS Organizations console . È necessario accedere come utente IAM, assumere un ruolo IAM o accedere come utente root (non consigliato) nell'account di gestione dell'organizzazione.
2. Nel riquadro di navigazione, scegli Servizi.
3. Scegli Amazon Elastic Compute Cloud nell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di dialogo Abilita accesso affidabile per Amazon Elastic Compute Cloud, digita enable per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore di Amazon Elastic Compute Cloud che ora può abilitare il servizio in modo che funzioni AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitare Amazon Elastic Compute Cloud come servizio affidabile con Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal ec2.amazonaws.com
```

Questo comando non produce alcun output se ha esito positivo.

- AWS API: Abilita AWSService l'accesso

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 affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  Esegui il comando seguente per disabilitare Amazon Elastic Compute Cloud come servizio affidabile con Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal ec2.amazonaws.com
```

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita l'accesso AWSService

Amazon Elastic Kubernetes Service e AWS Organizations

Amazon Elastic Kubernetes Service Dashboard è una dashboard consolidata che puoi utilizzare per monitorare, gestire e ottenere visibilità sui tuoi cluster Kubernetes in più regioni e account. AWS AWS

La dashboard EKS ti offre un controllo completo e informazioni dettagliate per la tua infrastruttura Amazon EKS attraverso un'interfaccia centralizzata.

La dashboard di Amazon Elastic Kubernetes Service ti consente di tenere traccia dei cluster pianificati per gli upgrade, dei costi del piano di controllo del progetto, di esaminare le informazioni sui cluster e monitorare le distribuzioni dei gruppi di nodi nell'organizzazione. I tuoi AWS amministratori possono visualizzare i dati aggregati sulle risorse del cluster, tra cui lo stato di salute, la distribuzione delle versioni e le configurazioni aggiuntive attraverso diverse opzioni di visualizzazione tra cui grafici, elenchi di risorse e mappe geografiche. La dashboard si integra con AWS Organizations per fornire una visibilità sicura tra account e regioni diverse delle risorse EKS.

Utilizza le seguenti informazioni per facilitare l'integrazione di Amazon Elastic Kubernetes Service 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 utilizzando la console Amazon Elastic Kubernetes Service. Tale ruolo consente a Amazon EKS 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 Elastic Kubernetes Service e Organizations.

Se abiliti l'accesso attendibile direttamente dalla console Organizations, CLI o SDK, il ruolo collegato al servizio non viene creato automaticamente.

- `AWSServiceRoleForAmazonEKSDashboard`

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 EKS concedono l'accesso ai seguenti principali del servizio:

- `dashboard.eks.amazonaws.com`

Abilitazione dell'accesso attendibile con Amazon EKS

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Per abilitare l'accesso attendibile tramite la console Amazon EKS

Consulta Abilita l'accesso affidabile nella Guida per l'utente di Amazon EKS.

Disabilitazione dell'accesso attendibile con Amazon EKS

Per abilitare l'accesso attendibile tramite la console Amazon EKS

Consulta Disabilitare l'accesso affidabile nella Guida per l'utente di Amazon EKS.

Abilitazione di un account amministratore delegato per Amazon EKS

L'amministratore dell'account di gestione può delegare le autorizzazioni amministrative di Amazon EKS a un account membro designato noto come amministratore delegato.

Gli account di gestione e gli account amministratore delegato possono visualizzare il dashboard di Amazon EKS.

Per abilitare un account amministratore delegato

Consulta Abilitare un account amministratore delegato nella Amazon EKS User Guide.

Disattivazione di un amministratore delegato per Amazon EKS

Solo un amministratore nell'account di gestione dell'organizzazione può configurare un amministratore delegato per Amazon EKS.

Per disabilitare un account di amministratore delegato

Consulta Disabilitare un account amministratore delegato nella Amazon EKS User Guide.

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 in tutta l'organizzazione Account AWS e nelle applicazioni dell'organizzazione. Con Firewall Manager, puoi implementare AWS WAF regole, creare AWS Shield Advanced protezioni, configurare e controllare i gruppi di sicurezza di Amazon Virtual Private Cloud (Amazon VPC) e AWS Network Firewall distribuirli. 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 in merito AWS Firewall Manager, consulta la Guida per gli sviluppatori AWS Firewall Manager .

Utilizza le seguenti informazioni per facilitare l'integrazione 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 affidabile utilizzando la AWS Firewall Manager console o la AWS Organizations console.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS Firewall Manager console o gli strumenti per abilitare l'integrazione con Organizations. Ciò consente di AWS Firewall Manager eseguire qualsiasi configurazione richiesta, ad esempio la creazione

delle 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 affidabile utilizzando la AWS Firewall Manager console o gli strumenti, non è necessario completare questi passaggi.

Devi accedere con il tuo account di AWS Organizations gestione e configurare un account all'interno dell'organizzazione come account AWS Firewall Manager amministratore. 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 affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in uno dei AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Firewall Managernell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di AWS Firewall Manager dialogo Abilita accesso affidabile per, digita enable per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS Firewall Manager che ora può abilitare il funzionamento del servizio AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

Esegui il comando seguente per abilitarlo AWS Firewall Manager come servizio affidabile con Organizations.

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

Questo comando non produce alcun output se ha esito positivo.

- AWS API: Abilita AWSService l'accesso

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.

Puoi disabilitare l'accesso affidabile utilizzando gli AWS Firewall Manager o gli AWS Organizations strumenti.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS Firewall Manager console o gli strumenti per disabilitare l'integrazione con Organizations. Ciò consente di AWS Firewall Manager eseguire tutte le operazioni di pulizia necessarie, ad esempio l'eliminazione di risorse o l'accesso a ruoli che non sono più necessari al 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 affidabile utilizzando la AWS Firewall Manager console o gli strumenti, non è necessario completare questi passaggi.

Per disabilitare l'accesso attendibile tramite la console Firewall Manager

Puoi modificare o revocare l'account AWS Firewall Manager amministratore seguendo le istruzioni in Designazione di un altro account come account AWS Firewall Manager amministratore nella Guida per gli AWS Firewall Manager sviluppatori.

Se revochi l'account amministratore, devi accedere all'account di AWS Organizations gestione e impostare un nuovo account amministratore per. AWS Firewall Manager

È possibile disabilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Firewall Managernell'elenco dei servizi.
4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Nella finestra di AWS Firewall Manager dialogo Disabilita l'accesso affidabile per, digita disabilita per confermare, quindi scegli Disabilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS Firewall Manager che ora può disabilitare il funzionamento di quel servizio AWS Organizations utilizzando la console o gli strumenti di servizio.

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

  Esegui il comando seguente per disabilitarlo AWS Firewall Manager come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal fms.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita AWSService l'accesso

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 Impostare l'account AWS Firewall Manager amministratore nella Guida per gli AWS Firewall Manager sviluppatori.

Amazon GuardDuty e AWS Organizations

Amazon GuardDuty è un servizio di monitoraggio continuo della sicurezza che analizza ed elabora diverse fonti di dati, utilizzando feed di intelligence sulle minacce e apprendimento automatico per identificare attività impreviste e potenzialmente non autorizzate e dannose all'interno del tuo ambiente. AWS Ciò può includere problemi come l'aumento dei privilegi, l'uso di credenziali esposte, la comunicazione con indirizzi IP o domini dannosi o la presenza di malware sulle istanze di Amazon Elastic Compute Cloud e sui carichi di lavoro dei container. URLs

Puoi contribuire a semplificare la gestione GuardDuty utilizzando Organizations per gestire GuardDuty tutti gli account della tua organizzazione.

Per ulteriori informazioni, consulta Gestire GuardDuty gli account con AWS Organizations nella Amazon GuardDuty User Guide

Utilizza le seguenti informazioni per aiutarti a integrare 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. Questi ruoli consentono GuardDuty di

eseguire operazioni supportate all'interno degli account dell'organizzazione. Puoi eliminare un ruolo solo se disabiliti l'accesso affidabile tra GuardDuty e Organizations o se rimuovi l'account membro dall'organizzazione.

- Il ruolo `AWSServiceRoleForAmazonGuardDuty` collegato al servizio viene creato automaticamente negli account integrati con GuardDuty Organizations. Per ulteriori informazioni, consulta Managing GuardDuty accounts with Organizations nella Amazon GuardDuty User Guide
- Il ruolo `AmazonGuardDutyMalwareProtectionServiceRolePolicy` collegato al servizio viene creato automaticamente negli account che hanno abilitato la protezione GuardDuty da malware. Per ulteriori informazioni, consulta le autorizzazioni dei ruoli collegati ai servizi per la protezione GuardDuty da malware nella Amazon User Guide 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 affidabile solo tramite Amazon GuardDuty.

Amazon GuardDuty richiede un accesso affidabile AWS Organizations prima di poter designare un account membro come GuardDuty amministratore della tua organizzazione. Se configuri un amministratore delegato utilizzando la GuardDuty console, abilita GuardDuty automaticamente l'accesso affidabile per te.

Tuttavia, se desideri configurare un account di amministratore delegato utilizzando AWS CLI o uno dei seguenti AWS SDKs, devi richiamare esplicitamente l'operazione Enable AWSService Access e fornire l'entità del servizio come parametro. Quindi puoi chiamare EnableOrganizationAdminAccountper delegare l' GuardDuty account amministratore.

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 affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  Esegui il comando seguente per disabilitare Amazon GuardDuty come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal guardduty.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita AWSService l'accesso

Abilitazione di un account 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 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 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 Amazon User Guide GuardDuty

Designazione di 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 offre una visibilità continua sulle prestazioni delle risorse e sulla disponibilità dei vostri Servizi AWS account. AWS Health offre eventi in cui le AWS risorse e i servizi sono interessati da un problema o saranno influenzati da modifiche imminenti. Dopo aver abilitato la visualizzazione organizzativa, un utente dell'account di gestione dell'organizzazione può aggregare AWS Health gli eventi in tutti gli account dell'organizzazione. La visualizzazione organizzativa mostra solo AWS Health gli eventi distribuiti dopo l'attivazione della funzionalità e li conserva per 90 giorni.

È possibile abilitare la visualizzazione organizzativa utilizzando la AWS Health console, AWS Command Line Interface (AWS CLI) o l' AWS Health API.

Per ulteriori informazioni, consulta Aggregazione AWS Health degli eventi nella Guida per l'AWS Health utente.

Utilizza le seguenti informazioni per semplificare l'integrazione AWS Health con AWS Organizations.

Ruoli collegati ai servizi per l'integrazione

Il ruolo `AWSServiceRoleForHealth_Organizations` collegato al servizio consente di eseguire operazioni supportate AWS Health all'interno degli account dell'organizzazione all'interno dell'organizzazione.

Questo ruolo viene creato automaticamente nell'account di gestione dell'organizzazione quando si abilita l'accesso affidabile chiamando l'operazione EnableHealthServiceAccessForOrganizationAPI. Altrimenti, crea il ruolo utilizzando la AWS Health console, l'API o la CLI, come descritto in Creazione di un ruolo collegato al servizio nella Guida per l'utente IAM.

È possibile eliminare o modificare questo ruolo solo se si disabilita l'accesso affidabile tra AWS Health e Organizations o se si rimuove l'account membro dall'organizzazione.

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 responsabili 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 abiliti la funzionalità di visualizzazione organizzativa per AWS Health, anche l'accesso affidabile viene abilitato automaticamente.

È possibile abilitare l'accesso affidabile utilizzando la AWS Health console o la AWS Organizations console.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS Health console o gli strumenti per abilitare l'integrazione con Organizations. Ciò consente di AWS Health eseguire qualsiasi configurazione richiesta, ad esempio la creazione delle 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 affidabile utilizzando la AWS Health console o gli strumenti, non è necessario completare questi passaggi.

Per abilitare l'accesso affidabile tramite la AWS Health console

È possibile abilitare l'accesso affidabile utilizzando AWS Health una delle seguenti opzioni:

- Usa la AWS Health console. 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.

È possibile abilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile ai servizi:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitarlo AWS Health come servizio affidabile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: Abilita AWSService l'accesso

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 aver disabilitato la funzionalità di visualizzazione organizzativa, AWS Health interrompe l'aggregazione degli eventi per tutti gli altri account dell'organizzazione. Ciò, inoltre, disabilita automaticamente l'accesso attendibile.

Puoi disabilitare l'accesso affidabile utilizzando gli AWS Organizations strumenti AWS Health o.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS Health console o gli strumenti per disabilitare l'integrazione con Organizations. Ciò consente di AWS Health

eseguire tutte le operazioni di pulizia necessarie, ad esempio l'eliminazione di risorse o l'accesso a ruoli che non sono più necessari al servizio. Procedi con questi passaggi solo se non è possibile disabilitare l'integrazione utilizzando gli strumenti forniti da AWS Health. Se disabiliti l'accesso affidabile utilizzando la AWS Health console o gli strumenti, non è necessario completare questi passaggi.

Per disabilitare l'accesso affidabile tramite la AWS Health console

Puoi disabilitare l'accesso attendibile con una delle seguenti opzioni:

- Usa la AWS Health console. 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.

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  Esegui il comando seguente per disabilitarlo AWS Health come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal health.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita AWSService l'accesso

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

AWS Identity and Access Management e AWS Organizations

AWS Identity and Access Management è un servizio web per il controllo sicuro dell'accesso ai AWS servizi.

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 politiche di controllo dei servizi (SCPs) che limitano l'accesso solo ai AWS servizi 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.

IAM consente di gestire centralmente le credenziali degli utenti root ed eseguire attività privilegiate sugli account dei membri. Dopo aver abilitato la gestione degli accessi root, che consente l'accesso affidabile per IAM in AWS Organizations, puoi proteggere centralmente le credenziali utente root degli account dei membri. Gli account dei membri non possono accedere al proprio utente root o eseguirne il recupero della password. L'account di gestione o un account amministratore delegato per IAM possono inoltre eseguire alcune attività privilegiate sugli account dei membri utilizzando l'accesso root a breve termine. Le sessioni con privilegi a breve termine forniscono credenziali temporanee utilizzabili per intraprendere azioni con privilegi su un account membro dell'organizzazione.

Per ulteriori informazioni, consulta Gestire centralmente l'accesso root per gli account dei membri nella Guida per l'utente IAM.

Utilizza le seguenti informazioni per aiutarti a eseguire l'integrazione AWS Identity and Access Management con AWS Organizations.

Abilitare l'accesso affidabile con IAM

Quando abiliti la gestione degli accessi root, viene abilitato l'accesso affidabile per IAM in AWS Organizations.

Disabilitazione dell'accesso affidabile con IAM

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Solo un amministratore dell'account di AWS Organizations gestione può disabilitare l'accesso affidabile con AWS Identity and Access Management.

Puoi disabilitare l'accesso affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Identity and Access Managementnell'elenco dei servizi.
4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Nella finestra di AWS Identity and Access Management dialogo Disabilita l'accesso affidabile per, digita disabilita per confermare, quindi scegli Disabilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS Identity and Access Management che ora può disabilitare il funzionamento di quel servizio AWS Organizations utilizzando la console o gli strumenti di servizio.

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

  Esegui il comando seguente per disabilitarlo AWS Identity and Access Management come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal iam.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita AWSService l'accesso

Abilitazione di un account amministratore delegato per IAM

Quando si designa un account membro come amministratore delegato dell'organizzazione, gli utenti e i ruoli di tale account possono eseguire attività privilegiate sugli account dei membri che altrimenti possono essere eseguite solo da utenti o ruoli nell'account di gestione dell'organizzazione. Per ulteriori informazioni, consulta Esegui un'attività privilegiata su un account membro di Organizations nella IAM User Guide.

Solo un amministratore dell'account di gestione dell'organizzazione può configurare un amministratore delegato per IAM.

Puoi specificare un account amministratore delegato dalla console o dall'API IAM oppure utilizzando l'operazione Organizations CLI o SDK.

Disabilitazione di un amministratore delegato per IAM

Solo un amministratore dell'account di gestione Organizations o dell'account amministratore delegato IAM può rimuovere un account amministratore delegato dall'organizzazione. È possibile disabilitare l'amministrazione delegata utilizzando l'operazione Organizations `DeregisterDelegatedAdministrator` CLI o SDK.

Amazon Inspector e AWS Organizations

Amazon Inspector è un servizio automatizzato di gestione delle vulnerabilità che analizza continuamente i carichi di lavoro di EC2 Amazon e dei container alla ricerca di vulnerabilità del software ed esposizione involontaria della rete.

Con Amazon Inspector puoi gestire più account associati semplicemente delegando un account amministratore AWS Organizations 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 aiutarti a integrare 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 un accesso affidabile AWS Organizations prima di poter designare un account membro come amministratore delegato di questo servizio per la tua 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 amministratore delegato utilizzando la AWS CLI o uno dei seguenti, è necessario chiamare esplicitamente AWS SDKs l'operazione e fornire `EnableAWSServiceAccess` l'entità del servizio come parametro. Quindi è possibile chiamare `EnableDelegatedAdminAccount` per delegare l'account amministratore di Inspector.

È possibile abilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile ai servizi:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitare Amazon Inspector come servizio affidabile con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal inspector2.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: Abilita AWSService l'accesso

> **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 dell'account di AWS Organizations gestione può disabilitare l'accesso affidabile con Amazon Inspector.

