aws

Guida per l'utente

AWS Resource Access Manager

AWS Resource Access Manager: Guida per l'utente

Table of Contents

Cos'è AWS Resource Access Manager?

AWS Resource Access Manager(AWS RAM) consente di condividere in modo sicuro le risorse traAccount AWS, all'interno dell'organizzazione o delle unità organizzative (OU) e con i ruoli e gli utentiAWS Identity and Access Management (IAM) per i tipi di risorse supportati. Se ne hai piùAccount AWS, puoi creare una risorsa una sola volta eAWS RAM usarla per renderla utilizzabile dagli altri account. Se l'account è gestito daAWS Organizations, è possibile condividere le risorse con tutti gli altri account dell'organizzazione o solo con gli account contenuti in una o più unità organizzative (OU) specificate. Puoi anche condividere con un ID account specificoAccount AWS, indipendentemente dal fatto che l'account faccia parte di un'organizzazione. Alcuni tipi di risorse supportati consentono anche di condividerli con ruoli e utenti IAM specificati.

Indice

Panoramica dei video

Il video seguente fornisce una breve introduzioneAWS RAM e descrive come creare una condivisione di risorse. Per ulteriori informazioni, consulta ???.

Il video seguente illustra come applicare le autorizzazioniAWS gestite alleAWS risorse. Per ulteriori informazioni, consulta ???.

In questo video viene illustrato come creare e associare le autorizzazioni gestite dal cliente seguendo le best practice dei privilegi minimi. Per ulteriori informazioni, consultare ???.

Vantaggi di AWS RAM

Perché utilizzare AWS RAM? Offre i seguenti vantaggi:

- Riduce il sovraccarico operativo: crea una risorsa una sola volta e usalaAWS RAM per condividerla con altri account. In questo modo viene meno la necessità di effettuare il provisioning di risorse duplicate in ogni account e si riducono i costi operativi. All'interno dell'account proprietario della risorsa,AWS RAM semplifica la concessione dell'accesso a ogni ruolo e utente di quell'account senza dover utilizzare criteri di autorizzazione basati sull'identità.
- Fornisce sicurezza e coerenza: semplifica la gestione della sicurezza per le risorse condivise utilizzando un unico set di politiche e autorizzazioni. Se invece dovessi creare risorse duplicate in tutti i tuoi account separati, avresti il compito di implementare politiche e autorizzazioni identiche e quindi mantenerle identiche per tutti quegli account. Al contrario, tutti gli utenti di una condivisione diAWS RAM risorse sono gestiti da un unico set di politiche e autorizzazioni. AWS RAMoffre un'esperienza coerente per la condivisione di diversi tipi diAWS risorse.
- Fornisce visibilità e verificabilità: visualizza i dettagli di utilizzo delle risorse condivise tramite l'integrazioneAWS RAM con Amazon CloudWatch eAWS CloudTrail. AWS RAMfornisce una visibilità completa delle risorse e degli account condivisi.

Che dire dell'accesso tra account con policy basate su risorse?

Puoi condividere alcuni tipi diAWS risorse con altriAccount AWS allegando una politica basata sulle risorse che identifichi i responsabiliAWS Identity and Access Management (IAM) (ruoli e utenti IAM) esterni al tuoAccount AWS. Tuttavia, la condivisione di una risorsa allegando una politica non sfrutta i vantaggi aggiuntivi cheAWS RAM offre. UtilizzandoAWS RAM si ottengono le seguenti caratteristiche:

- È possibile condividere con un'organizzazione o un'unità organizzativa (UO) senza dover enumerare tutti gliAccount AWS ID.
- Gli utenti possono vedere le risorse condivise con loro direttamente nellaServizio AWS console di origine e nelle operazioni API come se tali risorse fossero direttamente nell'account dell'utente. Ad esempio, se utilizzi perAWS RAM condividere una sottorete Amazon VPC con un altro account, gli utenti di quell'account possono vedere la sottorete nella console Amazon VPC e nei risultati delle operazioni API Amazon VPC eseguite in quell'account. Le risorse condivise allegando una politica basata sulle risorse non sono visibili in questo modo; devi invece scoprire e fare riferimento esplicito alla risorsa tramite il relativo Amazon Resource Name (ARN).