Puoi disabilitare l'accesso affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  Esegui il comando seguente per disabilitare Amazon Inspector come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal inspector2.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita l'accesso AWSService

Abilitazione di un account amministratore delegato per Amazon Inspector

Con Amazon Inspector puoi gestire più account in un'organizzazione utilizzando un amministratore delegato con servizio. AWS Organizations

L'account di AWS Organizations gestione 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 amministratore delegato utilizzando la AWS CLI o uno dei seguenti, puoi utilizzare AWS SDKs i seguenti comandi:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal inspector2.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 Inspector

Solo un amministratore dell'account di AWS Organizations gestione può rimuovere un account 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 semplifica il processo di trasferimento delle licenze dei fornitori di software sul cloud. Man mano che costruisci un'infrastruttura cloud AWS, puoi risparmiare sui costi sfruttando le opportunità bring-your-own-license (BYOL), ovvero riadattando l'inventario delle licenze esistente per utilizzarlo 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 License Manager a AWS Organizations, è possibile:

- 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 semplificare l'integrazione 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 solo utilizzando 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 proprio account di AWS Organizations gestione e associarlo al proprio account License Manager. Per ulteriori informazioni, consulta Impostazioni in 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 affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

È possibile 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 License Manager come servizio affidabile 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
```

- AWS API: disabilita AWSService l'accesso

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.

AWS Managed Services (AMS) Segnalazione self-service (SSR) e AWS Organizations

AWS Managed Services (AMS) Self-Service Reporting (SSR) raccoglie dati da vari AWS servizi nativi e fornisce l'accesso ai report sulle principali offerte AMS. SSR fornisce le informazioni che è possibile utilizzare per supportare le operazioni, la gestione della configurazione, la gestione degli asset, la gestione della sicurezza e la conformità.

Dopo l'integrazione con AWS Organizations, puoi abilitare il reporting self-service aggregato (SSR). Si tratta di una funzionalità AMS che consente ai clienti di Advanced e Accelerate di visualizzare i report self-service esistenti aggregati a livello di organizzazione, su più account. Ciò offre visibilità su parametri operativi chiave come la conformità delle patch, la copertura dei backup e gli incidenti in tutti gli account gestiti da AMS all'interno. AWS Organizations

Utilizza le seguenti informazioni per aiutarti a integrare AWS Managed Services (AMS) Self-Service Reporting (SSR) 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 AMS 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 AMS e Organizations o se si rimuove l'account membro dall'organizzazione.

- `AWSServiceRoleForManagedServices_SelfServiceReporting`

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 AMS concedono l'accesso ai seguenti principali di servizio:

- `selfservicereporting.managedservices.amazonaws.com`

Abilitare l'accesso affidabile con AMS

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

È possibile abilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile ai servizi:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitare AWS Managed Services (AMS) Self-Service Reporting (SSR) come servizio affidabile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: Abilita l'accesso AWSService

Disabilitazione dell'accesso affidabile con AMS

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

Puoi disabilitare l'accesso affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  Esegui il comando seguente per disabilitare AWS Managed Services (AMS) Self-Service Reporting (SSR) come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal selfservicereporting.managedservices.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: disabilita l'accesso AWSService

Abilitazione di un account amministratore delegato per AMS

Gli account di amministratore delegato possono visualizzare i report AMS (come patch e backup) su tutti gli account in un'unica visualizzazione aggregata nella console AMS.

È possibile aggiungere un amministratore delegato utilizzando la console o l'API AMS o utilizzando l'operazione Organizations `RegisterDelegatedAdministrator` CLI o SDK.

Disabilitazione di un amministratore delegato per AMS

Solo un amministratore dell'account di gestione dell'organizzazione può configurare un amministratore delegato per AMS.

È possibile rimuovere l'amministratore delegato utilizzando la console o l'API AMS o utilizzando l'operazione Organizations `DeregisterDelegatedAdministrator` CLI o SDK.

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 aiutarti a integrare 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 un accesso affidabile per AWS Organizations designare un account membro come amministratore Macie della tua 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.

È possibile abilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile ai servizi:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitare Amazon Macie come servizio affidabile con Organizations.

```
$ aws organizations enable-aws-service-access \
```

```
    --service-principal macie.amazonaws.com
```

Questo comando non produce alcun output se ha esito positivo.

- AWS API: Abilita AWSService l'accesso

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 un accesso affidabile per AWS Organizations designare un account membro come amministratore Macie della tua 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 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.

Marketplace AWS crea e gestisce le licenze utilizzandole 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 semplificare l'integrazione 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. Questo ruolo consente di Marketplace AWS 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 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 di 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 affidabile utilizzando la Marketplace AWS console o la console. AWS Organizations

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la Marketplace AWS console o gli strumenti per abilitare l'integrazione con Organizations. Ciò consente di Marketplace AWS eseguire qualsiasi configurazione richiesta, ad esempio la creazione delle 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 affidabile utilizzando la Marketplace AWS console o gli strumenti, non è necessario completare questi passaggi.

Per abilitare l'accesso affidabile tramite la Marketplace AWS console

Consulta Creazione di un ruolo collegato ai servizi per Marketplace AWS nella Guida per gli acquirenti di Marketplace AWS .

È possibile abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli Marketplace AWSnell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di Marketplace AWS dialogo Abilita accesso affidabile per, digita enable per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore Marketplace AWS che ora può abilitare il funzionamento del servizio AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitarlo Marketplace AWS come servizio affidabile 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.
- AWS API: Abilita AWSService l'accesso

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 affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  Esegui il comando seguente per disabilitarlo Marketplace AWS come servizio affidabile 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.

- AWS API: disabilita AWSService l'accesso

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 uno o più OUs o uno o più account dell'organizzazione, ciascuno con il proprio set di prodotti approvati. I tuoi AWS 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 AWS nella Guida Marketplace 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 Guida Marketplace 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 dei AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli Marketplace AWS Private Marketplace nell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di dialogo Abilita accesso affidabile per Marketplace AWS Private Marketplace, digita enable per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore di Marketplace AWS Private Marketplace che ora può abilitare il funzionamento di quel servizio AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  Esegui 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 AWSService l'accesso

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 affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  Esegui 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 AWSService l'accesso

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 utilizzando la console Private Marketplace, consulta Creazione e gestione di un marketplace privato nella Guida all'Marketplace AWS acquisto

Marketplace AWS dashboard di approfondimenti sugli acquisti e AWS Organizations

Utilizzi la dashboard di Marketplace AWS Procurement Insights per visualizzare gli accordi e i dati di analisi dei costi per tutti gli AWS account della tua organizzazione. Se integrata con Organizations, la dashboard Marketplace AWS Procurement Insights ascolta le modifiche organizzative, ad esempio l'ingresso di un account nell'organizzazione, e aggrega i dati per i contratti corrispondenti per creare i relativi dashboard.

Per ulteriori informazioni, consulta Procurement insights nella Buyer Guide.Marketplace AWS

Utilizza le seguenti informazioni per aiutarti a integrare la dashboard di Marketplace AWS Procurement Insights con. AWS Organizations

Ruoli collegati ai servizi e politiche gestite creati quando abiliti l'integrazione

Quando si attiva la dashboard di Marketplace AWS Procurement Insights, vengono creati il ruolo `AWSServiceRoleForProcurementInsightsPolicy`collegato ai servizi e la `AWSServiceRoleForProcurementInsightsPolicy` AWS policy gestita.

Consentire un accesso affidabile con Procurement Insights Marketplace AWS

L'abilitazione dell'accesso affidabile garantisce alla dashboard di Marketplace AWS Procurement Insights la capacità di integrarsi con il servizio Organizations del cliente. Marketplace AWS la

dashboard di Procurement Insights ascolta le modifiche organizzative, ad esempio l'ingresso di un account nell'organizzazione, e aggrega i dati relativi ai contratti corrispondenti per creare dashboard.

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 dashboard di Marketplace AWS Procurement Insights o la console. AWS Organizations

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti del dashboard di Marketplace AWS Procurement Insights per abilitare l'integrazione con Organizations. Ciò consente alla dashboard Marketplace AWS di Procurement Insights 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 dalla dashboard di Marketplace AWS Procurement Insights. Per ulteriori informazioni, consulta questa nota.
> Se abiliti l'accesso affidabile utilizzando la console o gli strumenti del dashboard di Marketplace AWS Procurement Insights, non è necessario completare questi passaggi.

Per consentire un accesso affidabile abilitando la dashboard di Marketplace AWS Procurement Insights

Vedi Abilitazione della dashboard di Marketplace AWS Procurement Insights nella Guida all'Marketplace AWS acquisto.

Per abilitare l'accesso affidabile utilizzando gli strumenti Organizations

È possibile abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in uno dei AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli la dashboard Marketplace AWS di Procurement Insights nell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di dialogo Abilita accesso affidabile per il dashboard Marketplace AWS Procurement Insights, digita abilita per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore della dashboard di Marketplace AWS Procurement Insights che ora può abilitare il funzionamento di quel servizio AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitare il dashboard di Marketplace AWS Procurement Insights come servizio affidabile con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal procurement-insights.marketplace.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: Abilita AWSService l'accesso

Disabilitazione dell'accesso affidabile con Marketplace AWS Procurement Insights

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

Puoi disabilitare l'accesso affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  Esegui il comando seguente per disabilitare il dashboard Marketplace AWS di Procurement Insights come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal procurement-insights.marketplace.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita l'accesso AWSService

Abilitazione di un account amministratore delegato per Marketplace AWS gli approfondimenti sugli acquisti

Per configurare un amministratore delegato nella console Marketplace AWS Procurement Insights, consulta la sezione Registrazione degli amministratori delegati> nella Guida all'acquisto.Marketplace AWS

Puoi anche configurare un amministratore delegato utilizzando l'`RegisterDelegatedAdministrator`API Organizations. Per ulteriori informazioni, vedere RegisterDelegatedAdministratorOrganizations Command Reference.

Disabilitazione di un amministratore delegato per Marketplace AWS gli approfondimenti sugli acquisti

Solo un amministratore dell'account di gestione dell'organizzazione può configurare un amministratore delegato per Procurement Insights. Marketplace AWS

Per rimuovere un amministratore delegato tramite la console Marketplace AWS Procurement Insights, consulta Annullamento della registrazione degli amministratori delegati nella Guida all'acquisto.Marketplace AWS

Puoi anche rimuovere l'amministratore delegato utilizzando l'operazione Organizations `DeregisterDelegatedAdministrator` CLI o SDK.

AWS Network Manager e AWS Organizations

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. Con il supporto multiaccount puoi creare un'unica rete globale per tutti AWS i tuoi account e registrare i gateway di transito da più account alla 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 Network Manager per gestire le impostazioni di più account (amministratori enable/disable trusted access and register/deregister 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 affidabile per Network Manager nella console Network Manager, la console abilita anche il servizio. AWS CloudFormation StackSets Network Manager utilizza StackSets per distribuire i ruoli IAM personalizzati necessari per la gestione di più account.

Per ulteriori informazioni sull'integrazione di Network Manager con Organizations, consulta Gestione di più account in Network Manager con AWS Organizations nella Guida per l'utente di Amazon VPC.

Utilizza le seguenti informazioni per aiutarti a integrare 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 dell'account di gestione Organizations dispone delle autorizzazioni per abilitare l'accesso affidabile con un altro AWS servizio. 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 l'amministratore di un account di gestione Organizations dispone delle autorizzazioni per disabilitare l'accesso affidabile con un altro AWS servizio.

> **Important**
>
> Consigliamo vivamente di utilizzare la console Network Manager per disabilitare l'accesso attendibile. Se disabiliti l'accesso affidabile in qualsiasi altro modo, ad esempio utilizzando AWS CLI, con un'API o con la AWS CloudFormation console, i ruoli IAM distribuiti AWS CloudFormation StackSets e personalizzati 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.

Sviluppatore Amazon Q e AWS Organizations

Amazon Q Developer è un assistente conversazionale generativo basato sull'intelligenza artificiale che può aiutarti a comprendere, creare, estendere e utilizzare le applicazioni. AWS È anche un generatore di codice generico basato sull'apprendimento automatico che fornisce consigli sul codice in tempo reale. La versione in abbonamento a pagamento di Amazon Q Developer richiede l'integrazione di Organizations. Per ulteriori informazioni, consulta la configurazione di Account, IAM Identity Center and Organizations nella guida per l'utente di Amazon Q.

Utilizza le seguenti informazioni per aiutarti a integrare Amazon Q Developer con AWS Organizations.

Ruoli collegati ai servizi

Il ruolo `AWSServiceRoleForAmazonQDeveloper` collegato ai servizi consente ad Amazon Q Developer di eseguire operazioni supportate all'interno della tua organizzazione. Crea il ruolo utilizzando la console, l'API o la CLI di Amazon Q Developer, come descritto nella sezione Creazione di un ruolo collegato al servizio nella IAM User Guide.

Se utilizzi un account membro, puoi eliminare o modificare questo ruolo solo se disabiliti l'accesso affidabile tra Amazon Q Developer e Organizations o se rimuovi l'account membro dall'organizzazione.

Principali di servizio utilizzati da Amazon Q Developer

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 Q Developer concedono l'accesso ai seguenti principali di servizio:

- `q.amazonaws.com`

Abilitare l'accesso affidabile con Amazon Q Developer

Amazon Q Developer Pro utilizza l'accesso affidabile per condividere le impostazioni effettuate nell'account di gestione Organizations con gli account dei membri della stessa organizzazione.

Ad esempio, l'amministratore di Amazon Q Developer Pro, che lavora nell'account di gestione Organizations, può abilitare suggerimenti con riferimenti al codice. Se l'accesso affidabile è abilitato, i suggerimenti con riferimenti al codice verranno abilitati anche per tutti gli account membri di quell'organizzazione.

Puoi abilitare l'accesso affidabile solo utilizzando Amazon Q Developer.

Per abilitare l'accesso affidabile per Amazon Q Developer, utilizza questa procedura.

1. Nella pagina Impostazioni sviluppatore di Amazon Q, in Impostazioni dell'account membro, scegli Modifica.
2. Nella finestra pop-up, seleziona Attivato.
3. Seleziona Salva.

Per ulteriori informazioni, consulta Enabling trusted access nella guida per l'utente di Amazon Q Developer.

Disabilitazione dell'accesso affidabile con Amazon Q Developer

Puoi disabilitare l'accesso affidabile solo utilizzando gli strumenti Amazon Q Developer.

Per disabilitare l'accesso affidabile per Amazon Q Developer, usa questa procedura.

1. Nella pagina Impostazioni sviluppatore di Amazon Q, in Impostazioni dell'account membro, scegli Modifica.
2. Nella finestra pop-up, seleziona Disattivato.
3. Seleziona Salva.

Per ulteriori informazioni, consulta Enabling trusted access nella guida per l'utente di Amazon Q Developer.

AWS Resource Access Manager e AWS Organizations

AWS Resource Access Manager (AWS RAM) ti consente di condividere AWS risorse specifiche di tua proprietà con altri Account AWS. È un servizio centralizzato che offre un'esperienza coerente per la condivisione di diversi tipi di AWS risorse su più account.

Per ulteriori informazioni in merito AWS RAM, consulta la Guida per l'AWS RAM utente.

Utilizza le seguenti informazioni per facilitare l'integrazione 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. Questo ruolo consente di AWS RAM 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 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 di 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 affidabile utilizzando la AWS Resource Access Manager console o la console. AWS Organizations

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS Resource Access Manager console o gli strumenti per abilitare l'integrazione con Organizations. Ciò consente di AWS Resource Access Manager eseguire qualsiasi configurazione richiesta, ad esempio la creazione delle 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 affidabile utilizzando la AWS Resource Access Manager console o gli strumenti, non è necessario completare questi passaggi.

Per abilitare l'accesso affidabile tramite la AWS RAM console o la CLI

Consulta Abilitazione della condivisione con AWS Organizations nella Guida per l'utente di AWS RAM .

È possibile abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Resource Access Managernell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di AWS Resource Access Manager dialogo Abilita accesso affidabile per, digita enable per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS Resource Access Manager che ora può abilitare il funzionamento del servizio AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitarlo AWS Resource Access Manager come servizio affidabile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: Abilita AWSService l'accesso

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.

Puoi disabilitare l'accesso affidabile utilizzando gli AWS Resource Access Manager o gli AWS Organizations strumenti.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS Resource Access Manager console o gli strumenti per disabilitare l'integrazione con Organizations. Ciò consente di AWS Resource Access Manager eseguire tutte le operazioni di pulizia necessarie, ad esempio l'eliminazione di risorse o l'accesso a ruoli che non sono più necessari al 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 affidabile utilizzando la AWS Resource Access Manager console o gli strumenti, non è necessario completare questi passaggi.

Per disabilitare l'accesso affidabile tramite la AWS Resource Access Manager console o la CLI

Consulta Abilitazione della condivisione con AWS Organizations nella Guida per l'utente di AWS RAM .

È possibile disabilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Resource Access Managernell'elenco dei servizi.
4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Nella finestra di AWS Resource Access Manager dialogo Disabilita l'accesso affidabile per, digita disabilita per confermare, quindi scegli Disabilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS Resource Access Manager che ora può disabilitare il funzionamento di quel servizio AWS Organizations utilizzando la console o gli strumenti di servizio.

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

  Esegui il comando seguente per disabilitarlo AWS Resource Access Manager come servizio affidabile con Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal ram.amazonaws.com
```

Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita AWSService l'accesso

Esploratore di risorse AWS e AWS Organizations

Esploratore di risorse AWS è un servizio di ricerca e scoperta 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 IDs. Resource Explorer funziona in tutte AWS le regioni del tuo account per semplificare i carichi di lavoro interregionali.

Integrando Resource Explorer con AWS Organizations, puoi raccogliere prove da una fonte più ampia, includendo più prove Account AWS provenienti dalla tua organizzazione nell'ambito delle tue valutazioni.

Utilizza le seguenti informazioni per semplificare l'integrazione 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.

Resource Explorer richiede un accesso affidabile AWS Organizations prima di poter 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 di Esploratore di risorse AWS eseguire qualsiasi configurazione richiesta, ad esempio la creazione delle 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 configuri un amministratore delegato utilizzando la Esploratore di risorse AWS console, abilita Esploratore di risorse AWS automaticamente l'accesso affidabile per te.

È possibile abilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile ai servizi:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitarlo Esploratore di risorse AWS come servizio affidabile 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.

- AWS API: Abilita AWSService l'accesso

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 dell'account di AWS Organizations gestione può disabilitare l'accesso affidabile con Esploratore di risorse AWS.

È possibile disabilitare l'accesso affidabile utilizzando gli AWS Organizations strumenti Esploratore di risorse AWS o.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la Esploratore di risorse AWS console o gli strumenti per disabilitare l'integrazione con Organizations. Ciò consente di Esploratore di risorse AWS eseguire tutte le operazioni di pulizia necessarie, ad esempio l'eliminazione di risorse o l'accesso a ruoli che non sono più necessari al 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 affidabile utilizzando la Esploratore di risorse AWS console o gli strumenti, non è necessario completare questi passaggi.

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  Esegui il comando seguente per disabilitarlo Esploratore di risorse AWS come servizio affidabile 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.

- AWS API: disabilita AWSService l'accesso

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 le visualizzazioni di più account con qualsiasi account della tua organizzazione AWS Resource Access Manager tramite la creazione di 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 Esploratore di risorse AWS console, Resource Explorer abilita automaticamente l'accesso affidabile.