- I proprietari di una risorsa possono vedere quali responsabili hanno accesso a ogni singola risorsa che hanno condiviso.
- Se condividi risorse con un account che non fa parte della tua organizzazione,AWS RAM avvia una procedura di invito. Il destinatario deve accettare l'invito prima che il responsabile possa accedere alle risorse condivise. Dopo aver attivato la possibilità di condivisione all'interno dell'organizzazione, la condivisione con gli account dell'organizzazione non richiede inviti.

Se disponi di risorse che hai condiviso utilizzando una politica di autorizzazione basata sulle risorse, puoi promuoverle trasformandole in risorse completamenteAWS RAM gestite eseguendo una delle seguenti operazioni:

- Usa l'operazione API PromoteResourceShareCreatedFromPolicy.
- Usa l'equivalente dell'operazione API, che è il promote-resource-share-created-from-policycomandoAWS Command Line Interface (AWS CLI).

Come funziona la condivisione di risorse

Quando si condivide una risorsa dell'account proprietario con un altroAccount AWS, l'account di consumo, si concede l'accesso alla risorsa condivisa ai responsabili dell'account utente. Tutte le politiche e le autorizzazioni che si applicano ai ruoli e agli utenti dell'account utente si applicano anche alla risorsa condivisa. Le risorse della condivisione sembrano risorse native della condivisione conAccount AWS cui le hai condivise.

Puoi condividere risorse globali e regionali. Per ulteriori informazioni, consulta Condivisione delle risorse regionali rispetto alle risorse globali.

Condivisione delle risorse

Con AWS RAM, condividi le risorse di cui sei proprietario creando una condivisione delle risorse. Per creare una condivisione di risorse, si specifica quanto segue:

- Regione AWSIn cui si desidera creare la condivisione di risorse. Nella console, scegli dal menu a discesa Regione nell'angolo in alto a destra della console. NelAWS CLI, si utilizza il`--region` parametro.
  - Una condivisione di risorse può contenere solo risorse regionali che si trovano nellaRegione AWS stessa condivisione di risorse.

  - Una condivisione di risorse può contenere risorse globali solo se la condivisione di risorse si trova nella regione di origine designata per le risorse globali, Stati Uniti orientali (Virginia settentrionale)`us-east-1`.
- Un nome per la condivisione di risorse.
- L'elenco delle risorse a cui desideri concedere l'accesso come parte di questa condivisione di risorse.
- I responsabili a cui concedi l'accesso alla condivisione di risorse. I responsabili possono essere singoliAccount AWS, gli account di un'organizzazione o di un'unità organizzativa (OU) o singoli ruoli o utentiAWS Identity and Access Management (IAM).AWS Organizations

  > **Note**
  >
  > Non tutti i tipi di risorse possono essere condivisi con ruoli e utenti IAM. Per informazioni sulle risorse che puoi condividere con questi responsabili, consultaRisorse condivisibili AWS.

- Un'autorizzazione gestita per l'associazione a ogni tipo di risorsa che includi in una condivisione di risorse. L'autorizzazione gestita determina cosa possono fare i responsabili degli altri account con le risorse della condivisione di risorse.

  Il comportamento dell'autorizzazione dipende dal tipo di responsabile:

  - Se il committente si trova in un account diverso da quello proprietario della risorsa, le autorizzazioni associate alla condivisione di risorse sono le autorizzazioni massime disponibili da concedere ai ruoli e agli utenti di tali account. L'amministratore di tali account deve quindi concedere ai singoli ruoli e utenti l'accesso alla risorsa condivisa con politiche basate sull'identità IAM. Le autorizzazioni concesse in tali politiche non possono superare quelle definite nelle autorizzazioni allegate alla condivisione di risorse.

L'account proprietario delle risorse mantiene la piena proprietà delle risorse che condivide.