AWS CLI, AWS API

Se desideri configurare un account amministratore delegato utilizzando la AWS CLI o uno dei seguenti, puoi utilizzare AWS SDKs i seguenti comandi:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal resource-explorer-2.amazonaws.com
```

- AWS SDK: richiama l'`RegisterDelegatedAdministrator`operazione Organizations e il numero ID dell'account membro e identifica il 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 Account AWS i prodotti partner di terze parti Servizi AWS che utilizzi e 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 di AWS 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.

Disabilitazione dell'accesso affidabile con Security Hub

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso affidabile, consulta Autorizzazioni necessarie per disabilitare l'accesso affidabile nella Guida per l'AWS Organizations utente.

Prima di disabilitare l'accesso affidabile, consigliamo di collaborare con l'amministratore delegato dell'organizzazione per disabilitare Security Hub negli account dei membri e per ripulire le risorse del Security Hub in tali account.

Puoi disabilitare l'accesso affidabile utilizzando la AWS Organizations console, l'API Organizations o AWS CLI. Solo un amministratore dell'account di gestione Organizations può disabilitare l'accesso affidabile con Security Hub.

Per istruzioni su come disabilitare l'accesso affidabile con Security Hub, vedere Disabilitazione dell'integrazione di Security Hub con. AWS Organizations

Abilitazione di un 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 di AWS 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.

Disabilitazione di un amministratore delegato per Security Hub

Solo l'account di gestione dell'organizzazione può rimuovere l'account amministratore delegato di Security Hub.

Per cambiare l'amministratore delegato di Security Hub, è necessario prima rimuovere l'account amministratore delegato corrente e quindi designarne uno nuovo.

Se si utilizza la console Security Hub per rimuovere l'amministratore delegato in una regione, l'amministratore delegato viene rimosso automaticamente in tutte le regioni.

L'API Security Hub rimuove solo l'account amministratore delegato di Security Hub dalla regione in cui viene emessa la chiamata o il comando API. È necessario ripetere l'azione in altre regioni.

Se si utilizza l'API Organizations per rimuovere l'account amministratore delegato di Security Hub, questo viene rimosso automaticamente in tutte le regioni.

Per istruzioni sulla disabilitazione dell'amministratore delegato del Security Hub, vedere Rimozione o modifica dell'amministratore delegato.

Amazon S3 Storage Lens e AWS Organizations

Offrendo ad Amazon S3 Storage Lens un accesso affidabile alla tua organizzazione, consenti a quest'ultima di raccogliere e aggregare i parametri relativi a tutti i membri dell' Account AWS 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 aiutarti a integrare 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

Vedi Abilitazione dell'accesso affidabile per S3 Storage Lens nella Guida per l'utente di Amazon Simple Storage Service.

Puoi abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli Amazon S3 Storage Lens nell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di dialogo Abilita accesso affidabile per Amazon S3 Storage Lens, digita enable per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore di Amazon S3 Storage Lens che ora può abilitare il servizio in modo che funzioni AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitare Amazon S3 Storage Lens come servizio affidabile 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.
- AWS API: Abilita AWSService l'accesso

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 affidabile solo utilizzando gli strumenti di Amazon S3 Storage Lens.

Puoi disabilitare l'accesso affidabile utilizzando la console Amazon S3, AWS CLI o una qualsiasi delle. AWS SDKs

Per disabilitare l'accesso attendibile tramite la console Amazon S3

Consulta Disabilitazione dell'accesso affidabile per S3 Storage Lens 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, AWS CLI il o uno qualsiasi dei. AWS SDKs Per registrare un account membro come account amministratore delegato per la tua organizzazione utilizzando la console Amazon S3, consulta Registrazione di un amministratore delegato per S3 Storage Lens 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, il o uno qualsiasi dei AWS CLI . AWS SDKs Per annullare la registrazione di un amministratore delegato utilizzando la console Amazon S3, consulta Annullamento della registrazione di un amministratore delegato per S3 Storage Lens nella Guida per l'utente di Amazon Simple Storage Service.

AWS Risposta agli incidenti di sicurezza e AWS Organizations

AWS Security Incident Response è un servizio di sicurezza che fornisce supporto in tempo reale, 24 ore su 24, 7 giorni su 7, con assistenza umana, per aiutare i clienti a rispondere rapidamente agli incidenti di sicurezza informatica come il furto di credenziali e gli attacchi ransomware. L'integrazione con Organizations abilita la copertura di sicurezza per l'intera organizzazione. Per ulteriori informazioni, consulta la sezione Gestione degli account AWS Security Incident Response AWS Organizations nella Security Incident Response User Guide.

Utilizza le seguenti informazioni per aiutarti a integrare AWS Security Incident Response 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.

- `AWSServiceRoleForSecurityIncidentResponse`- utilizzato per creare l'iscrizione a Security Incident Response, tramite l'iscrizione al servizio AWS Organizations.
- `AWSServiceRoleForSecurityIncidentResponse_Triage`- utilizzato solo quando abiliti la funzione di triage durante la registrazione.

Principali del servizio utilizzati da Security Incident Response

I ruoli collegati ai servizi nella sezione precedente possono essere assunti solo dai responsabili del servizio autorizzati dalle relazioni fiduciarie definite per il ruolo. I ruoli collegati ai servizi utilizzati da Security Incident Response concedono l'accesso al seguente responsabile del servizio:

- `security-ir.amazonaws.com`

Abilitazione dell'accesso affidabile a Security Incident Response

L'abilitazione dell'accesso affidabile a Security Incident Response consente al servizio di tenere traccia della struttura dell'organizzazione e di garantire che tutti gli account dell'organizzazione abbiano una copertura attiva degli incidenti di sicurezza. Inoltre, consente al servizio di utilizzare un ruolo collegato al servizio negli account dei membri per le funzionalità di triaging quando si abilita la funzione di triage.

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

È possibile abilitare l'accesso affidabile utilizzando la console AWS Security Incident Response o la console. AWS Organizations

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la console o gli strumenti AWS di Security Incident Response per abilitare l'integrazione con Organizations. Ciò consente a AWS Security Incident Response 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 AWS Security Incident Response. Per ulteriori informazioni, consulta questa nota.
Se abiliti l'accesso affidabile utilizzando la console o gli strumenti di AWS Security Incident Response, non è necessario completare questi passaggi.

Organizations abilita automaticamente l'accesso affidabile dell'organizzazione quando si utilizza la console Security Incident Response per la configurazione e la gestione. Se utilizzi Security Incident Response CLI/SDK, devi abilitare manualmente l'accesso affidabile utilizzando l'API Enable AWSService Access. Per informazioni su come abilitare l'accesso affidabile tramite la console Security Incident Response, consulta Abilitazione dell'accesso affidabile per la gestione degli AWS account nella Guida per l'utente di Security Incident Response.

È possibile abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Security Incident Response nell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di dialogo Abilita accesso affidabile per AWS Security Incident Response, digita enable per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore di AWS Security Incident Response che ora può abilitare il funzionamento di quel servizio AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitare AWS Security Incident Response come servizio affidabile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: Abilita AWSService l'accesso

Disabilitazione dell'accesso affidabile con Security Incident Response

Solo un amministratore dell'account di gestione Organizations può disabilitare l'accesso affidabile con Security Incident Response.

Puoi disabilitare l'accesso affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Security Incident Response nell'elenco dei servizi.
4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Nella finestra di dialogo Disabilita l'accesso affidabile per AWS Security Incident Response, digita disable per confermare, quindi scegli Disabilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore di AWS Security Incident Response che ora può disabilitare il funzionamento di quel servizio AWS Organizations utilizzando la console o gli strumenti del servizio.

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

  Esegui il comando seguente per disabilitare AWS Security Incident Response come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal security-ir.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita AWSService l'accesso

Abilitazione di un account amministratore delegato per Security Incident Response

Quando si designa un account membro come amministratore delegato dell'organizzazione, gli utenti e i ruoli di tale account possono eseguire azioni amministrative per Security Incident Response che altrimenti possono essere eseguite solo da utenti o ruoli nell'account di gestione dell'organizzazione. Ciò consente di separare la gestione dell'organizzazione dalla gestione del Security Incident Response. Per ulteriori informazioni, vedere Gestione degli account AWS Security Incident Response AWS Organizations nella Security Incident Response User Guide.

> **Autorizzazioni minime**
>
> Solo un utente o un ruolo nell'account di gestione Organizations può configurare un account membro come amministratore delegato per Security Incident Response nell'organizzazione.

Per informazioni su come configurare un amministratore delegato tramite la console Security Incident Response, vedere Designazione di un account amministratore delegato di Security Incident Response nella Security Incident Response User Guide.

AWS CLI, AWS API

Se desideri configurare un account amministratore delegato utilizzando la AWS CLI o uno dei seguenti, puoi utilizzare AWS SDKs i seguenti comandi:

- AWS CLI:

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

- AWS SDK: richiama l'`RegisterDelegatedAdministrator`operazione Organizations e il numero ID dell'account membro e identifica il servizio dell'account `security-ir.amazonaws.com` come parametri.

Disattivazione di un amministratore delegato per Security Incident Response

> **Important**
>
> Se l'iscrizione è stata creata dall'account amministratore delegato, l'annullamento della registrazione dell'amministratore delegato è un'azione distruttiva e causerà l'interruzione del servizio. Per registrare nuovamente DA:
>
> 1. Accedi alla console Security Incident Response all'indirizzo https://console.aws.amazon.com/security-ir/ home#/membership/settings
> 2. Annulla l'iscrizione dalla console di servizio. L'iscrizione rimane attiva fino alla fine del ciclo di fatturazione.
> 3. Una volta annullata l'iscrizione, disabilita l'accesso al servizio tramite la console Organizations, la CLI o l'SDK.

Solo un amministratore dell'account di gestione Organizations può rimuovere un amministratore delegato per Security Incident Response. Puoi rimuovere l'amministratore delegato utilizzando la CLI o l'operazione SDK `DeregisterDelegatedAdministrator` di Organizations.

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 al servizio viene creato automaticamente nell'account di gestione della tua organizzazione quando chiami l'RegisterDataLakeDelegatedAdministratorAPI. 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`

> ⚠ Raccomandazione: utilizza l' RegisterDataLakeDelegatedAdministratorAPI di Security Lake per consentire a Security Lake l'accesso alla tua organizzazione e per registrare l'amministratore delegato dell'organizzazione
>
> Se si utilizza Organizations APIs per registrare un amministratore delegato, è possibile che i ruoli collegati ai servizi per le Organizzazioni non vengano creati correttamente. Per garantire la piena funzionalità, utilizza Security Lake. APIs

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 affidabile solo utilizzando gli strumenti Organizations.

È possibile abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in uno dei AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli Amazon Security Lake nell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di dialogo Abilita accesso affidabile per Amazon Security Lake, digita abilita per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore di Amazon Security Lake che ora può abilitare il funzionamento di quel servizio AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitare Amazon Security Lake come servizio affidabile 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 AWSService l'accesso

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 affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli Amazon Security Lake nell'elenco dei servizi.
4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Nella finestra di dialogo Disabilita l'accesso affidabile per Amazon Security Lake, digita disable per confermare, quindi scegli Disabilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore di Amazon Security Lake che ora può disabilitare l'utilizzo di quel servizio AWS Organizations utilizzando la console o gli strumenti di servizio.

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

  Esegui il comando seguente per disabilitare Amazon Security Lake come servizio affidabile 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 AWSService l'accesso

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'operazione `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 dei seguenti, puoi utilizzare AWS SDKs 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'operazione `DeregisterDataLakeDelegatedAdministrator` API Amazon Security Lake, il comando `deregister-data-lake-delegated-administrator` 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 portafogli e la copia dei prodotti all'interno dell'organizzazione. Gli amministratori di Service Catalog possono fare riferimento a un'organizzazione esistente AWS Organizations quando condividono un portfolio e possono condividere il portfolio con qualsiasi unità organizzativa (OU) affidabile nella struttura ad albero dell'organizzazione. Ciò elimina la necessità di condividere il portafoglio IDs e l'account ricevente deve fare riferimento manualmente all'ID del portafoglio durante l'importazione del portafoglio. 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 semplificare l'integrazione AWS Service Catalog con AWS Organizations.

Ruoli collegati ai servizi creato quando è stata abilitata l'integrazione

AWS Service Catalog non crea ruoli collegati ai servizi come parte dell'abilitazione dell'accesso affidabile.

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 affidabile utilizzando la AWS Service Catalog console o la AWS Organizations console.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS Service Catalog console o gli strumenti per abilitare l'integrazione con Organizations. Ciò consente di AWS Service Catalog eseguire qualsiasi configurazione richiesta, ad esempio la creazione delle 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 affidabile utilizzando la AWS Service Catalog console o gli strumenti, non è necessario completare questi passaggi.

Per abilitare l'accesso affidabile utilizzando la CLI o l'SDK di Service Catalog AWS

Chiama uno dei seguenti comandi o operazioni:

- AWS CLI: aws servicecatalog enable-aws-organizations-access
- AWS SDKs: Catalog: :Abilita AWSService l'accesso AWSOrganizations

È possibile abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Service Catalognell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di AWS Service Catalog dialogo Abilita accesso affidabile per, digita enable per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS Service Catalog che ora può abilitare il funzionamento del servizio AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitarlo AWS Service Catalog come servizio affidabile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: Abilita AWSService l'accesso

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 affidabile AWS Organizations mentre si utilizza Service Catalog, le condivisioni correnti non vengono eliminate, ma si impedisce la creazione di nuove condivisioni all'interno dell'organizzazione. Le condivisioni attuali non saranno sincronizzate con la struttura dell'organizzazione se quest'ultima cambia dopo questa operazione.

Per disabilitare l'accesso affidabile utilizzando la CLI o l'SDK di Service Catalog AWS

Chiama uno dei seguenti comandi o operazioni:

- AWS CLI: aws servicecatalog disable-aws-organizations-access
- AWS SDKs: AWSOrganizationsDisabilita l'accesso

È possibile disabilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Service Catalognell'elenco dei servizi.
4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Nella finestra di AWS Service Catalog dialogo Disabilita l'accesso affidabile per, digita disabilita per confermare, quindi scegli Disabilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS Service Catalog che ora può disabilitare il funzionamento di quel servizio AWS Organizations utilizzando la console o gli strumenti di servizio.

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

  Esegui il comando seguente per disabilitarlo AWS Service Catalog come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal servicecatalog.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita AWSService l'accesso

Service Quotas e AWS Organizations

Service Quotas è un AWS servizio che 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 a AWS Organizations, è possibile creare un modello di richiesta di quote per richiedere automaticamente aumenti di quota al momento della creazione degli account.

Per ulteriori informazioni su Service Quotas, consulta la Guida per l'utente di Service Quotas.

Utilizza le seguenti informazioni per aiutarti a integrare 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.

È possibile abilitare l'accesso affidabile solo utilizzando Service Quotas.

Puoi abilitare l'accesso affidabile utilizzando la console Service Quotas AWS CLI o l'SDK:

- Per abilitare l'accesso attendibile tramite la console Service Quotas

  Accedi con il tuo account di AWS Organizations gestione, 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 affidabile utilizzando Service Quotas AWS CLI o SDK

  Chiama il seguente comando o operazione:
  - AWS CLI: aws service-quotas associate-service-quota-template
  - AWS SDKs: AssociateServiceQuotaTemplate

AWS IAM Identity Center e AWS Organizations

AWS IAM Identity Center fornisce l'accesso Single Sign-On per tutte le tue applicazioni Account AWS e per il cloud. Si connette a Microsoft Active Directory AWS Directory Service per consentire agli utenti di quella directory di accedere a un portale di AWS accesso personalizzato utilizzando i nomi utente e le password di Active Directory esistenti. Dal portale di AWS accesso, gli utenti hanno accesso a tutte Account AWS le applicazioni cloud per le 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 semplificare l'integrazione 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 affidabile utilizzando la AWS IAM Identity Center console o la AWS Organizations console.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS IAM Identity Center console o gli strumenti per abilitare l'integrazione con Organizations. Ciò consente di AWS IAM Identity Center eseguire qualsiasi configurazione richiesta, ad esempio la creazione delle 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 affidabile utilizzando la AWS IAM Identity Center console o gli strumenti, non è necessario completare questi passaggi.

IAM Identity Center richiede un accesso affidabile 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 .

Puoi abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in uno dei AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS IAM Identity Centernell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di AWS IAM Identity Center dialogo Abilita accesso affidabile per, digita enable per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS IAM Identity Center che ora può abilitare il funzionamento del servizio AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitarlo AWS IAM Identity Center come servizio affidabile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: Abilita AWSService l'accesso

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 un accesso affidabile AWS Organizations per funzionare. Se disabiliti l'accesso affidabile AWS Organizations mentre utilizzi IAM Identity Center, smette di funzionare perché 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 affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS IAM Identity Centernell'elenco dei servizi.
4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Nella finestra di AWS IAM Identity Center dialogo Disabilita l'accesso affidabile per, digita disabilita per confermare, quindi scegli Disabilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS IAM Identity Center che ora può disabilitare il funzionamento di quel servizio AWS Organizations utilizzando la console o gli strumenti di servizio.

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

  Esegui il comando seguente per disabilitarlo AWS IAM Identity Center come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal sso.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: disabilita AWSService l'accesso

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 la visibilità e il controllo delle AWS risorse. Le seguenti funzionalità di Systems Manager funzionano con Organizations di Account AWS in tutta l'organizzazione:

- Systems Manager Explorer è una dashboard operativa personalizzabile che riporta informazioni sulle AWS risorse. È possibile sincronizzare i dati operativi Account AWS in tutta l'organizzazione

utilizzando Organizations and 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 .
- Systems Manager OpsCenter offre una posizione centrale in cui gli ingegneri operativi e i professionisti IT possono visualizzare, esaminare e risolvere gli elementi di lavoro operativi (OpsItems) relativi alle AWS risorse. Quando si utilizza OpsCenter con Organizations, supporta l'utilizzo OpsItems da un account di gestione (un account di gestione 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 azione:
  - Crea, visualizza e aggiorna OpsItems in un altro account.
  - Visualizza informazioni dettagliate sulle AWS risorse specificate OpsItems in un altro account.
  - Avvia i runbook di Systems Manager Automation per risolvere i problemi relativi alle AWS risorse di un altro account.

  Per ulteriori informazioni, consulta AWS Systems Manager OpsCenter nella Guida per l'utente di AWS Systems Manager .
- Utilizzate Quick Setup per configurare rapidamente AWS i servizi e le funzionalità utilizzati di frequente con le best practice consigliate. Per ulteriori informazioni, consulta AWS Systems Manager Quick Setup nella Guida per l'utente di AWS Systems Manager .

  Quando si registra un account amministratore AWS Organizations delegato per Systems Manager, è possibile creare, aggiornare, visualizzare ed eliminare i gestori di configurazione Quick Setup destinati alle unità organizzative di un'organizzazione. Scopri di più in Utilizzo di un amministratore delegato per la configurazione rapida nella Guida per l'AWS Systems Manager utente.
- Quando si configura la console integrata per Systems Manager, si immette un account amministratore delegato. Questo account viene utilizzato per registrare gli account di amministratore AWS Organizations delegato con Quick Setup CloudFormation StackSets, Explorer e Resource Explorer. Scopri di più nella Guida per l'AWS Systems Manager utente alla configurazione della console integrata Systems Manager per un'organizzazione.

Utilizza le seguenti informazioni per semplificare l'integrazione 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 affidabile solo utilizzando gli strumenti Organizations.

È possibile abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in uno dei AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Systems Managernell'elenco dei servizi.

4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di AWS Systems Manager dialogo Abilita accesso affidabile per, digita enable per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS Systems Manager che ora può abilitare il funzionamento del servizio AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitarlo AWS Systems Manager come servizio affidabile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: Abilita AWSService l'accesso

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 un accesso affidabile con AWS Organizations per sincronizzare i dati operativi Account AWS all'interno dell'organizzazione. Se disabiliti l'accesso attendibile, Systems Manager non riesce a sincronizzare i dati delle operazioni e segnala un errore.

Puoi disabilitare l'accesso affidabile solo utilizzando gli strumenti Organizations.

È possibile disabilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Systems Managernell'elenco dei servizi.
4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Nella finestra di AWS Systems Manager dialogo Disabilita l'accesso affidabile per, digita disabilita per confermare, quindi scegli Disabilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS Systems Manager che ora può disabilitare il funzionamento di quel servizio AWS Organizations utilizzando la console o gli strumenti di servizio.

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

  Esegui il comando seguente per disabilitarlo AWS Systems Manager come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ssm.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita AWSService l'accesso

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 Account AWS che è stato designato come account per la gestione dei modelli di modifica, delle richieste di modifica, dei runbook delle modifiche e dei 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.
- Per la configurazione rapida, vedi Registrazione di un amministratore delegato per la configurazione rapida.

Disattivazione di un account amministratore delegato per Systems Manager

Per annullare la registrazione di un amministratore delegato, consulta i seguenti argomenti nella Guida per l'utente:AWS Systems Manager

- Per Explorer e OpsCenter, consulta Annullare la registrazione di un amministratore delegato Explorer.
- Per Change Manager, consulta Impostazione di un'organizzazione e di un account delegato per Change Manager.
- Per la configurazione rapida, vedi Annullare la registrazione di un amministratore delegato per la configurazione rapida.

Notifiche all'utente AWS e AWS Organizations

Notifiche all'utente AWSè una posizione centrale per AWS le tue notifiche.

Dopo l'integrazione con AWS Organizations, puoi configurare e visualizzare le notifiche centralmente su tutti gli account della tua organizzazione.

Utilizza le seguenti informazioni per semplificare l'integrazione Notifiche all'utente 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 di Notifiche all'utente 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 Notifiche all'utente e Organizations o se rimuovi l'account membro dall'organizzazione.

- `AWSServiceRoleForAWSUserNotifications`

Per ulteriori informazioni, consulta Using Service-Linked Roles nella Guida per l'Notifiche all'utente AWS utente.

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 Notifiche all'utente concedono l'accesso ai seguenti principali di servizio:

- `notifications.amazon.com`

Abilitazione dell'accesso attendibile con Notifiche all'utente

Per informazioni sulle autorizzazioni necessarie per abilitare l'accesso attendibile, consulta Autorizzazioni necessarie per abilitare l'accesso sicuro.

È possibile abilitare l'accesso affidabile solo utilizzando. Notifiche all'utente AWS

Per abilitare l'accesso affidabile tramite la Notifiche all'utente console, consulta Enabling AWS Organizations in Notifiche all'utente AWS nella Guida Notifiche all'utente per l'utente.

Disabilitazione dell'accesso attendibile con Notifiche all'utente

Per informazioni sulle autorizzazioni necessarie per disabilitare l'accesso attendibile, consulta Autorizzazioni necessarie per disabilitare l'accesso sicuro.

È possibile abilitare l'accesso affidabile solo utilizzando Notifiche all'utente AWS.

Per disabilitare l'accesso affidabile tramite la Notifiche all'utente console, vedere Enabling AWS Organizations in Notifiche all'utente AWS nella Guida Notifiche all'utente per l'utente.

Abilitazione di un account amministratore delegato per Notifiche all'utente

L'amministratore dell'account di gestione può delegare le autorizzazioni Notifiche all'utente amministrative 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 Notifiche all'utente amministrative, come creare esperienze, aggiornare le impostazioni di branding, associare o dissociare i destinatari, aggiungere o rimuovere prodotti e approvare o rifiutare le richieste in sospeso.

Per configurare un amministratore delegato utilizzando la Notifiche all'utente console, consulta Registrazione degli amministratori delegati nella Guida per l'utente. Notifiche all'utente AWSNotifiche all'utente

Puoi anche configurare un amministratore delegato utilizzando l'`RegisterDelegatedAdministrator`API Organizations. Per ulteriori informazioni, vedere RegisterDelegatedAdministratorOrganizations Command Reference.

Disabilitazione di un amministratore delegato per Notifiche all'utente

Solo un amministratore dell'account di gestione dell'organizzazione può configurare un amministratore delegato per. Notifiche all'utente

È possibile rimuovere l'amministratore delegato utilizzando la Notifiche all'utente console o l'API oppure utilizzando l'operazione Organizations `DeregisterDelegatedAdministrator` CLI o SDK.

Per disabilitare l' Notifiche all'utente account amministratore delegato utilizzando la Notifiche all'utente console, consulta la sezione Rimozione degli amministratori delegati nella Guida per l'utente. Notifiche all'utente AWSNotifiche all'utente

Policy di tag e AWS Organizations

Le politiche relative ai tag sono un tipo di politica AWS Organizations che può aiutarti a standardizzare i tag tra le risorse degli account della tua organizzazione. Per ulteriori informazioni sulle policy di tag, consulta Policy di tag.

Utilizza le seguenti informazioni per aiutarti a integrare le politiche sui 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

Puoi abilitare l'accesso affidabile abilitando le politiche di tag nell'organizzazione o utilizzando la AWS Organizations console.

> **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, consulta Abilitazione di un tipo di policy.

È possibile abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in una delle AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli le politiche relative ai tag nell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di dialogo Abilita accesso affidabile per le politiche sui tag, digita abilita per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore delle politiche di tag che ora può abilitare il funzionamento di quel servizio AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

  Esegui il comando seguente per abilitare le politiche dei tag come servizio affidabile con Organizations.

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

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: Abilita AWSService l'accesso

Disabilitazione dell'accesso attendibile con le policy di tag

È possibile disabilitare l'accesso affidabile per le politiche di tag disabilitando il tipo di politica dei tag nella AWS Organizations console. Per ulteriori informazioni, consulta Disabilitazione di un tipo di policy.

AWS Trusted Advisor e AWS Organizations

AWS 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. Se integrato con Organizations, puoi ricevere i risultati dei Trusted Advisor controlli per tutti gli account della tua organizzazione e scaricare report per visualizzare i riepiloghi dei controlli e le eventuali risorse interessate.

Per ulteriori informazioni, consulta Visualizzazione organizzativa per AWS Trusted Advisor nella Guida per l'utente di Supporto AWS .

Utilizza le seguenti informazioni per semplificare l'integrazione 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. Questo ruolo consente di Trusted Advisor 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 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 di 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 solo utilizzando. AWS Trusted Advisor

Per abilitare l'accesso affidabile tramite la Trusted Advisor console

Consulta Abilitazione della visualizzazione organizzativa nella Guida per l'utente di Supporto AWS .

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 aver disabilitato questa funzionalità, Trusted Advisor interrompe la registrazione delle informazioni sugli assegni 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 gli strumenti AWS Trusted Advisor o gli AWS Organizations strumenti.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS Trusted Advisor console o gli strumenti per disabilitare l'integrazione con Organizations. Ciò consente di AWS Trusted Advisor eseguire tutte le operazioni di pulizia necessarie, ad esempio l'eliminazione di risorse o l'accesso a ruoli che non sono più necessari al 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 affidabile utilizzando la AWS Trusted Advisor console o gli strumenti, non è necessario completare questi passaggi.

Per disabilitare l'accesso affidabile tramite la Trusted Advisor console

Consulta Disabilitazione della visualizzazione organizzativa nella Guida per l'utente di Supporto AWS .

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  Esegui il comando seguente per disabilitarlo AWS Trusted Advisor come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal reporting.trustedadvisor.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita AWSService l'accesso

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 Organizations può configurare un account membro come amministratore delegato per Trusted Advisor l'organizzazione.

Per istruzioni sull'attivazione di un account amministratore delegato per Trusted Advisor, consulta Registrare gli amministratori delegati nella Guida per l'utente.Supporto

AWS CLI, AWS API

Se desideri configurare un account amministratore delegato utilizzando la AWS CLI o uno dei seguenti, puoi utilizzare AWS SDKs i seguenti comandi:

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal reporting.trustedadvisor.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.

Disattivazione di un amministratore delegato per Trusted Advisor

È possibile rimuovere l'amministratore delegato utilizzando la Trusted Advisor console o l'operazione Organizations `DeregisterDelegatedAdministrator` CLI o SDK. Per informazioni su come disabilitare l' Trusted Advisor account amministratore delegato utilizzando la Trusted Advisor console, consulta Annullare la registrazione degli amministratori delegati nella guida per l'utente.Supporto

AWS Well-Architected Tool e AWS Organizations

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.

L'utilizzo AWS Well-Architected Tool con Organizations consente AWS Well-Architected Tool sia ai clienti di Organizations che a quelli di Organizations di semplificare il processo di condivisione AWS Well-Architected Tool delle risorse con gli altri membri della propria organizzazione.

Per ulteriori informazioni, consulta Condivisione delle risorse AWS Well-Architected Tool nella Guida per l'utente di AWS Well-Architected Tool .

Utilizza le seguenti informazioni per semplificare l'integrazione 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. Questo ruolo consente di AWS WA Tool 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 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 di servizio:

- `wellarchitected.amazonaws.com`

Abilitazione dell'accesso attendibile con AWS WA Tool

Consente l'aggiornamento di 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 affidabile utilizzando la AWS Well-Architected Tool console o la AWS Organizations console.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS Well-Architected Tool console o gli strumenti per abilitare l'integrazione con Organizations. Ciò consente di AWS Well-Architected Tool eseguire qualsiasi configurazione richiesta, ad esempio la creazione delle 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 affidabile utilizzando la AWS Well-Architected Tool console o gli strumenti, non è necessario completare questi passaggi.

Per abilitare l'accesso affidabile tramite la AWS WA Tool console

Vedi Condivisione AWS Well-Architected Tool delle risorse nella Guida AWS Well-Architected Tool per l'utente.

Puoi abilitare l'accesso affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in uno dei AWS SDKs.

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. Nel riquadro di navigazione, scegli Servizi.
3. Scegli AWS Well-Architected Toolnell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di AWS Well-Architected Tool dialogo Abilita accesso affidabile per, digita enable per confermare, quindi scegli Abilita accesso affidabile.
6. Se sei l'amministratore di Only AWS Organizations, comunica all'amministratore AWS Well-Architected Tool che ora può abilitare il funzionamento del servizio AWS Organizations dalla console di servizio.

AWS CLI, AWS API

Per abilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per abilitare l'accesso affidabile al servizio:

- AWS CLI: enable-aws-service-access

Esegui il comando seguente per abilitarlo AWS Well-Architected Tool come servizio affidabile con Organizations.

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

Questo comando non produce alcun output se ha esito positivo.

- AWS API: Abilita AWSService l'accesso

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 affidabile utilizzando gli strumenti AWS Well-Architected Tool o gli AWS Organizations strumenti.

> **Important**
>
> Ti consigliamo vivamente di utilizzare, quando possibile, la AWS Well-Architected Tool console o gli strumenti per disabilitare l'integrazione con Organizations. Ciò consente di AWS Well-Architected Tool eseguire tutte le operazioni di pulizia necessarie, ad esempio l'eliminazione di risorse o l'accesso a ruoli che non sono più necessari al 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 affidabile utilizzando la AWS Well-Architected Tool console o gli strumenti, non è necessario completare questi passaggi.

Per disabilitare l'accesso affidabile tramite la AWS WA Tool console

Vedi Condivisione AWS Well-Architected Tool delle risorse nella Guida AWS Well-Architected Tool per l'utente.

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  Esegui il comando seguente per disabilitarlo AWS Well-Architected Tool come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal wellarchitected.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.
- AWS API: disabilita AWSService l'accesso

Amazon VPC IP Address Manager (IPAM) e AWS Organizations

Amazon VPC IP Address Manager (IPAM) è una funzionalità VPC che semplifica la pianificazione, il monitoraggio e il monitoraggio degli indirizzi IP per i carichi di lavoro. AWS

L'utilizzo AWS Organizations consente di monitorare l'utilizzo degli indirizzi IP in tutta l'organizzazione e di condividere pool di indirizzi IP tra gli account dei 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 aiutarti a integrare Amazon VPC IP Address Manager (IPAM) 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 `IPAMEnableIpamOrganizationAdminAccount`.

- `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 un accesso affidabile AWS Organizations prima di poter designare un account membro come amministratore delegato di questo servizio per la tua organizzazione.

Puoi abilitare l'accesso attendibile utilizzando solo gli strumenti di Amazon VPC IP Address Manager (IPAM).

Se integri IPAM utilizzando la console IPAM o AWS Organizations utilizzando l'`EnableIpamOrganizationAdminAccount`API IPAM, concedi automaticamente l'accesso affidabile a IPAM. La concessione di un accesso attendibile crea il ruolo collegato ai servizi `AWS ServiceRoleForIPAM` nell'account di gestione e in tutti gli account membri dell'organizzazione. IPAM utilizza il ruolo collegato al servizio per monitorare le risorse di EC2 rete CIDRs associate all'interno dell'organizzazione e per archiviare le metriche relative all'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 puoi abilitare l'accesso affidabile con IPAM utilizzando la AWS Organizations console o 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 dell'account di AWS Organizations gestione può disabilitare l'accesso affidabile con IPAM utilizzando l' AWS Organizations `disable-aws-service-access`API.

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.

È possibile disabilitare l'accesso affidabile eseguendo un AWS CLI comando Organizations o chiamando un'operazione dell'API Organizations in uno dei AWS SDKs.

AWS CLI, AWS API

Per disabilitare l'accesso al servizio attendibile tramite la CLI/gli SDK di Organizations

Utilizza i seguenti AWS CLI comandi o operazioni API per disabilitare l'accesso affidabile ai servizi:

- AWS CLI: disable-aws-service-access

  Esegui il comando seguente per disabilitare Amazon VPC IP Address Manager (IPAM) come servizio affidabile con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ipam.amazonaws.com
  ```