Utilizzo di risorse condivise

Quando il proprietario di una risorsa la condivide con il tuo account, puoi accedere alla risorsa condivisa proprio come faresti se fosse il tuo account la possedesse. È possibile accedere alla risorsa utilizzando la console,AWS CLI i comandi e le operazioni API del servizio pertinente. Le operazioni API che i responsabili del tuo account possono eseguire variano a seconda del tipo di risorsa e sono

specificate dall'AWS RAMautorizzazione associata alla condivisione di risorse. Continuano inoltre ad applicarsi tutte le politiche IAM e le politiche di controllo dei servizi configurate nel tuo account, il che ti consente di utilizzare gli investimenti esistenti nei controlli di sicurezza e governance.

Quando accedi a una risorsa condivisa utilizzando il servizio di quella risorsa, hai le stesse capacità e limitazioni delAccount AWS proprietario della risorsa.

- Se la risorsa è regionale, puoi accedervi solo da quellaRegione AWS in cui esiste nell'account proprietario.
- Se la risorsa è globale, è possibile accedervi da qualsiasi dispositivoRegione AWS supportato dalla console di servizio e dagli strumenti della risorsa. È possibile visualizzare e gestire la condivisione di risorse e le relative risorse globali nellaAWS RAM console e negli strumenti solo nella regione di origine designata, Stati Uniti orientali (Virginia settentrionale)`us-east-1`.

Accesso a AWS RAM

Puoi lavorare con AWS RAM nei modi descritti di seguito:

Console AWS RAM

AWS RAM fornisce la console AWS RAM, un'interfaccia utente basata sul Web. Se ti sei registrato e hai ottenuto unAccount AWS, puoi accedere allaAWS RAM console accedendo alla AWS Management Consolee scegliendoAWS RAM dalla pagina iniziale della console.

Puoi anche accedere direttamente alla AWS RAMconsole nel tuo browser. Se non ti sei già registrato, ti verrà chiesto di farlo prima che venga visualizzata la console.

AWS CLIe strumenti per Windows PowerShell

AWS CLIAWS Tools for PowerShellForniscono l'accesso diretto alle operazioni dell'APIAWS RAM pubblica. AWSsupporta questi strumenti suWindowsmacOS, eLinux. Per ulteriori informazioni sulle nozioni di base, consulta la Guida perAWS Command Line Interface l'utente o la Guida per l'AWS Tools for Windows PowerShellutente di. Per ulteriori informazioni sui comandi perAWS RAM, consulta Riferimento per iAWS CLI comandi o i riferimenti per i AWS Tools for Windows PowerShellcmdlet.

SDK AWS

AWSoffre comandi API per un'ampia gamma di linguaggi di programmazione. Per ulteriori informazioni sulle nozioni di base, consulta la Guida di riferimento per gliAWS SDK e gli strumenti.

API della query

Se non si utilizza uno dei linguaggi di programmazione supportati, l'API di interrogazioneAWS RAM HTTPS consente l'accesso programmatico aAWS RAM eAWS. Con l'AWS RAMAPI, puoi eseguire richieste HTTPS direttamente al servizio. Quando utilizzi le API AWS RAM, devi includere il codice per firmare in modo digitale le richieste utilizzando le tue credenziali. Per ulteriori informazioni, consulta la Documentazione di riferimento delle API di AWS RAM.

Prezzi di AWS RAM

Non sono previsti costi aggiuntivi per l'utilizzoAWS RAM o la creazione di condivisioni di risorse e la condivisione delle risorse tra account. I costi di utilizzo delle risorse variano a seconda del tipo di risorsa. Per ulteriori informazioni su comeAWS fatturare le risorse condivisibili, consulta la documentazione relativa al servizio di proprietà della risorsa.

Conformità e standard internazionali

PCI DSS

AWS RAMsupporta l'elaborazione, lo storage e la trasmissione di dati di carte di credito da parte di un esercente o di un provider di servizi, oltre a essere conforme allo standard Payment Card Industry Data Security Standard (PCI DSS).

Per ulteriori informazioni sullo standard PCI DSS, incluse le istruzioni su come richiedere una copia del Pacchetto conformità PCI di AWS, consulta PCI DSS livello 1.

FedRAMP

AWS RAMè autorizzata come FedRAMP Moderate neiRegioni AWS seguenti Stati Uniti orientali (Virginia), Stati Uniti orientali (Ohio), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (Oregon).

AWS RAMè autorizzato come FedRAMP High nei seguenti paesiRegioni AWS:AWS GovCloud (Stati Uniti occidentali) eAWS GovCloud (Stati Uniti orientali).

FedRAMP sta per Federal Risk and Authorization Management Program; si tratta di un programma federale statunitense per la gestione di rischio e autorizzazioni applicato a livello di pubblica amministrazione che fornisce un approccio standard a valutazioni di sicurezza, assegnazione di autorizzazioni e monitoraggio continuo nell'ambito di servizi e prodotti cloud.

Per ulteriori informazioni sulla conformità a FedRAMP, vedere FedRAMP.

SOC e ISO

AWS RAMpuò essere utilizzato per carichi di lavoro soggetti alla conformità al Service Organization Control (SOC) e agli standard ISO 9001, ISO 27001, ISO 27017, ISO 27018 e ISO 27701. I clienti del settore finanziario, sanitario e di altri settori regolamentati possono ottenere informazioni sui processi e sui controlli di sicurezza che proteggono i dati dei clienti, disponibili nei report SOC e nei certificatiAWS ISO e CSA STAR in AWS Artifact.

Per ulteriori informazioni sulla conformità SOC, consulta SOC.

Per ulteriori informazioni sulla conformità ISO, vedere ISO 9001, ISO 27001, ISO 27017, ISO 27018 e ISO 27701.

Nozioni di base su AWS RAM

ConAWS Resource Access Manager, puoi condividere le risorse di tua proprietàAccount AWS. Se il tuo account è gestito daAWS Organizations, puoi anche condividere risorse con gli altri account della tua organizzazione. Puoi anche utilizzare risorse condivise con te da altriAccount AWS.

Se non abiliti la condivisione all'internoAWS Organizations, non puoi condividere risorse con la tua organizzazione o con le unità organizzative (OU) dell'organizzazione. Tuttavia, è ancora possibile condividere risorse con altriAccount AWSnella tua organizzazione. Pertipi di risorse supportati, puoi anche condividere le risorse con singoli utentiAWS Identity and Access Managementruoli o utenti (IAM) della tua organizzazione. In questo caso, questi responsabili vengono trattati come se fossero account esterni, anziché come parte dell'organizzazione. ricevono un invito a unirsi alla condivisione di risorse e viene loro concesso l'invito a partecipare alla condivisione di risorse e, dopo averlo accettato, ottengono l'invito a unirsi alla condivisione di risorse e, dopo averlo accettato, ottengono l'invito

Indice

Termini e concetti per AWS RAM

I seguenti concetti aiutano a spiegare come è possibile utilizzare AWS Resource Access Manager (AWS RAM) per condividere le proprie risorse.

Condivisione delle risorse

Le risorse vengono condivise AWS RAM tramite la creazione di una condivisione di risorse. Una condivisione di risorse è composta dai tre elementi seguenti:

- Un elenco di una o più AWS risorse da condividere.
- Un elenco di uno o più responsabili a cui è concesso l'accesso alle risorse.
- Un'autorizzazione gestita per ogni tipo di risorsa inclusa nella condivisione. Ogni autorizzazione gestita si applica a tutte le risorse di quel tipo in quella condivisione di risorse.

Dopo aver creato una condivisione di risorse, AWS RAM ai principali specificati nella condivisione di risorse può essere concesso l'accesso alle risorse della condivisione.