  Questo comando non produce alcun output se ha esito positivo.

- AWS API: disabilita l'accesso AWSService

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 maggiori informazioni, vedi enable-ipam-organization-admin-account nel AWS AWS CLI Command Reference.

> **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 il AWS AWS CLI, vedi disable-ipam-organization-admin-account nella Guida ai AWS AWS CLI comandi.

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.

Amazon VPC Reachability Analyzer 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 (). VPCs

L'utilizzo AWS Organizations con Reachability Analyzer consente di tracciare i percorsi tra gli account delle organizzazioni.

Per ulteriori informazioni, consulta Gestire gli account di amministratore delegato in Reachability Analyzer nella guida per l'utente di Reachability Analyzer.

Utilizza le seguenti informazioni per aiutarti a integrare 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 un accesso AWS Organizations affidabile prima di poter designare un account membro come amministratore delegato di 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 affidabile utilizzando la AWS Organizations console, eseguendo un AWS CLI comando o chiamando un'operazione API in uno dei. AWS SDKs

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 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 di Only AWS Organizations, comunica all'amministratore di Reachability Analyzer 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

  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.

- AWS API: Abilita AWSService l'accesso

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 con AWS 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, vedere RegisterDelegatedAdministratorOrganizations Command Reference.

> **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 con AWS 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 Servizi AWS quel lavoro con Organizations

Si consiglia di utilizzare l'account di AWS Organizations gestione e i relativi utenti e ruoli solo per le attività che devono essere eseguite da tale account. Si consiglia inoltre di archiviare AWS le risorse negli account di altri membri dell'organizzazione e di tenerle lontane dall'account di gestione. Questo perché le funzionalità di sicurezza come Organizations service control policies (SCPs) 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 di Servizi AWS quelli 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 Servizi AWS che puoi usare 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 Servizi AWS che puoi usare 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 Servizi AWS che puoi usare 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 organizzativa, tutti gli account e OUs le politiche organizzative
- Appartenenze
- Tutti gli account e OUs.
- 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 funziona Servizi AWS 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 maggiori informazioni sui programmi di conformità applicabili AWS Organizations, consulta Servizi AWS la sezione 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. Imparerai anche a utilizzarne altri Servizi AWS 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 VPCs, consulta la Amazon VPC User Guide.

Per connettere il tuo Amazon VPC AWS Organizations, devi prima definire un endpoint VPC di interfaccia (endpoint di interfaccia). Gli endpoint dell'interfaccia sono rappresentati da una o più interfacce di rete elastiche (ENIs) a cui vengono assegnati indirizzi IP privati dalle sottoreti del 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 per AWS Organizations
- 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 per AWS Organizations

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 VPCEndpoint risorsa AWS:::EC2: nella AWS CloudFormation User Guide.

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 Controllo degli accessi agli endpoint VPC tramite le policy degli endpoint nella Guida per l'utente di Amazon VPC.

Esempio: policy di endpoint VPC per le operazioni dell' AWS Organizations

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "Organizations:DescribeAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

Identity and Access Management per AWS Organizations

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Organizations. IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

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

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

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

su come la tua azienda può utilizzare IAM with Organizations, consultaCome AWS Organizations funziona con IAM.

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

Autenticazione con identità

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

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

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

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

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

Account AWS utente root

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

Identità federata

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

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

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

Utenti e gruppi IAM

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

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti

alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per amministrare le risorse IAM.

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

Ruoli IAM

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

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

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Create a role for a third-party identity provider (federation) nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso inoltrato (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che AWS CLI effettuano richieste AWS API. È preferibile archiviare le chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni.

AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

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

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

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

Policy basate sull'identità

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

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

Policy basate sulle risorse

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

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

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

Elenchi di controllo degli accessi () ACLs

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

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

Altri tipi di policy

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

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

- Politiche di controllo delle risorse (RCPs): RCPs sono politiche JSON che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le politiche IAM allegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di Servizi AWS tale supporto RCPs, vedere Resource control policies (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

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

Come AWS Organizations funziona con IAM

Prima di utilizzare IAM per gestire l'accesso alle Organizzazioni, scopri quali funzionalità IAM sono disponibili per l'uso con Organizations.

Funzionalità IAM	Organizations support
Policy basate su identità	Sì
Policy basate su risorse	Sì
Azioni di policy	Sì
Risorse relative alle policy	Sì

Funzionalità IAM	Organizations support
Chiavi di condizione della policy (specifica del servizio)	Sì
ACLs	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	No
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	Sì

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

Politiche basate sull'identità per Organizations

Supporta le policy basate su identità: sì

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

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

Esempi di policy basate sull'identità per Organizations

Per visualizzare esempi di politiche basate sull'identità di Organizations, vedere. Esempi di policy basate su identità per AWS Organizations

Politiche basate sulle risorse all'interno di Organizations

Supporta le policy basate sulle risorse: sì

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

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

Il servizio Organizations supporta solo un tipo di policy basata sulle risorse, denominata policy di delega basata sulle risorse, che specifica quali account membro possono eseguire azioni sulle policy. Puoi aggiungere più istruzioni nella policy per indicare un diverso set di autorizzazioni per gli account membri.

Per ulteriori informazioni, consulta Amministratore delegato per AWS Organizations.

Esempi di policy basate sulle risorse all'interno di Organizations

Per visualizzare esempi di politiche basate sulle risorse di Organizations, consulta, Esempi di policy basate sulle risorse per AWS Organizations

Azioni politiche per le Organizzazioni

Supporta le operazioni di policy: si

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

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

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

Per visualizzare un elenco delle azioni di Organizations, vedere Actions defined by AWS Organizations nel Service Authorization Reference.

Le azioni politiche in Organizations utilizzano il seguente prefisso prima dell'azione:

```
organizations
```

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

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

Per visualizzare esempi di politiche basate sull'identità di Organizations, vedere. Esempi di policy basate su identità per AWS Organizations

Risorse politiche per Organizzazioni

Supporta le risorse di policy: sì

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

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). È

possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

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

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

Per visualizzare un elenco dei tipi di risorse Organizations e relativi ARNs, vedere Resources defined by AWS Organizations nel Service Authorization Reference. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta la sezione Operazioni definite da AWS Organizations.

Per visualizzare esempi di politiche basate sull'identità di Organizations, vedere. Esempi di policy basate su identità per AWS Organizations

Chiavi relative alle condizioni delle policy per Organizations

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

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

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

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

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

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

Per visualizzare un elenco delle chiavi di condizione di Organizations, vedere Condition keys for AWS Organizations nel Service Authorization Reference. Per sapere con quali azioni e risorse è possibile utilizzare una chiave di condizione, consulta Azioni definite da AWS Organizations.

Per visualizzare esempi di politiche basate sull'identità di Organizations, vedere. Esempi di policy basate su identità per AWS Organizations

ACLs in Organizations

Supporti ACLs: no

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

ABAC con Organizations

Supporta ABAC (tag nelle policy): sì

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

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

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

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

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

Utilizzo di credenziali temporanee con Organizations

Supporta credenziali temporanee: No

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

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

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

Sessioni di accesso diretto per Organizations

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

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

Ruoli di servizio per Organizations

Supporta i ruoli di servizio: sì

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

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

Ruoli collegati ai servizi per Organizations

Supporta ruoli collegati ai servizi: Sì

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

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Gestione delle autorizzazioni di accesso per un'organizzazione con AWS Organizations

Tutte le AWS risorse, incluse le radici OUs, gli account e le politiche di un'organizzazione, sono di proprietà di un Account AWS e le autorizzazioni per creare o accedere a una risorsa sono regolate dalle politiche di autorizzazione. Per un'organizzazione, l'account di gestione possiede tutte le risorse. Un amministratore di account può controllare l'accesso alle AWS risorse associando politiche 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 le migliori pratiche di sicurezza in IAM nella Guida di riferimento.Gestione dell'account AWS

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.

AWS Organizations risorse e operazioni

Questa sezione illustra come i concetti si associano ai AWS Organizations concetti equivalenti a IAM.

Risorse

In AWS Organizations, puoi controllare l'accesso alle seguenti risorse:

- La radice e il OUs 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 in AWS Organizations, vedere Tipi di risorse definiti da AWS Organizations nel Service Authorization Reference.

Operazioni

AWS fornisce una serie di operazioni per utilizzare le risorse di 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 di AWS Organizations operazioni che possono essere utilizzate come autorizzazioni in una policy IAM, consulta Azioni definite dalle organizzazioni 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 su cui è possibile interrogare per fornire un controllo più granulare su determinate azioni. 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.

I seguenti tasti di condizione sono particolarmente utili con AWS Organizations:

- `aws:PrincipalOrgID` - Semplifica la determinazione dell'elemento `Principal` in una policy basata su risorse. Questa chiave globale offre un'alternativa all'elenco di tutti IDs gli account Account AWS 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 testuale della struttura di un' AWS Organizations entità. 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 di condizione corrisponde ai membri di una delle due persone OUs della 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:

  - `SERVICE_CONTROL_POLICY`
  - `RESOURCE_CONTROL_POLICY`
  - `DECLARATIVE_POLICY_EC2`
  - `BACKUP_POLICY`
  - `TAG_POLICY`
  - `CHATBOT_POLICY`
  - `AISERVICES_OPT_OUT_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.

  JSON

```
{
    "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 operazioni Abilita AWSService accesso o Disabilita AWSService accesso 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 politica consente all'utente di specificare solo AWS Firewall Manager quando abilitare e disabilitare l'accesso affidabile con AWS Organizations.

  JSON

```
{
    "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

È Account AWS proprietario delle risorse create nell'account, indipendentemente da chi le ha create. In particolare, il proprietario Account AWS della risorsa è l'entità principale (ovvero l'utente root, un utente IAM o un ruolo IAM) che autentica la richiesta di creazione delle risorse. Per un'organizzazione, questo è sempre l'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 l'unità organizzativa).
- 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 illustra l'utilizzo di IAM nel contesto di 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 sono denominate policy basate sulle risorse.

Argomenti

- Policy di autorizzazione basate su identità (policy IAM)

Policy di autorizzazione basate su identità (policy IAM)

Puoi allegare policy alle identità IAM per consentire a tali identità di eseguire operazioni sulle risorse. AWS Ad esempio, puoi eseguire le operazioni seguenti:

- Allega una politica di autorizzazioni a un utente o a un gruppo nel tuo account: per concedere a un utente le autorizzazioni per creare una AWS Organizations risorsa, ad esempio una policy di controllo del servizio (SCP) o un'unità organizzativa, puoi allegare una politica 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 responsabile della politica di fiducia può anche essere un responsabile del AWS servizio se si desidera concedere le autorizzazioni a un AWS servizio per assumere il ruolo.

  Per ulteriori informazioni sull'uso di IAM per delegare le autorizzazioni, consulta Access Management nella IAM User Guide (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.

JSON

```
{
   "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.

JSON

```
{
   "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.

JSON

```
{
   "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.

Specifica degli elementi della policy: operazioni, condizioni, effetti e risorse

Per ogni AWS Organizations risorsa, il servizio definisce una serie di operazioni o azioni API che possono interagire con quella risorsa o manipolarla in qualche modo. Per concedere le autorizzazioni per queste operazioni, AWS Organizations definisce una serie di azioni che è possibile specificare in una politica. Ad esempio, per la risorsa OU, AWS Organizations definisce azioni come le seguenti:

- `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 di quanto specificato`Effect`, `organizations:CreateAccount` consente o nega all'utente le autorizzazioni per eseguire l' AWS Organizations `CreateAccount`operazione. 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 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 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).

Per ulteriori informazioni sulla sintassi e le descrizioni delle policy IAM, consulta il riferimento alla policy IAM JSON nella IAM User Guide.

Esempi di policy basate su identità per AWS Organizations

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

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

Per i dettagli sulle azioni e sui tipi di risorse definiti da Organizations, incluso il formato di ARNs per ogni tipo di risorsa, vedere Azioni, risorse e chiavi di condizione AWS Organizations nel Service Authorization Reference.

Argomenti

Best practice per le policy

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

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue policy. Ad esempio, è possibile

scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.

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

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

Utilizzo della console Organizations

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

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

Per garantire che gli utenti e i ruoli possano ancora utilizzare la console Organizations, collega anche l'Organizations `AWSOrganizationsFullAccess`o la policy `AWSOrganizationsReadOnlyAccess` AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

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

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

Concessione delle autorizzazioni complete di amministratore a un utente

Puoi creare una policy IAM che conceda autorizzazioni di AWS Organizations amministratore complete a un utente IAM della tua 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 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. Scegli Next (Successivo).

> **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 saperne di più 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"` non `"servicename:some*action"` sono entrambe valide in SCPs.

JSON

```
{
    "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 a nessun bambino. OUs Non viene concesso alcun accesso alla fatturazione. Tieni presente che questo non ti dà accesso amministrativo all' Account AWS interno dell'unità organizzativa. Concede solo le autorizzazioni per eseguire AWS Organizations operazioni sugli account all'interno dell'unità organizzativa specificata:

JSON

```
{
    "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 IDs l'unità organizzativa e l'organizzazione dalla AWS Organizations console o chiamando il. `List*` APIs 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 sulle quattro ARNs 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'entità di servizio diversa da quella per cui si trova AWS IAM Identity Center, questa politica non corrisponde e la richiesta viene rifiutata:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals" : {
                    "organizations:ServicePrincipal" : "sso.amazonaws.com"
                }
            }
        }
    ]
}
```

Per ulteriori informazioni sulle ARNs varie risorse, vedere Tipi di risorse definiti da AWS Organizations nel Service Authorization Reference.

Esempi di policy basate sulle risorse per AWS Organizations

I seguenti esempi di codice mostrano come è possibile utilizzare le policy di delega basate sulle risorse. Per ulteriori informazioni, consulta Amministratore delegato per AWS Organizations.

Argomenti

Esempio: visualizzare l'organizzazione OUs, gli account e le politiche

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

Questo esempio mostra come è possibile includere queste autorizzazioni nella politica 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.

Questo esempio di politica di delega concede le autorizzazioni necessarie per completare le azioni in modo programmatico dall'API o. AWS AWS CLI Per utilizzare questa politica di delega, sostituisci il testo AWS segnaposto con le tue informazioni. *AccountId* Quindi, segui le indicazioni in Amministratore delegato per AWS Organizations.

JSON

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

```
    "Statement": [
        {
            "Sid": "DelegatingNecessaryDescribeListActions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333: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: creare, leggere, aggiornare ed eliminare le politiche

È possibile creare una politica di delega basata sulle risorse che consenta all'account di gestione di delegare `create` e azioni per qualsiasi tipo di politica. `read` `update` `delete` Questo esempio mostra come è possibile delegare queste azioni per le politiche di controllo del servizio all'account membro,. *`MemberAccountId`* Le due risorse mostrate nell'esempio concedono l'accesso rispettivamente alle politiche di controllo dei servizi gestite dai clienti e AWS gestite dai clienti.

> **Important**
>
> Questa politica consente agli amministratori delegati di eseguire azioni specifiche sulle politiche create da qualsiasi account dell'organizzazione, incluso l'account di gestione.

Non consente agli amministratori delegati di allegare o scollegare le politiche perché non include le autorizzazioni necessarie per eseguire o eseguire azioni. `organizations:AttachPolicy` `organizations:DetachPolicy`

Questo esempio di politica di delega concede le autorizzazioni necessarie per completare le azioni in modo programmatico dall'API o. AWS AWS CLI Sostituisci il testo AWS segnaposto con e con *`MemberAccountId`* le tue informazioni*`ManagementAccountId`*. *`OrganizationId`* Quindi, segui le indicazioni in Amministratore delegato per AWS Organizations.

Esempio: politiche relative all'etichettatura e all'eliminazione dei tag

Questo esempio mostra come è possibile creare una politica di delega basata sulle risorse che consenta agli amministratori delegati di etichettare o rimuovere i tag dalle politiche di backup. Concede le autorizzazioni necessarie per completare le azioni in modo programmatico dall'API o. AWS AWS CLI

Per utilizzare questa politica di delega, sostituisci il testo AWS segnaposto con e con le *`MemberAccountId`* tue informazioni*`ManagementAccountId`*. *`OrganizationId`* Quindi, segui le indicazioni in Amministratore delegato per AWS Organizations.

Esempio: allega le politiche a una singola unità organizzativa o a un account

Questo esempio mostra come è possibile creare una politica di delega basata sulle risorse che consenta agli amministratori delegati di accedere alle politiche `detach` Organizations da un'unità organizzativa (OU) specificata `attach` o da un account specifico. Prima di delegare queste azioni, è necessario delegare le autorizzazioni necessarie per navigare nella struttura di un'organizzazione e visualizzare gli account che la compongono. Per maggiori dettagli, consulta Esempio: visualizzare l'organizzazione OUs, gli account e le politiche.

Important

- Sebbene questa politica consenta di allegare o scollegare i criteri dall'unità organizzativa o dall'account specificati, esclude i bambini e gli account minori. OUs OUs

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

Questo esempio di politica di delega concede le autorizzazioni necessarie per completare le azioni in modo programmatico dall'API o. AWS AWS CLI Per utilizzare questa politica di delega, sostituisci il testo AWS segnaposto per*MemberAccountId*, *ManagementAccountIdOrganizationId*, e con le tue informazioni. *TargetAccountId* Quindi, segui le indicazioni in Amministratore delegato per AWS Organizations.

Per delegare il collegamento e il distacco delle politiche a qualsiasi unità organizzativa o account delle organizzazioni, sostituisci la risorsa dell'esempio precedente con le seguenti risorse:

```
"Resource": [
    "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
    "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
    "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/backup_policy/
*"
]
```

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`.

> **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.

Questo esempio di politica di delega concede le autorizzazioni necessarie per completare le azioni in modo programmatico dall'API o. AWS AWS CLI Per utilizzare questa politica di delega, sostituisci

il testo AWS segnaposto per*MemberAccountId*, *ManagementAccountIdOrganizationId*, e con le tue informazioni. *RootId* Quindi, segui le indicazioni in Amministratore delegato per AWS Organizations.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DelegatingNecessaryDescribeListActions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListRoots",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListTagsForResource"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DelegatingNecessaryDescribeListActionsForSpecificPolicyType",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "organizations:DescribePolicy",
                "organizations:DescribeEffectivePolicy",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": "BACKUP_POLICY"
                }
            }
        },
        {
            "Sid": "DelegatingAllActionsForBackupPolicies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "organizations:CreatePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
                "organizations:AttachPolicy",
                "organizations:DetachPolicy",
                "organizations:EnablePolicyType",
                "organizations:DisablePolicyType"
            ],
            "Resource": [
                "arn:aws:organizations::111122223333:root/o-OrganizationId/
r-RootId",
                "arn:aws:organizations::111122223333:ou/o-OrganizationId/*",
                "arn:aws:organizations::111122223333:account/o-OrganizationId/*",
                "arn:aws:organizations::111122223333:policy/o-OrganizationId/
backup_policy/*"
            ],
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": "BACKUP_POLICY"
                }
            }
        }
    ]
}
```

AWS politiche gestite per AWS Organizations

Questa sezione identifica le politiche AWS gestite fornite da utilizzare per gestire l'organizzazione. Non è possibile modificare o eliminare una politica AWS gestita, ma è possibile allegarla o scollegarla alle entità dell'organizzazione in base alle esigenze.

AWS Organizations politiche gestite da utilizzare 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 è necessario scrivere personalmente la politica e, quando AWS aggiorna la politica in modo 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.

AWS politica gestita: AWSOrganizationsFullAccess

Fornisce tutte le autorizzazioni necessarie per creare e amministrare completamente un'organizzazione.

Visualizza la politica: `AWSOrganizationsFullAccess`.

AWS politica gestita: AWSOrganizationsReadOnlyAccess

Consente l'accesso in sola lettura alle informazioni sull'organizzazione. Non consente all'utente di apportare modifiche.

Visualizza la politica: `AWSOrganizationsReadOnlyAccess`.

AWS politica gestita: DeclarativePoliciesEC2Report

Questa politica viene utilizzata dal ruolo collegato al servizio AWSServiceRoleForDeclarativePoliciesEC2Report per consentirgli di descrivere gli stati degli attributi degli account per gli account dei membri.

Visualizza la politica: DeclarativePolicies EC2 Report.

Aggiornamenti alle politiche AWS gestite da Organizations

La tabella seguente descrive in dettaglio gli aggiornamenti alle politiche AWS gestite da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivi il feed RSS nella pagina della cronologia dei documenti di .