- Se attivi la AWS RAM condivisione con AWS Organizations e i tuoi responsabili della condivisione fanno parte della stessa organizzazione dell'account di condivisione, tali responsabili possono ricevere l'accesso non appena l'amministratore dell'account concede loro le autorizzazioni per utilizzare le risorse utilizzando una AWS Identity and Access Management politica di autorizzazione (). IAM
- Se non attivi la AWS RAM condivisione con Organizations, puoi comunque condividere le risorse con le persone Account AWS che fanno parte della tua organizzazione. L'amministratore dell'account consumatore riceve un invito a partecipare alla condivisione di risorse e deve accettare l'invito prima che i responsabili specificati nella condivisione delle risorse possano accedere alle risorse condivise.
- È inoltre possibile condividere con account esterni all'organizzazione, se il tipo di risorsa lo supporta. L'amministratore dell'account consumatore riceve un invito a partecipare alla condivisione di risorse e deve accettare l'invito prima che i responsabili specificati nella condivisione delle risorse possano accedere alle risorse condivise. Per informazioni sui tipi di risorse che supportano questo tipo di condivisione, consulta Risorse condivisibili AWS e visualizza la colonna Può condividere con account esterni alla propria organizzazione.

Account di condivisione

L'account di condivisione contiene la risorsa condivisa e in cui l' AWS RAM amministratore crea la condivisione di AWS risorse utilizzando AWS RAM.

Un AWS RAM amministratore è un IAM principale che dispone delle autorizzazioni per creare e configurare condivisioni di risorse in. Account AWS Poiché AWS RAM funziona associando una politica basata sulle risorse alle risorse in una condivisione di risorse, l' AWS RAM amministratore deve inoltre disporre delle autorizzazioni per richiamare l'`PutResourcePolicy`operazione specificata Servizio AWS per ogni tipo di risorsa incluso in una condivisione di risorse.

Principi di consumo

L'account di consumo è l'account Account AWS con cui viene condivisa una risorsa. La condivisione delle risorse può specificare un intero account come principale o, per alcuni tipi di risorse, singoli ruoli o utenti dell'account. Per informazioni sui tipi di risorse che supportano questo tipo di condivisione, consulta Risorse condivisibili AWS e visualizza la colonna Può condividere con IAM ruoli e utenti.

AWS RAM supporta anche i responsabili del servizio in quanto consumatori di condivisioni di risorse. Per informazioni sui tipi di risorse che supportano questo tipo di condivisione, consulta Risorse condivisibili AWS e visualizza la colonna Può condividere con i responsabili del servizio.

I responsabili dell'account consumatore possono eseguire solo le azioni consentite da entrambe le seguenti autorizzazioni:

- Le autorizzazioni gestite allegate alla condivisione delle risorse. Queste specificano le autorizzazioni massime che possono essere concesse ai responsabili dell'account di consumo.
- Le politiche IAM basate sull'identità associate ai singoli ruoli o utenti dall'IAMamministratore dell'account utente. Tali politiche devono garantire `Allow` l'accesso a azioni specifiche e all'Amazon Resource Name (ARN) di una risorsa nell'account di condivisione.

AWS RAM supporta i seguenti tipi IAM principali in qualità di consumatori di condivisioni di risorse:

- Un altro Account AWS: la condivisione delle risorse rende disponibili all'account di condivisione le risorse incluse nell'account di condivisione all'account consumatore.
- IAMRuoli o utenti individuali in un altro account: alcuni tipi di risorse supportano la condivisione diretta con singoli IAM ruoli o utenti. Specificate questo tipo principale in base al suoARN.
  - IAMruolo — `arn:aws:iam::123456789012:role/rolename`
  - IAMutente — `arn:aws:iam::123456789012:user/username`
- Responsabile del servizio: condividi una risorsa con un AWS servizio per concedere al servizio l'accesso a una condivisione di risorse. La condivisione dei principali del servizio consente a un AWS servizio di intraprendere azioni per conto dell'utente per alleggerire l'onere operativo.