Modifica	Descrizione	Data
AWSOrganizationsFullAccess— aggiornato per consentire le autorizzazioni API dell'account necessarie per visualizzare o modificare un nome di account tramite la console Organizations.	È stata aggiunta l'`account:GetAccountInformation` azione per abilitare l'accesso alla visualizzazione del nome account di qualsiasi account in un'organizzazione e l'`account:PutAccountName` azione per abilitare l'accesso per modificare qualsiasi nome di account in un'organizzazione.	22 aprile 2025
DeclarativePoliciesEC2Report — Nuova politica gestita	È stata aggiunta la `DeclarativePoliciesEC2Report` policy per abilitare la funzionalità del ruolo `AWSServiceRoleForDeclarativePoliciesEC2Report` collegato al servizio.	22 novembre 2024
AWSOrganizationsReadOnlyAccess— aggiornato per consentire le autorizzazioni API dell'account necessarie per visualizzare l'indirizzo e-mail di un utente root (indirizzo e-mail).	È stata aggiunta l'`account:GetPrimaryEmail` azione per consentire l'accesso alla visualizzazione dell'indirizzo e-mail dell'utente root (per qualsiasi account membro di un'organizzazione) e l'`account:GetRegionOptStatus` azione per consentire l'accesso alla visualizzazione delle regioni abilitate per	6 giugno 2024

Modifica	Descrizione	Data
	qualsiasi account membro di un'organizzazione.	
AWSOrganizationsFullAccess— aggiornato per includere `Sid` elementi che descrivono la dichiarazione politica.	`Sid`Elementi aggiunti per la politica `AWSOrganizationsFullAccess` gestita.	6 febbraio 2024
AWSOrganizationsReadOnlyAccess— aggiornato per includere `Sid` elementi che descrivono la dichiarazione politica.	`Sid`Elementi aggiunti per la politica `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.	È stata aggiunta `account:ListRegions` l'`account:DisableRegion` azione `account:EnableRegion` e alla politica per abilitare 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.	È stata aggiunta l'`account:ListRegions` azione alla politica per consentire l'accesso alla visualizzazione delle regioni per un account.	22 dicembre 2022
AWSOrganizationsFullAccess— aggiornato per consentire le autorizzazioni API dell'account necessarie per aggiungere o modificare i contatti dell'account tramite la console Organizations.	È stata aggiunta l'`account:PutContactInformation` azione `account:GetContactInformation` and alla policy per consentire l'accesso in scrittura per modificare i contatti di un account.	21 ottobre 2022

Modifica	Descrizione	Data
AWSOrganizationsReadOnlyAccess— aggiornato per consentire le autorizzazioni API dell'account necessarie per visualizzare i contatti dell'account tramite la console Organizations.	È stata aggiunta l'`account:GetContactInformation` azione alla policy per consentire l'accesso alla visualizzazione dei contatti di un account.	21 ottobre 2022
AWSOrganizationsFullAccess— aggiornato per consentire la creazione di un'organizzazione.	È stata aggiunta l'`CreateServiceLinkedRole` autorizzazione alla politica per consentire la creazione del ruolo collegato al servizio necessario 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.	Sono state aggiunte `account:GetAlternateContact` le `account:DeleteAlternateContact` `account:PutAlternateContact` azioni alla policy per consentire l'accesso in scrittura alla modifica di contatti alternativi per un account.	7 febbraio 2022
AWSOrganizationsReadOnlyAccess— aggiornato per consentire le autorizzazioni API dell'account necessarie per visualizzare i contatti alternativi dell'account tramite la console Organizations.	È stata aggiunta l'`account:GetAlternateContact` azione alla politica per consentire l'accesso alla visualizzazione di contatti alternativi per un account.	7 febbraio 2022

AWS politiche di autorizzazione gestite

Le politiche di autorizzazione sono simili alle politiche di autorizzazione IAM, ma sono una funzionalità AWS Organizations piuttosto che IAM. Utilizzi le politiche di autorizzazione per configurare e gestire centralmente l'accesso ai principali e alle risorse nei tuoi account membro.

Puoi consultare l'elenco delle policy della tua organizzazione nella pagina Policies (Policy) della console Organizations.

Nome policy	Descrizione	ARN
CompletaAWSAccess	Consente l'accesso a tutte le operazioni.	arn:aws:organizations: :aws: -Full policy/service_control_policy/p AWSAccess
RCPFullAWSAccess	Consente l'accesso a tutte le risorse.	arn:aws:organizations: :aws: - policy/ resource_control_policy/p RCPFull AWSAccess

Controllo degli accessi basato sugli attributi con tag per AWS Organizations

Il controllo degli accessi basato sugli attributi consente di utilizzare attributi gestiti dall'amministratore, come i tag allegati sia alle AWS risorse che alle AWS identità, per controllare l'accesso a tali 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.

AWS Organizations Le risorse etichettabili includono la radice Account AWS, le unità organizzative () o le politiche dell'organizzazione. OUs Quando si associano tag alle risorse di Organizations, è possibile utilizzarli per controllare chi può accedere a tali risorse. A tale scopo, aggiungi `Condition` elementi alle dichiarazioni sulla politica delle autorizzazioni AWS Identity and Access Management (IAM) che controllano la presenza di determinate chiavi e valori dei tag prima di consentire l'azione. Ciò ti consente di creare una policy IAM che dica efficacemente «Consenti all'utente di gestire solo quelli OUs che hanno un tag con una chiave `X` e un valore`Y`» o «Consenti all'utente di gestire solo quelli a OUs cui è associata una chiave `Z` che ha lo stesso valore della chiave di tag allegata 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 AWS Management Console, the AWS Command Line Interface (AWS CLI) o una delle AWS SDKs, specifichi a quali risorse desideri accedere con quella 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`.

JSON

```
{
    "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 su come utilizzare questo elemento, consulta Controlling access to resource and aws: ResourceTag nella IAM User Guide.

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 interrompere un' EC2 istanza Amazon solo se l'istanza è etichettata con lo stesso `cost-center` valore dell'utente.

JSON

```
{
    "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 politica di esempio consente qualsiasi operazione Organizations solo se tutti i tag presenti nella richiesta sono un sottoinsieme dei tre tag di questa politica.

JSON

```
{
    "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.

JSON

```
{
    "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 politica di esempio nega qualsiasi richiesta da parte dell'utente o del ruolo di creare un tag Account AWS in cui nella richiesta manca il `costcenter` tag o fornisce al tag un valore diverso da 12, o. 3

JSON

```
{
    "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 su come utilizzare questi elementi, consulta aws: TagKeys and aws: RequestTag nella IAM User Guide.

Risoluzione dei problemi di AWS Organizations identità e accesso

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

Argomenti

Non sono autorizzato a eseguire un'azione in Organizations

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `organizations:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 organizations:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `organizations:`*`GetWidget`*.

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

Non sono autorizzato a eseguire iam: PassRole

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

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

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

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

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

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

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse Organizations

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

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Organizations supporta queste funzionalità, vedereCome AWS Organizations funziona con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Registrazione e monitoraggio AWS Organizations

Come best practice, dovresti monitorare la tua organizzazione per accertarti che le modifiche vengano registrate. Questo ti aiuta a garantire che eventuali modifiche impreviste possano essere esaminate e che le modifiche indesiderate possano essere annullate. AWS Organizations attualmente ne supporta due Servizi AWS che consentono di monitorare l'organizzazione e l'attività che si svolge al suo interno.

Argomenti

Registrazione delle chiamate API con for AWS CloudTrailAWS Organizations

AWS Organizations è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, un ruolo o un AWS servizio in AWS Organizations. CloudTrail acquisisce tutte le chiamate API relative AWS Organizations agli eventi, incluse le chiamate dalla AWS Organizations console e le chiamate in codice a. AWS Organizations APIs Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per. AWS Organizations Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare a quale richiesta è stata inviata AWS Organizations, l'indirizzo IP da cui è stata effettuata, chi l'ha effettuata, quando è stata effettuata e dettagli aggiuntivi.

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

> **Important**
>
> È possibile visualizzare tutte le CloudTrail informazioni AWS Organizations solo nella regione Stati Uniti orientali (Virginia settentrionale). Se non vedi la tua AWS Organizations attività nella CloudTrail console, imposta la console su Stati Uniti orientali (Virginia settentrionale) utilizzando il menu nell'angolo in alto a destra. Se esegui una query CloudTrail con gli strumenti AWS CLI o l'SDK, indirizza la query all'endpoint degli Stati Uniti orientali (Virginia settentrionale).

AWS Organizations informazioni in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in AWS Organizations, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti in Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nell' Account AWS che includa gli eventi per AWS Organizations, crea un trail. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Quando CloudTrail la registrazione è abilitata nel tuo Account AWS, le chiamate API effettuate alle AWS Organizations azioni vengono tracciate nei file di CloudTrail registro, dove vengono scritte insieme ad altri record di servizio. AWS Puoi configurarne altri Servizi AWS per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un trail
- CloudTrail Servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail

Tutte AWS Organizations le azioni vengono registrate CloudTrail e documentate nell'API Reference.AWS Organizations Ad esempio, le chiamate a `CreateAccount` (incluso l'`CreateAccountResult`evento) e `InviteAccountToOrganization` generano voci nei file di CloudTrail registro. `ListHandshakesForAccount` `CreatePolicy`

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 AWS servizio

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Comprensione delle AWS Organizations voci dei file di registro

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

Esempi di voci di registro: CloseAccount

L'esempio seguente mostra una voce di CloudTrail registro per una `CloseAccount` chiamata di esempio generata quando viene chiamata l'API e il flusso di lavoro per chiudere l'account inizia 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 CloudTrail registro per una `CloseAccountResult` chiamata dopo il completamento corretto 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"
}
```

Esempi di voci di registro: CreateAccount

L'esempio seguente mostra una voce di CloudTrail registro per una `CreateAccount` chiamata di esempio generata quando viene chiamata l'API e il flusso di lavoro per creare l'account inizia 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 CloudTrail registro per una `CreateAccount` chiamata dopo il completamento corretto 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 CloudTrail registro generata dopo che un flusso di lavoro in `CreateAccount` background non riesce a creare l'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 registro: CreateOrganizationalUnit

L'esempio seguente mostra una voce di CloudTrail registro per una `CreateOrganizationalUnit` chiamata 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 registro: InviteAccountToOrganization

L'esempio seguente mostra una voce di CloudTrail registro per una `InviteAccountToOrganization` chiamata 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 registro: AttachPolicy

L'esempio seguente mostra una voce di CloudTrail registro per una `AttachPolicy` chiamata 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 e AWS Organizations

AWS Organizations può lavorare con Amazon EventBridge, precedentemente Amazon CloudWatch Events, per generare eventi quando si verificano azioni specificate dall'amministratore in un'organizzazione. 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. Puoi configurare EventBridge regole che cercano queste azioni e quindi inviare gli eventi generati a destinazioni definite dall'amministratore. 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 EventBridge abilitare il monitoraggio delle attività chiave nell'organizzazione, consulta. Tutorial: monitora le modifiche importanti alla tua organizzazione con Amazon EventBridge

> **Important**
>
> Attualmente AWS Organizations è ospitato solo nella regione Stati Uniti orientali (Virginia settentrionale) (anche se è disponibile a livello globale). Per eseguire i passaggi di questo tutorial, è necessario configurare l'utilizzo AWS Management Console di quella regione.

Per ulteriori informazioni EventBridge, incluso come configurarlo e abilitarlo, consulta la Amazon EventBridge User Guide.

Convalida della conformità per AWS Organizations

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

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

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

- Governance e conformità per la sicurezza: queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.

- Riferimenti sui servizi conformi ai requisiti HIPAA: elenca i servizi HIPAA idonei. Non tutti Servizi AWS sono idonei alla normativa HIPAA.
- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in AWS Organizations

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

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

Sicurezza dell'infrastruttura in AWS Organizations

In quanto servizio gestito, AWS Organizations è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere a Organizations attraverso la rete. I client devono supportare quanto segue:

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

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

Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Risoluzione dei problemi AWS Organizations

Se si verificano problemi durante l'utilizzo di AWS Organizations, consulta gli argomenti in questa sezione.

Risoluzione dei problemi generali

Utilizza le informazioni qui riportate per eseguire la diagnosi e risolvere problemi di accesso negato o altri problemi comuni che possono verificarsi durante l'utilizzo di. AWS Organizations

Argomenti

Messaggio di accesso rifiutato quando si effettua 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 politiche che concedono tali autorizzazioni includono condizioni,

ad time-of-day esempio restrizioni relative all'indirizzo IP, è necessario soddisfare anche tali requisiti al momento dell'invio della 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 firmi manualmente le richieste API (senza utilizzare il AWS SDKs), verifica di aver firmato la richiesta correttamente.

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 i dettagli, consulta la documentazione del toolkit per l'SDK scelto o Utilizzo delle credenziali di sicurezza temporanee per richiedere l'accesso alle AWS risorse nella Guida per l'utente 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 crei un account in un'organizzazione utilizzando la AWS Organizations console, l'API o AWS CLI i comandi, le informazioni non vengono raccolte automaticamente. Se desideri rendere standalone un account, devi accettare il contratto con il AWS cliente, 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 AWS attività fatturabili (non il piano AWS gratuito) di effettuate durante il periodo in cui l'account non è associato a un'organizzazione. Per ulteriori informazioni, consulta Uscire da un'organizzazione da un account membro con AWS Organizations.

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 azioni richiedono un periodo di attesa a causa delle quote degli account. Ad esempio, non è possibile rimuovere immediatamente gli account appena creati. Prova a ripetere l'operazione dopo qualche giorno.

Per problemi con l'aggiunta di account, consulta la quota Numero massimo predefinito di account. Se si verificano problemi con la rimozione di account, consulta la quota Numero di account membri che è possibile chiudere in un periodo di 30 giorni.

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 Supporto AWS.

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. È necessario del AWS Organizations tempo affinché le modifiche apportate risultino visibili da tutti i possibili endpoint. Alcuni dei ritardi sono dovuti al tempo necessario per inviare i dati da un server a un altro o da una zona di replica a un'altra. AWS Organizations utilizza inoltre la memorizzazione nella cache per migliorare le prestazioni, ma in alcuni casi è possibile che ciò 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 Servizi AWS alcuni altri, 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
- Garantire la consistenza quando si utilizzano Amazon S3 e Amazon Elastic MapReduce for ETL Workflows nel blog dei Big Data. AWS

- EC2 Eventuale coerenza nell'Amazon EC2 API Reference.

Ricevo il messaggio «Registrazione completa» quando cerco di accedere a un account che fa già parte di un'organizzazione

- Potrebbero essere necessarie fino a 48 ore prima che l'account membro erediti i dati di fatturazione dell'account di gestione.
- Se il problema persiste dopo 48 ore, puoi aprire una richiesta di assistenza al team di assistenza per account e fatturazione. Per ulteriori informazioni, consulta Creazione di una richiesta di supporto.

Chiamata dell'API tramite richieste di query HTTP

Questa sezione contiene informazioni generali sull'utilizzo 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 AWS Organizations Query, puoi utilizzare uno dei AWS SDKs. AWS SDKs Sono costituiti da librerie e codice di esempio per vari linguaggi e piattaforme di programmazione (Java, Ruby, .NET, iOS, Android e altri). SDKs Forniscono un modo conveniente per creare un accesso programmatico a AWS Organizations e. AWS Ad esempio, SDKs si occupano di attività come la firma crittografica delle richieste, la gestione degli errori e il ritentativo automatico delle richieste. Per informazioni su AWS SDKs, incluso come scaricarli e installarli, consulta Tools for Amazon Web Services.

L'API Query per AWS Organizations ti consente di richiamare azioni di servizio. Le richieste API di query sono richieste HTTPS che devono contenere un `Action` parametro per indicare l'operazione da eseguire. AWS Organizations supporta le 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
- HTTPS obbligatorio
- Firma AWS Organizations delle richieste API

Endpoints

AWS Organizations dispone di un unico endpoint API globale ospitato nella regione Stati Uniti orientali (Virginia settentrionale).

Per ulteriori informazioni sugli AWS endpoint e sulle regioni per tutti i servizi, consulta 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 AWS Organizations delle richieste API

Le richieste devono essere firmate usando un ID chiave di accesso e una Secret Access Key. Ti consigliamo vivamente di non utilizzare Utente root dell'account AWS le tue credenziali per il lavoro quotidiano con AWS Organizations. È possibile utilizzare le credenziali di un utente o un ruolo.

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

AWS Organizations non supporta versioni precedenti, come Signature Version 2.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- AWS Credenziali di sicurezza: fornisce informazioni generali sui tipi di credenziali che è possibile utilizzare per accedere. AWS
- Best practice di sicurezza in IAM: offre suggerimenti per l'utilizzo del servizio IAM per proteggere le AWS risorse, incluse quelle in. AWS Organizations
- Credenziali di sicurezza temporanee in IAM: descrive come creare e usare credenziali di sicurezza temporanee.

Esempi di codice per Organizations che utilizzano AWS SDKs

I seguenti esempi di codice mostrano come utilizzare Organizations con un kit di sviluppo AWS software (SDK).

Le operazioni sono estratti di codice da programmi più grandi e devono essere eseguite nel contesto. Sebbene le operazioni mostrino come richiamare le singole funzioni del servizio, è possibile visualizzarle contestualizzate negli scenari correlati.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Organizations con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Esempi di codice

- Esempi di base per le Organizzazioni che utilizzano AWS SDKs
  - Azioni per le organizzazioni che utilizzano AWS SDKs
    - Utilizzo AttachPolicy con un AWS SDK o una CLI
    - Utilizzo CreateAccount con un AWS SDK o una CLI
    - Utilizzo CreateOrganization con un AWS SDK o una CLI
    - Utilizzo CreateOrganizationalUnit con un AWS SDK o una CLI
    - Utilizzo CreatePolicy con un AWS SDK o una CLI
    - Utilizzo DeleteOrganization con un AWS SDK o una CLI
    - Utilizzo DeleteOrganizationalUnit con un AWS SDK o una CLI
    - Utilizzo DeletePolicy con un AWS SDK o una CLI
    - Utilizzo DescribePolicy con un AWS SDK o una CLI
    - Utilizzo DetachPolicy con un AWS SDK o una CLI
    - Utilizzo ListAccounts con un AWS SDK o una CLI
    - Utilizzo ListOrganizationalUnitsForParent con un AWS SDK o una CLI
    - Utilizzo ListPolicies con un AWS SDK o una CLI

Esempi di base per le Organizzazioni che utilizzano AWS SDKs

I seguenti esempi di codice mostrano come utilizzare le nozioni di base di AWS Organizations with. AWS SDKs

Esempi

- Azioni per le organizzazioni che utilizzano AWS SDKs
  - Utilizzo AttachPolicy con un AWS SDK o una CLI
  - Utilizzo CreateAccount con un AWS SDK o una CLI
  - Utilizzo CreateOrganization con un AWS SDK o una CLI
  - Utilizzo CreateOrganizationalUnit con un AWS SDK o una CLI
  - Utilizzo CreatePolicy con un AWS SDK o una CLI
  - Utilizzo DeleteOrganization con un AWS SDK o una CLI
  - Utilizzo DeleteOrganizationalUnit con un AWS SDK o una CLI
  - Utilizzo DeletePolicy con un AWS SDK o una CLI
  - Utilizzo DescribePolicy con un AWS SDK o una CLI
  - Utilizzo DetachPolicy con un AWS SDK o una CLI
  - Utilizzo ListAccounts con un AWS SDK o una CLI
  - Utilizzo ListOrganizationalUnitsForParent con un AWS SDK o una CLI
  - Utilizzo ListPolicies con un AWS SDK o una CLI

Azioni per le organizzazioni che utilizzano AWS SDKs

I seguenti esempi di codice mostrano come eseguire azioni individuali di Organizations con AWS SDKs. Ogni esempio include un collegamento a GitHub, dove sono disponibili le istruzioni per la configurazione e l'esecuzione del codice.

Gli esempi seguenti includono solo le operazioni più comunemente utilizzate. Per un elenco completo, consulta la Documentazione di riferimento API di AWS Organizations.

Esempi

- Utilizzo AttachPolicy con un AWS SDK o una CLI
- Utilizzo CreateAccount con un AWS SDK o una CLI
- Utilizzo CreateOrganization con un AWS SDK o una CLI

- Utilizzo CreateOrganizationalUnit con un AWS SDK o una CLI
- Utilizzo CreatePolicy con un AWS SDK o una CLI
- Utilizzo DeleteOrganization con un AWS SDK o una CLI
- Utilizzo DeleteOrganizationalUnit con un AWS SDK o una CLI
- Utilizzo DeletePolicy con un AWS SDK o una CLI
- Utilizzo DescribePolicy con un AWS SDK o una CLI
- Utilizzo DetachPolicy con un AWS SDK o una CLI
- Utilizzo ListAccounts con un AWS SDK o una CLI
- Utilizzo ListOrganizationalUnitsForParent con un AWS SDK o una CLI
- Utilizzo ListPolicies con un AWS SDK o una CLI

Utilizzo **`AttachPolicy`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `AttachPolicy`.

.NET

SDK per .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to attach an AWS Organizations policy to an organization,
/// an organizational unit, or an account.
/// </summary>
public class AttachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then calls the
```

```
        /// AttachPolicyAsync method to attach the policy to the root
        /// organization.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var policyId = "p-00000000";
            var targetId = "r-0000";

            var request = new AttachPolicyRequest
            {
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.AttachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully attached Policy ID {policyId} to
Target ID: {targetId}.");
            }
            else
            {
                Console.WriteLine("Was not successful in attaching the policy.");
            }
        }
    }
```

- Per i dettagli sull'API, AttachPolicyconsulta AWS SDK per .NET API Reference.

CLI

AWS CLI

Per allegare una policy a una root, a un'unità organizzativa o a un account

Esempio 1

L'esempio seguente mostra come collegare una policy di controllo del servizio (SCP) a un'unità organizzativa:

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id ou-examplerootid111-exampleouid111
```

Esempio 2

L'esempio seguente mostra come allegare una politica di controllo del servizio direttamente a un account:

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id 333333333333
```

- Per i dettagli sull'API, consulta AttachPolicy AWS CLICommand Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
def attach_policy(policy_id, target_id, orgs_client):
    """
    Attaches a policy to a target. The target is an organization root, account,
 or
    organizational unit.

    :param policy_id: The ID of the policy to attach.
    :param target_id: The ID of the resources to attach the policy to.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.attach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Attached policy %s to target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
```

```
            "Couldn't attach policy %s to target %s.", policy_id, target_id
        )
        raise
```

- Per i dettagli sull'API, consulta AttachPolicy AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Organizations con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`CreateAccount`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `CreateAccount`.

.NET

SDK per .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new AWS Organizations account.
/// </summary>
public class CreateAccount
{
    /// <summary>
    /// Initializes an Organizations client object and uses it to create
    /// the new account with the name specified in accountName.
    /// </summary>
```

```
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var accountName = "ExampleAccount";
            var email = "someone@example.com";

            var request = new CreateAccountRequest
            {
                AccountName = accountName,
                Email = email,
            };

            var response = await client.CreateAccountAsync(request);
            var status = response.CreateAccountStatus;

            Console.WriteLine($"The staus of {status.AccountName} is
{status.State}.");
        }
    }
```

- Per i dettagli sull'API, CreateAccountconsulta AWS SDK per .NET API Reference.

CLI

AWS CLI

Per creare un account membro che faccia automaticamente parte dell'organizzazione

L'esempio seguente mostra come creare un account membro in un'organizzazione. L'account membro è configurato con il nome Account di produzione e l'indirizzo e-mail susan@example.com. Organizations crea automaticamente un ruolo IAM utilizzando il nome predefinito di OrganizationAccountAccessRole perché il parametro RoleName non è specificato. Inoltre, l'impostazione che consente agli utenti o ai ruoli IAM con autorizzazioni sufficienti di accedere ai dati di fatturazione dell'account è impostata sul valore predefinito di ALLOW perché il IamUserAccessToBilling parametro non è specificato. Organizations invia automaticamente a Susan un'e-mail di «Benvenuto a AWS»:

```
aws organizations create-account --email susan@example.com --account-
name "Production Account"
```

L'output include un oggetto di richiesta che mostra che lo stato è ora`IN_PROGRESS`:

```
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

Successivamente è possibile interrogare lo stato corrente della richiesta fornendo il valore di risposta Id al describe-create-account-status comando come valore per il create-account-request-id parametro.

Per ulteriori informazioni, consulta Creare un AWS account nella tua organizzazione nella AWS Organizations Users Guide.

- Per i dettagli sull'API, consulta CreateAccount AWS CLICommand Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo AWS Organizations con un SDK AWS. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`CreateOrganization`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `CreateOrganization`.

.NET

SDK per .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;
```

```
    /// <summary>
    /// Creates an organization in AWS Organizations.
    /// </summary>
    public class CreateOrganization
    {
        /// <summary>
        /// Creates an Organizations client object and then uses it to create
        /// a new organization with the default user as the administrator, and
        /// then displays information about the new organization.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var response = await client.CreateOrganizationAsync(new
CreateOrganizationRequest
            {
                FeatureSet = "ALL",
            });

            Organization newOrg = response.Organization;

            Console.WriteLine($"Organization: {newOrg.Id} Main Accoount:
{newOrg.MasterAccountId}");
        }
    }
```

- Per i dettagli sull'API, CreateOrganizationconsulta AWS SDK per .NET API Reference.

CLI

AWS CLI

Esempio 1: creare una nuova organizzazione

Bill desidera creare un'organizzazione utilizzando le credenziali dell'account 1111. L'esempio seguente mostra che l'account diventa l'account principale nella nuova organizzazione. Poiché non specifica un set di funzionalità, per impostazione predefinita la nuova organizzazione prevede che tutte le funzionalità siano abilitate e le politiche di controllo del servizio sono abilitate nella directory principale.

```
aws organizations create-organization
```

L'output include un oggetto dell'organizzazione con dettagli sulla nuova organizzazione:

```
{
        "Organization": {
                "AvailablePolicyTypes": [
                        {
                                "Status": "ENABLED",
                                "Type": "SERVICE_CONTROL_POLICY"
                        }
                ],
                "MasterAccountId": "111111111111",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "FeatureSet": "ALL",
                "Id": "o-exampleorgid",
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid"
        }
}
```

Esempio 2: creare una nuova organizzazione con solo le funzionalità di fatturazione consolidate abilitate

L'esempio seguente crea un'organizzazione che supporta solo le funzionalità di fatturazione consolidata:

```
aws organizations create-organization --feature-set CONSOLIDATED_BILLING
```

L'output include un oggetto dell'organizzazione con dettagli sulla nuova organizzazione:

```
{
        "Organization": {
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
                "AvailablePolicyTypes": [],
                "Id": "o-exampleorgid",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
```

```
                "MasterAccountId": "111111111111",
                "FeatureSet": "CONSOLIDATED_BILLING"
        }
}
```

Per ulteriori informazioni, vedere Creating an Organization nella AWS Organizations Users Guide.

- Per i dettagli sull'API, consulta CreateOrganization AWS CLICommand Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo AWS Organizations con un SDK AWS. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`CreateOrganizationalUnit`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `CreateOrganizationalUnit`.

.NET

SDK per .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new organizational unit in AWS Organizations.
/// </summary>
public class CreateOrganizationalUnit
{
    /// <summary>
    /// Initializes an Organizations client object and then uses it to call
    /// the CreateOrganizationalUnit method. If the call succeeds, it
```

```
        /// displays information about the new organizational unit.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var orgUnitName = "ProductDevelopmentUnit";

            var request = new CreateOrganizationalUnitRequest
            {
                Name = orgUnitName,
                ParentId = "r-0000",
            };

            var response = await client.CreateOrganizationalUnitAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully created organizational unit:
{orgUnitName}.");
                Console.WriteLine($"Organizational unit {orgUnitName} Details");
                Console.WriteLine($"ARN: {response.OrganizationalUnit.Arn} Id:
{response.OrganizationalUnit.Id}");
            }
            else
            {
                Console.WriteLine("Could not create new organizational unit.");
            }
        }
    }
```

- Per i dettagli sull'API, CreateOrganizationalUnitconsulta AWS SDK per .NET API Reference.

CLI

AWS CLI

Per creare un'unità organizzativa in un'unità organizzativa principale o principale

L'esempio seguente mostra come creare un'unità organizzativa denominata AccountingOU:

```
aws organizations create-organizational-unit --parent-id r-examplerootid111 --
name AccountingOU
```

L'output include un oggetto OrganizationalUnit con dettagli sulla nuova unità organizzativa:

```
{
        "OrganizationalUnit": {
                "Id": "ou-examplerootid111-exampleouid111",
                "Arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-
examplerootid111-exampleouid111",
                "Name": "AccountingOU"
        }
}
```

- Per i dettagli sull'API, vedere CreateOrganizationalUnitin AWS CLI Command Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo AWS Organizations con un SDK AWS. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`CreatePolicy`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `CreatePolicy`.

.NET

SDK per .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    using System;
    using System.Threading.Tasks;
    using Amazon.Organizations;
    using Amazon.Organizations.Model;

    /// <summary>
```

```
    /// Creates a new AWS Organizations Policy.
    /// </summary>
    public class CreatePolicy
    {
        /// <summary>
        /// Initializes the AWS Organizations client object, uses it to
        /// create a new Organizations Policy, and then displays information
        /// about the newly created Policy.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var policyContent = "{" +
                "   \"Version\": \"2012-10-17\"," +
                " \"Statement\" : [{" +
                    " \"Action\" : [\"s3:*\"]," +
                    " \"Effect\" : \"Allow\"," +
                    " \"Resource\" : \"*\"" +
                "}]" +
            "}";

            try
            {
                var response = await client.CreatePolicyAsync(new
CreatePolicyRequest
                {
                    Content = policyContent,
                    Description = "Enables admins of attached accounts to
delegate all Amazon S3 permissions",
                    Name = "AllowAllS3Actions",
                    Type = "SERVICE_CONTROL_POLICY",
                });

                Policy policy = response.Policy;
                Console.WriteLine($"{policy.PolicySummary.Name} has the following
content: {policy.Content}");
            }
            catch (Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
        }
    }
```

- Per i dettagli sull'API, CreatePolicyconsulta AWS SDK per .NET API Reference.

CLI

AWS CLI

Esempio 1: creare una policy con un file sorgente di testo per la policy JSON

L'esempio seguente mostra come creare una policy di controllo del servizio (SCP) denominata. `AllowAllS3Actions` Il contenuto della policy è tratto da un file sul computer locale chiamato`policy.json`.

```
aws organizations create-policy --content file://policy.json --
name AllowAllS3Actions, --type SERVICE_CONTROL_POLICY --description "Allows
 delegation of all S3 actions"
```

L'output include un oggetto di policy con dettagli sulla nuova policy:

```
{
        "Policy": {
                "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Action\":[\"s3:*\"],\"Resource\":[\"*\"]}]}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::o-exampleorgid:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Allows delegation of all S3 actions",
                        "Name": "AllowAllS3Actions",
                        "Type":"SERVICE_CONTROL_POLICY"
                }
        }
}
```

Esempio 2: creare una policy con una policy JSON come parametro

L'esempio seguente mostra come creare lo stesso SCP, questa volta incorporando il contenuto della policy come stringa JSON nel parametro. La stringa deve essere cancellata con barre rovesciate prima delle virgolette doppie per garantire che vengano trattate come valori letterali nel parametro, che a sua volta è circondato da virgolette doppie:

```
aws organizations create-policy --content "{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"s3:*\"],\"Resource
\":[\"*\"]}]}" --name AllowAllS3Actions --type SERVICE_CONTROL_POLICY --
description "Allows delegation of all S3 actions"
```

Per ulteriori informazioni sulla creazione e l'utilizzo delle politiche nell'organizzazione, vedere Managing Organization Policies nella AWS Organizations User Guide.

- Per i dettagli sull'API, consulta CreatePolicy AWS CLICommand Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
def create_policy(name, description, content, policy_type, orgs_client):
    """
    Creates a policy.

    :param name: The name of the policy.
    :param description: The description of the policy.
    :param content: The policy content as a dict. This is converted to JSON
 before
                    it is sent to AWS. The specific format depends on the policy
 type.
    :param policy_type: The type of the policy.
    :param orgs_client: The Boto3 Organizations client.
    :return: The newly created policy.
    """
    try:
        response = orgs_client.create_policy(
            Name=name,
            Description=description,
            Content=json.dumps(content),
            Type=policy_type,
        )
```

```
        policy = response["Policy"]
        logger.info("Created policy %s.", name)
    except ClientError:
        logger.exception("Couldn't create policy %s.", name)
        raise
    else:
        return policy
```

- Per i dettagli sull'API, consulta CreatePolicy AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Organizations con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DeleteOrganization`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `DeleteOrganization`.

.NET

SDK per .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing organization using the AWS
/// Organizations Service.
/// </summary>
public class DeleteOrganization
```

```
    {
        /// <summary>
        /// Initializes the Organizations client and then calls
        /// DeleteOrganizationAsync to delete the organization.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var response = await client.DeleteOrganizationAsync(new
DeleteOrganizationRequest());

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine("Successfully deleted organization.");
            }
            else
            {
                Console.WriteLine("Could not delete organization.");
            }
        }
    }
```

- Per i dettagli sull'API, DeleteOrganizationconsulta AWS SDK per .NET API Reference.

CLI

AWS CLI

Per eliminare un'organizzazione

L'esempio seguente mostra come eliminare un'organizzazione. Per eseguire questa operazione, devi essere un amministratore dell'account principale dell'organizzazione. L'esempio presuppone che in precedenza siano stati rimossi tutti gli account dei membri e le politiche dall'organizzazione: OUs

```
aws organizations delete-organization
```

- Per i dettagli sull'API, consulta DeleteOrganization AWS CLICommand Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo AWS Organizations con un SDK AWS. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DeleteOrganizationalUnit`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `DeleteOrganizationalUnit`.

.NET

SDK per .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing AWS Organizations organizational unit.
/// </summary>
public class DeleteOrganizationalUnit
{
    /// <summary>
    /// Initializes the Organizations client object and calls
    /// DeleteOrganizationalUnitAsync to delete the organizational unit
    /// with the selected ID.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitId = "ou-0000-00000000";

        var request = new DeleteOrganizationalUnitRequest
        {
```

```
                OrganizationalUnitId = orgUnitId,
            };

            var response = await client.DeleteOrganizationalUnitAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted the organizational unit
with ID: {orgUnitId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete the organizational unit with
ID: {orgUnitId}.");
            }
        }
    }
```

- Per i dettagli sull'API, DeleteOrganizationalUnitconsulta AWS SDK per .NET API Reference.

CLI

AWS CLI

Per eliminare un'unità organizzativa

L'esempio seguente mostra come eliminare un'UO. L'esempio presuppone che in precedenza siano stati rimossi tutti gli account e altri account OUs dall'unità organizzativa:

```
aws organizations delete-organizational-unit --organizational-unit-id ou-
examplerootid111-exampleouid111
```

- Per i dettagli sull'API, vedere DeleteOrganizationalUnitin AWS CLI Command Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo AWS Organizations con un SDK AWS. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DeletePolicy`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `DeletePolicy`.

.NET

SDK per .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Deletes an existing AWS Organizations policy.
/// </summary>
public class DeletePolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// delete the policy with the specified policyId.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-00000000";

        var request = new DeletePolicyRequest
        {
            PolicyId = policyId,
        };

        var response = await client.DeletePolicyAsync(request);
```

```
            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted Policy: {policyId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete Policy: {policyId}.");
            }
        }
    }
```

- Per i dettagli sull'API, consulta la DeletePolicysezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Per eliminare una politica

L'esempio seguente mostra come eliminare una politica da un'organizzazione. L'esempio presuppone che in precedenza sia stata scollegata la politica da tutte le entità:

```
aws organizations delete-policy --policy-id p-examplepolicyid111
```

- Per i dettagli sull'API, consulta AWS CLI Command DeletePolicyReference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
def delete_policy(policy_id, orgs_client):
    """
```

```
    Deletes a policy.

    :param policy_id: The ID of the policy to delete.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.delete_policy(PolicyId=policy_id)
        logger.info("Deleted policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't delete policy %s.", policy_id)
        raise
```

- Per i dettagli sull'API, consulta DeletePolicy AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Organizations con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DescribePolicy`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `DescribePolicy`.

CLI

AWS CLI

Per ottenere informazioni su una politica

L'esempio seguente mostra come richiedere informazioni su una politica:

```
aws organizations describe-policy --policy-id p-examplepolicyid111
```

L'output include un oggetto politico che contiene dettagli sulla politica:

```
{
        "Policy": {
                "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement
\": [\n    {\n      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n
 \"Resource\": \"*\"\n    }\n  ]\n}",
```

```
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::111111111111:policy/o-
exampleorgid/service_control_policy/p-examplepolicyid111",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-examplepolicyid111",
                        "AwsManaged": false,
                        "Name": "AllowAllS3Actions",
                        "Description": "Enables admins to delegate S3
 permissions"
                }
        }
}
```

- Per i dettagli sull'API, vedere DescribePolicyin AWS CLI Command Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
def describe_policy(policy_id, orgs_client):
    """
    Describes a policy.

    :param policy_id: The ID of the policy to describe.
    :param orgs_client: The Boto3 Organizations client.
    :return: The description of the policy.
    """
    try:
        response = orgs_client.describe_policy(PolicyId=policy_id)
        policy = response["Policy"]
        logger.info("Got policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't get policy %s.", policy_id)
        raise
    else:
        return policy
```

- Per i dettagli sull'API, consulta DescribePolicy AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Organizations con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DetachPolicy`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `DetachPolicy`.

.NET

SDK per .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to detach a policy from an AWS Organizations organization,
/// organizational unit, or account.
/// </summary>
public class DetachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and uses it to call
    /// DetachPolicyAsync to detach the policy.
    /// </summary>
    public static async Task Main()
    {
```

```
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var policyId = "p-00000000";
            var targetId = "r-0000";

            var request = new DetachPolicyRequest
            {
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.DetachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully detached policy with Policy Id:
{policyId}.");
            }
            else
            {
                Console.WriteLine("Could not detach the policy.");
            }
        }
    }
```

- Per i dettagli sull'API, consulta la DetachPolicysezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Per scollegare una policy da una root, un'unità organizzativa o un account

L'esempio seguente mostra come scollegare una policy da un'unità organizzativa:

```
aws organizations  detach-policy  --target-id ou-examplerootid111-exampleouid111
 --policy-id p-examplepolicyid111
```

- Per i dettagli sull'API, vedere DetachPolicyin AWS CLI Command Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
def detach_policy(policy_id, target_id, orgs_client):
    """
    Detaches a policy from a target.