  Per condividere con un responsabile del servizio, scegli di consentire la condivisione con chiunque, quindi, in Seleziona il tipo principale, scegli Service principal dall'elenco a discesa. Specificate il nome del responsabile del servizio nel seguente formato:

  - *`service-id`*`.amazonaws.com`

  Per ridurre il rischio di confusione, la politica delle risorse mostra l'ID dell'account del proprietario della risorsa nella chiave di `aws:SourceAccount` condizione.
- Account di un'organizzazione: se l'account di condivisione è gestito da AWS Organizations, la condivisione delle risorse può specificare l'ID dell'organizzazione da condividere con tutti gli account dell'organizzazione. La condivisione di risorse può in alternativa specificare un ID di unità organizzativa (OU) da condividere con tutti gli account di quell'unità organizzativa. Un account

di condivisione può condividere solo con la propria organizzazione o unità organizzativa IDs all'interno della propria organizzazione. Specificare gli account ARN di un'organizzazione in base all'organizzazione o all'unità organizzativa.

- Tutti gli account di un'organizzazione: di seguito è riportato un esempio ARN di organizzazione in AWS Organizations:

  ```
  arn:aws:organizations::123456789012:organization/o-<orgid>
  ```

- Tutti gli account di un'unità organizzativa: di seguito è riportato un esempio ARN di ID OU:

  ```
  arn:aws:organizations::123456789012:organization/o-<orgid>/ou-<rootid>-<ouid>
  ```

> **Important**
>
> Quando si condivide con un'organizzazione o un'unità organizzativa e tale ambito include l'account proprietario della condivisione di risorse, tutti i responsabili dell'account di condivisione ottengono automaticamente l'accesso alle risorse della condivisione. L'accesso concesso è definito dalle autorizzazioni gestite associate alla condivisione. Ciò è dovuto al fatto che AWS RAM la politica basata sulle risorse associata a ciascuna risorsa della condivisione utilizza. `"Principal": "*"` Per ulteriori informazioni, consulta Implicazioni dell'uso "Principal": "*" in una politica basata sulle risorse.
> I responsabili degli altri account di consumo non hanno accesso immediato alle risorse della condivisione. Gli amministratori degli altri account devono prima allegare politiche di autorizzazione basate sull'identità ai principali appropriati. Tali politiche devono concedere `Allow` l'accesso alle singole risorse ARNs della condivisione di risorse. Le autorizzazioni contenute in tali politiche non possono superare quelle specificate nell'autorizzazione gestita associata alla condivisione di risorse.

Policy basata su risorse

Le politiche basate sulle risorse sono documenti di JSON testo che implementano il linguaggio delle politiche. IAM A differenza delle politiche basate sull'identità associate al principale, ad esempio un IAM ruolo o un utente, alla risorsa vengono allegate politiche basate sulle risorse. AWS RAM crea politiche basate sulle risorse per tuo conto in base alle informazioni fornite per la condivisione delle risorse. È necessario specificare un elemento di `Principal` policy che determini chi può accedere

alla risorsa. Per ulteriori informazioni, vedere Politiche basate sull'identità e politiche basate sulle risorse nella Guida per l'utente. IAM

Le politiche basate sulle risorse generate da vengono valutate insieme a tutti gli altri tipi di AWS RAM policy. IAM Ciò include tutte le politiche IAM basate sull'identità associate ai responsabili che stanno tentando di accedere alla risorsa, e le politiche di controllo dei servizi () che potrebbero applicarsi a. SCPs AWS Organizations Account AWS Le politiche basate sulle risorse generate da AWS RAM partecipano alla stessa logica di valutazione delle politiche di tutte le altre politiche. IAM Per i dettagli completi sulla valutazione delle politiche e su come determinare le autorizzazioni risultanti, consulta Logica di valutazione delle politiche nella Guida per l'utente. IAM

AWS RAM offre un'esperienza di condivisione delle risorse semplice e sicura fornendo policy di easy-to-use astrazione basate sulle risorse.

Per quei tipi di risorse che supportano le politiche basate sulle risorse, crea e gestisce AWS RAM automaticamente le politiche basate sulle risorse per te. Per una determinata risorsa, AWS RAM crea la politica basata sulle risorse combinando le informazioni provenienti da tutte le condivisioni di risorse che includono quella risorsa. Ad esempio, considera una pipeline Amazon SageMaker AI che condividi utilizzando AWS RAM e includi in due diverse condivisioni di risorse. Puoi utilizzare una condivisione di risorse per fornire l'accesso in sola lettura all'intera organizzazione. È quindi possibile utilizzare l'altra condivisione di risorse per concedere solo le autorizzazioni di esecuzione dell' SageMaker IA a un singolo account. AWS RAM combina automaticamente questi due diversi set di autorizzazioni in un'unica politica di risorse con più istruzioni. Quindi allega la politica combinata basata sulle risorse alla risorsa della pipeline. È possibile visualizzare questa politica di base in materia di risorse chiamando il GetResourcePolicyoperazione. Servizi AWS utilizza quindi tale politica basata sulle risorse per autorizzare qualsiasi principale che tenti di eseguire un'azione sulla risorsa condivisa.

Sebbene sia possibile creare manualmente le politiche basate sulle risorse e collegarle alle risorse chiamando`PutResourcePolicy`, si consiglia di AWS RAM utilizzarle perché offre i seguenti vantaggi:

- Disponibilità per gli utenti condivisi: se condividi le risorse utilizzando AWS RAM, gli utenti possono visualizzare tutte le risorse condivise con loro direttamente nella console del servizio di gestione delle risorse e API operare come se tali risorse fossero direttamente nell'account dell'utente. Ad esempio, se condividi un AWS CodeBuild progetto con un altro account, gli utenti dell'account consumatore possono vedere il progetto nella CodeBuild console e i risultati delle CodeBuild API operazioni eseguite. Le risorse condivise allegando direttamente una politica basata sulle risorse

non sono visibili in questo modo. Invece, è necessario scoprire e fare riferimento esplicitamente alla risorsa tramite la sua. ARN

- Gestibilità per i proprietari di azioni: se condividi risorse utilizzando AWS RAM, i proprietari delle risorse dell'account di condivisione possono vedere centralmente quali altri account hanno accesso alle proprie risorse. Se condividi una risorsa utilizzando una politica basata sulle risorse, puoi visualizzare gli account di consumo solo esaminando la politica per le singole risorse nella console di servizio pertinente o. API
- Efficienza: se condividi le risorse utilizzando AWS RAM, puoi condividere più risorse e gestirle come un'unità. Le risorse condivise utilizzando solo politiche basate sulle risorse richiedono politiche individuali allegate a ogni risorsa condivisa.
- Semplicità: non è necessario comprendere il linguaggio delle politiche JSON basato IAM sulle politiche. AWS RAM AWS RAM fornisce autorizzazioni ready-to-use AWS gestite tra cui scegliere da allegare alle condivisioni di risorse.

Utilizzando AWS RAM, puoi persino condividere alcuni tipi di risorse che non supportano ancora le politiche basate sulle risorse. Per tali tipi di risorse, genera AWS RAM automaticamente una politica basata sulle risorse come rappresentazione delle autorizzazioni effettive. Gli utenti possono visualizzare questa rappresentazione chiamando GetResourcePolicy. Ciò include i seguenti tipi di risorse:

- Amazon Aurora — cluster DB
- AmazonEC2: prenotazioni di capacità e host dedicati
- AWS License Manager — Configurazioni delle licenze
- AWS Outposts — Tabelle di routing, avamposti e siti dei gateway locali
- Amazon Route 53 — Regole di inoltro
- Amazon Virtual Private Cloud: IPv4 indirizzi, elenchi di prefissi, sottoreti, target Traffic Mirror, gateway di transito e domini multicast di gateway di transito di proprietà del cliente

AWS RAM Esempi di politiche generate basate sulle risorse

Se condividi una risorsa EC2 immagine Image Builder con un account individuale, AWS RAM genera una policy simile all'esempio seguente e la allega a tutte le risorse di immagine incluse nella condivisione di risorse.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::123456789012:root"},
            "Action": [
                "imagebuilder:GetImage",
                "imagebuilder:ListImages",
            ],
            "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
        }
    ]
}
```

Se condividi una risorsa EC2 immagine Image Builder con un IAMruolo o un utente in un altro ruolo Account AWS, AWS RAM genera una policy simile all'esempio seguente e la allega a tutte le risorse di immagine incluse nella condivisione di risorse.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/MySampleRole"
      },
      "Action": [
          "imagebuilder:GetImage",
          "imagebuilder:ListImages",
      ],
      "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
    }
  ]
}
```