    :param policy_id: The ID of the policy to detach.
    :param target_id: The ID of the resource where the policy is currently
 attached.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.detach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Detached policy %s from target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't detach policy %s from target %s.", policy_id, target_id
        )
        raise
```

- Per i dettagli sull'API, consulta DetachPolicy AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Organizations con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`ListAccounts`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `ListAccounts`.

.NET

SDK per .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Uses the AWS Organizations service to list the accounts associated
/// with the default account.
/// </summary>
public class ListAccounts
{
    /// <summary>
    /// Creates the Organizations client and then calls its
    /// ListAccountsAsync method.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var request = new ListAccountsRequest
        {
            MaxResults = 5,
        };

        var response = new ListAccountsResponse();
        try
        {
            do
            {
                response = await client.ListAccountsAsync(request);
                response.Accounts.ForEach(a => DisplayAccounts(a));
```

```
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (AWSOrganizationsNotInUseException ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about an Organizations account.
        /// </summary>
        /// <param name="account">An Organizations account for which to display
        /// information on the console.</param>
        private static void DisplayAccounts(Account account)
        {
            string accountInfo = $"{account.Id}
{account.Name}\t{account.Status}";

            Console.WriteLine(accountInfo);
        }
    }
```

- Per i dettagli sull'API, consulta la ListAccountssezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Per recuperare un elenco di tutti gli account di un'organizzazione

L'esempio seguente mostra come richiedere un elenco degli account di un'organizzazione:

```
aws organizations list-accounts
```

L'output include un elenco di oggetti di riepilogo degli account.

```
{
        "Accounts": [
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/111111111111",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481830215.45,
                        "Id": "111111111111",
                        "Name": "Master Account",
                        "Email": "bill@example.com",
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/222222222222",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835741.044,
                        "Id": "222222222222",
                        "Name": "Production Account",
                        "Email": "alice@example.com",
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/333333333333",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835795.536,
                        "Id": "333333333333",
                        "Name": "Development Account",
                        "Email": "juan@example.com",
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/444444444444",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835812.143,
                        "Id": "444444444444",
                        "Name": "Test Account",
                        "Email": "anika@example.com",
                        "Status": "ACTIVE"
                }
        ]
```

```
}
```

- Per i dettagli sull'API, consulta ListAccounts AWS CLICommand Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo AWS Organizations con un SDK AWS. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`ListOrganizationalUnitsForParent`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `ListOrganizationalUnitsForParent`.

.NET

SDK per .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Lists the AWS Organizations organizational units that belong to an
/// organization.
/// </summary>
public class ListOrganizationalUnitsForParent
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// call the ListOrganizationalUnitsForParentAsync method to retrieve
    /// the list of organizational units.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
```

```
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var parentId = "r-0000";

            var request = new ListOrganizationalUnitsForParentRequest
            {
                ParentId = parentId,
                MaxResults = 5,
            };

            var response = new ListOrganizationalUnitsForParentResponse();
            try
            {
                do
                {
                    response = await
client.ListOrganizationalUnitsForParentAsync(request);
                    response.OrganizationalUnits.ForEach(u =>
DisplayOrganizationalUnit(u));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about an Organizations organizational unit.
        /// </summary>
        /// <param name="unit">The OrganizationalUnit for which to display
        /// information.</param>
        public static void DisplayOrganizationalUnit(OrganizationalUnit unit)
        {
            string accountInfo = $"{unit.Id} {unit.Name}\t{unit.Arn}";

            Console.WriteLine(accountInfo);
        }
    }
```

- Per i dettagli sull'API, consulta la ListOrganizationalUnitsForParentsezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Per recuperare un elenco di file OUs in un'unità organizzativa o root principale

L'esempio seguente mostra come ottenere un elenco di OUs in una radice specificata:

```
aws organizations list-organizational-units-for-parent --parent-id r-
examplerootid111
```

L'output mostra che la radice specificata ne contiene due OUs e mostra i dettagli di ciascuna:

```
{
        "OrganizationalUnits": [
                {
                        "Name": "AccountingDepartment",
                        "Arn": "arn:aws:organizations::o-exampleorgid:ou/r-
examplerootid111/ou-examplerootid111-exampleouid111"
                },
                {
                        "Name": "ProductionDepartment",
                        "Arn": "arn:aws:organizations::o-exampleorgid:ou/r-
examplerootid111/ou-examplerootid111-exampleouid222"
                }
        ]
}
```

- Per i dettagli sull'API, vedere ListOrganizationalUnitsForParentin AWS CLI Command Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo AWS Organizations con un SDK AWS. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`ListPolicies`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `ListPolicies`.

.NET

SDK per .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to list the AWS Organizations policies associated with an
/// organization.
/// </summary>
public class ListPolicies
{
    /// <summary>
    /// Initializes an Organizations client object, and then calls its
    /// ListPoliciesAsync method.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        // The value for the Filter parameter is required and must must be
        // one of the following:
        //     AISERVICES_OPT_OUT_POLICY
        //     BACKUP_POLICY
        //     SERVICE_CONTROL_POLICY
        //     TAG_POLICY
        var request = new ListPoliciesRequest
        {
```

```
                Filter = "SERVICE_CONTROL_POLICY",
                MaxResults = 5,
            };

            var response = new ListPoliciesResponse();
            try
            {
                do
                {
                    response = await client.ListPoliciesAsync(request);
                    response.Policies.ForEach(p => DisplayPolicies(p));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (AWSOrganizationsNotInUseException ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about the Organizations policies associated
        /// with an organization.
        /// </summary>
        /// <param name="policy">An Organizations policy summary to display
        /// information on the console.</param>
        private static void DisplayPolicies(PolicySummary policy)
        {
            string policyInfo = $"{policy.Id}
{policy.Name}\t{policy.Description}";

            Console.WriteLine(policyInfo);
        }
    }
```

- Per i dettagli sull'API, consulta la ListPoliciessezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Per recuperare un elenco di tutte le politiche in un'organizzazione di un determinato tipo

L'esempio seguente mostra come ottenere un elenco di SCPs, come specificato dal parametro filter:

```
aws organizations list-policies --filter SERVICE_CONTROL_POLICY
```

L'output include un elenco di politiche con informazioni di riepilogo:

```
{
        "Policies": [
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllS3Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid111",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Enables account admins to delegate
 permissions for any S3 actions to users and roles in their accounts."
                },
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllEC2Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid222",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid222",
                        "Description": "Enables account admins to delegate
 permissions for any EC2 actions to users and roles in their accounts."
                },
                {
                        "AwsManaged": true,
                        "Description": "Allows access to every operation",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-FullAWSAccess",
                        "Arn": "arn:aws:organizations::aws:policy/
service_control_policy/p-FullAWSAccess",
                        "Name": "FullAWSAccess"
```

```
                }
        ]
}
```

- Per i dettagli sull'API, vedere ListPoliciesin AWS CLI Command Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
def list_policies(policy_filter, orgs_client):
    """
    Lists the policies for the account, limited to the specified filter.

    :param policy_filter: The kind of policies to return.
    :param orgs_client: The Boto3 Organizations client.
    :return: The list of policies found.
    """
    try:
        response = orgs_client.list_policies(Filter=policy_filter)
        policies = response["Policies"]
        logger.info("Found %s %s policies.", len(policies), policy_filter)
    except ClientError:
        logger.exception("Couldn't get %s policies.", policy_filter)
        raise
    else:
        return policies
```

- Per i dettagli sull'API, consulta ListPolicies AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Organizations con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Cronologia dei documenti per AWS Organizations

La tabella seguente descrive i principali aggiornamenti della documentazione per AWS Organizations.

- Versione API: 28-11-2016
- Ultimo aggiornamento della documentazione: 17 giugno 2025

Modifica	Descrizione	Data
Politiche di Security Hub aggiunte	Puoi utilizzare le policy di Security Hub per gestire centralmente le configura zioni di Security Hub in tutto il tuo AWS Organizations. Queste politiche consenton o di abilitare le funzional ità e mantenere controlli di sicurezza coerenti su più account dell'organizzazione.	17 giugno 2025
Aggiornata la politica AWSOrganizations FullAccess gestita	È stata aggiunta l'`account:G etAccountInformati on` azione per abilitare l'accesso alla visualizzazione del nome account di qualsiasi account in un'organizzazione e l'`account:PutAccount Name` azione per abilitare l'accesso per modificare qualsiasi nome di account in un'organizzazione.	22 aprile 2025
Integrazione delle organizza zioni con Notifiche all'utente AWS	Puoi eseguire l'integrazione Notifiche all'utente con AWS Organizations per configura	24 gennaio 2025

	re e visualizzare le notifiche centralmente tra gli account della tua organizzazione.	
Integrazione delle organizzazioni con AWS Managed Services (AMS) Self-Service Reporting (SSR)	È possibile integrare AMS SSR con AWS Organizations per abilitare il reporting self-service aggregato (SSR). Si tratta di una funzionalità AMS che consente ai clienti di Advanced e Accelerate di visualizzare i report self-service esistenti aggregati a livello di organizzazione, su più account.	21 gennaio 2025
Politiche dichiarative aggiunte	È possibile utilizzare le politiche dichiarative per dichiarare e applicare centralmente le configurazioni desiderate per un determinato ambiente su larga scala Servizio AWS all'interno dell'organizzazione. Una volta collegata, la configurazione viene sempre mantenuta quando il servizio aggiunge nuove funzionalità o. APIs	1 dicembre 2024
Nuova politica AWS gestita	È stata aggiunta la `DeclarativePoliciesEC2Report` politica per abilitare la funzionalità del ruolo collegato al servizio declarative-policies-ec2.amazonaws.com.	22 novembre 2024

Politiche di Backup aggiornate	AWS Backup le `selections` policy hanno aggiornato la chiave di policy per includere una chiave di `conditions` policy e hanno aggiunto una nuova chiave di `resources` policy allo schema. Con il nuovo schema, hai una maggiore flessibilità nella selezione delle risorse per le tue politiche di backup.	14 novembre 2024
Gestire centralmente l'accesso root per gli account membri	Ora puoi gestire le credenziali degli utenti root con privilegi tra gli account membri in AWS Organizations con l'accesso root centralizzato. Proteggi centralmente le credenziali utente root del tuo utilizzo Account AWS gestito AWS Organizations per rimuovere e impedire il ripristino e l'accesso alle credenziali degli utenti root su larga scala.	14 novembre 2024
Sono state aggiunte politiche di controllo delle risorse () RCPs	È possibile utilizzare le politiche di controllo delle risorse (RCPs) per controllare le autorizzazioni massime disponibili per le risorse in un'organizzazione.	13 novembre 2024

Aggiunte politiche per le applicazioni di chat	Puoi utilizzare le politiche delle applicazioni di chat per controllare l'accesso agli account della tua organizza zione da applicazioni di chat come Slack e Microsoft Teams.	26 settembre 2024
Aggiornamenti dei contenuti basati su scenari	La AWS Organizations documentazione è stata aggiornata per essere più basata sugli scenari in tutta la guida e il contenuto è stato riorganizzato per migliorar e la leggibilità e la scoperta. Se hai commenti su queste modifiche, usa il pulsante Fornisci feedback nella parte inferiore di una pagina.	4 settembre 2024
Nuova opzione di esclusione da tutti i servizi di intelligenza artificiale	È stata aggiunta documenta zione su come disattivare tutti i servizi di AWS intelligenza artificiale supportati.	16 agosto 2024
Organizations ora supporta 10.000 account in un'organi zzazione	Ora puoi gestire fino a 10.000 account membri in un'organi zzazione, raddoppiando il limite precedente di 5.000 account. Se hai un requisito valido e un'esigenza aziendale , puoi richiedere e ottenere l'approvazione per una quota di 10.000 account senza controlli sui limiti di servizio da Organizations o altri sistemi integrati Servizi AWS.	14 agosto 2024

Nuovo argomento sulla migrazione degli account	È stata aggiunta la documentazione su come migrare un account da un'organizzazione all'altra.	1° agosto 2024
Politiche di Backup aggiornate	AWS Backup le politiche ora supportano gli archivi di snapshot di Amazon Elastic Block Store (Amazon EBS). Per esempi aggiornati, vedere Aggiornamento di una policy di backup e Sintassi ed esempi della policy di Backup.	9 luglio 2024
È stata aggiornata la politica AWSOrganizations ReadOnlyAccess gestita	È stata aggiunta l'`account:GetPrimaryEmail` azione alla AWSOrganizations ReadOnlyAccess politica che consente l'accesso alla visualizzazione dell'indirizzo e-mail dell'utente root per qualsiasi account membro di un'organizzazione e ha aggiunto l'`account:GetRegion0ptStatus` azione per consentire l'accesso alla visualizzazione delle regioni abilitate per qualsiasi account membro di un'organizzazione.	6 giugno 2024
Nuovo aggiornamento dell'indirizzo e-mail dell'utente root, argomento dell'indirizzo	Organizations ora offre la possibilità di aggiornare centralmente l'indirizzo e-mail dell'utente root (indirizzo) per qualsiasi account membro di un'organizzazione.	6 giugno 2024

Dichiarazioni politiche aggiornate	Aggiunti nuovi `Sid` elementi alle dichiarazioni politiche AWS Organizations gestite.	6 febbraio 2024
Nuovo argomento relativo all'account di gestione chiuso	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 AWSOrganizations FullAccess e AWSOrganizations ReadOnlyAccess 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 AWSOrganizations FullAccess 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 servizi necessario a una nuova organizzazione.	24 agosto 2022

Organizations chiude la funzionalità dell'account dalla AWS Organizations console	I principali nell'account di gestione possono chiudere gli account membri dalla console AWS Organizations e proteggere gli account membri dalla chiusura accidentale utilizzando le policy IAM.	29 marzo 2022
Annuncio aggiornato per aggiornare i contatti alternativi con la console AWS Organizations	Organizations ora offre la possibilità di aggiornare i contatti alternativi per gli account all'interno dell'organizzazione utilizzando la AWS Organizations console. 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	Le politiche AWSOrganizations ReadOnlyAccess sono AWSOrganizations FullAccess state aggiornate e gestite per consentire le autorizzazioni API dell'account necessarie per aggiornare o visualizzare i contatti alternativi dell'account tramite la console. AWS Organizations	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	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.	16 dicembre 2021
L'integrazione di Organizations con AWS Config ora supporta l'aggregazione di dati multi-account e più 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	È possibile utilizzare la funzionalità di backup AWS Backup continuo con le politiche 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 per abilitare tutte le funzionalità di 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

Presenta la versione 2.0 della console AWS Organizations	AWS ha introdotto una nuova versione della AWS console. 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 Marketplace AWS condividere più facilmente le tue licenze software tra tutti gli account della tua organizza zione.	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 informazi oni 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 le policy di backup per il backup delle risorse dell'organizzazione, è ora possibile archiviare copie del backup Account AWS in altri membri dell'organizzazion e.	18 novembre 2020
Regioni AWS in Cina ora supporta AWS Resource Access Manager come servizio affidabile di Organizat ions	Ora puoi utilizzare AWS RAM le funzionalità che si integrano con Organizations come servizio affidabile quando usi Organizations 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 dell' «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 per AWS 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 di Organizations ora supportano backup coerenti con le applicazioni su EC2 istanze 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 affidabile	Puoi aggregare AWS Health gli eventi tra gli account della tua organizzazione.	4 agosto 2020

Policy di rifiuto dei servizi di Intelligenza Artificiale (IA)	Puoi utilizzare le politiche di esclusione dei servizi di intelligenza artificiale per controllare se i servizi di AWS intelligenza artificiale possono archiviare e utilizzare i contenuti dei clienti elaborati da tali servizi (contenuti di intelligenza artificiale) per lo sviluppo e il miglioramento continuo di servizi e tecnologie di AWS intelligenza artificiale.	8 luglio 2020
Aggiunte politiche 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 standardizzazione dei tag tra le risorse degli account dell'organizzazione.	26 novembre 2019
Integrazione con Systems Manager	È possibile sincronizzare i dati operativi in tutta l'organizzazione Account AWS in Systems Manager Explorer.	26 novembre 2019
leggi: PrincipalOrgPaths	La nuova chiave di condizione globale controlla il AWS Organizations percorso dell'utente IAM, del ruolo IAM o dell'utente Account AWS root che effettua la richiesta.	20 novembre 2019
Integrazione con AWS Config le regole	Puoi utilizzare le operazioni AWS Config API per gestire AWS Config le regole Account AWS in tutta l'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 in grado di funzionare con gli account dell'organizzazione.	24 giugno 2019

Integrazione con AWS Identity and Access Management	IAM fornisce i dati dell'ultimo accesso al servizio per le entità dell'organizzazione (la radice dell'organizzazione e gli account). OUs Puoi utilizzare questi dati per limitare l'accesso solo ai dati di Servizi AWS 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'`NotAction` elemento delle politiche di controllo del servizio (SCPs)	È ora possibile specificare le risorse, le condizioni e l'`NotAction` elemento in cui SCPs negare l'accesso a tutti gli account dell'organizzazione o dell'unità organizzativa (OU).	25 marzo 2019
Nuovi servizi per l'accesso sicuro	AWS License Manager e Service Catalog aggiunti come servizi compatibili con gli account dell'organizzazione.	21 dicembre 2018
Nuovi servizi per l'accesso sicuro	AWS CloudTrail e AWS RAM aggiunti come servizi compatibili con gli account dell'organizzazione.	4 dicembre 2018
Nuovo servizio per l'accesso sicuro	AWS Directory Service aggiunto come servizio in grado di funzionare con gli account dell'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 aggiunto come servizio in grado di funzionare con gli account dell'organizzazione.	20 giugno 2018
Nuovi servizi per l'accesso sicuro	AWS Config e AWS Firewall Manager aggiunti come servizi compatibili con gli account dell'organizzazione.	18 aprile 2018
Accesso sicuro ai servizi	Ora puoi abilitare o disabilitare l'accesso Servizi AWS a select to work negli account della tua organizzazione. IAM Identity Center è il servizio di affidabilità supportato iniziale.	29 marzo 2018
Ora rimozione dell'account self-service	Ora puoi rimuovere gli account che sono stati creati dall'interno AWS Organizations senza contattarli Supporto AWS.	19 dicembre 2017
È stato aggiunto il 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

AWS ha aggiunto un ruolo collegato al servizio a tutti gli account dell'organizzazione	Un ruolo collegato al servizio denominato `AWSServiceRoleForOrganizations` viene aggiunto a tutti gli account di un'organizzazione per consentire l'integrazione tra e altri. AWS Organizations 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 Supporto AWS.	15 giugno 2017
Avvio del servizio	Versione iniziale della AWS Organizations documentazione che ha accompagnato il lancio del nuovo servizio.	17 febbraio 2017

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.