Se si condivide una risorsa EC2 immagine Image Builder con tutti gli account di un'organizzazione o con gli account di un'unità organizzativa, AWS RAM genera una politica simile all'esempio seguente e la allega a tutte le risorse di immagine incluse nella condivisione di risorse.

> **Note**
>
> Questa politica utilizza `"Principal": "*"` e quindi utilizza l'`"Condition"`elemento per limitare le autorizzazioni alle identità che corrispondono a quelle specificate. `PrincipalOrgID` Per ulteriori informazioni, consulta Implicazioni dell'uso "Principal": "*" in una politica basata sulle risorse.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "imagebuilder:GetImage",
                "imagebuilder:ListImages",
            ],
            "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-123456789"
                }
            }
        }
    ]
}
```

Implicazioni dell'uso "Principal": "*" in una politica basata sulle risorse

Quando `"Principal": "*"` includi una politica basata sulle risorse, la politica concede l'accesso a tutti IAM i principali dell'account che contiene la risorsa, fatte salve le restrizioni imposte da un elemento, se esistente. `Condition` `Deny`Le dichiarazioni esplicite in qualsiasi politica che si applica al principale chiamante prevalgono sulle autorizzazioni concesse da questa politica. Tuttavia, una politica implicita ***`Deny`*** (vale a dire la mancanza di un elemento esplicito`Allow`) in qualsiasi politica di identità, permessi, limiti di sessione o policy di sessione applicabile non comporta la concessione ai principali di accedere `Deny` a un'azione mediante tale politica basata sulle risorse.

Se questo comportamento non è auspicabile per il tuo scenario, puoi limitarlo aggiungendo una ***Deny*** dichiarazione esplicita a una politica di identità, un limite di autorizzazioni o una politica di sessione che influenzi i ruoli e gli utenti pertinenti.

Autorizzazioni gestite

Le autorizzazioni gestite definiscono quali azioni possono eseguire i responsabili in quali condizioni sui tipi di risorse supportati in una condivisione di risorse. Quando si crea una condivisione di risorse, è necessario specificare quale autorizzazione gestita utilizzare per ogni tipo di risorsa incluso nella condivisione di risorse. Un'autorizzazione gestita elenca l'insieme `actions` e le condizioni che i responsabili possono eseguire con la risorsa condivisa utilizzando AWS RAM.

È possibile allegare una sola autorizzazione gestita per ogni tipo di risorsa in una condivisione di risorse. Non è possibile creare una condivisione di risorse in cui alcune risorse di un determinato tipo utilizzino un'autorizzazione gestita e altre risorse dello stesso tipo utilizzino un'autorizzazione gestita diversa. A tale scopo, è necessario creare due diverse condivisioni di risorse e suddividere le risorse tra di esse, assegnando a ciascun set un'autorizzazione gestita diversa. Esistono due diversi tipi di autorizzazioni gestite:

AWS autorizzazioni gestite

> AWS le autorizzazioni gestite vengono create e gestite da AWS e concedono autorizzazioni per scenari di clienti comuni. AWS RAM definisce almeno un'autorizzazione AWS gestita per ogni tipo di risorsa supportata. Alcuni tipi di risorse supportano più di un'autorizzazione AWS gestita, con un'autorizzazione gestita designata come AWS predefinita. L'autorizzazione AWS gestita predefinita è associata a meno che non venga specificato diversamente.

Autorizzazioni gestite dal cliente

> Le autorizzazioni gestite dai clienti sono autorizzazioni gestite che puoi creare e gestire specificando con precisione quali azioni possono essere eseguite in quali condizioni con l'utilizzo condiviso delle risorse. AWS RAM Ad esempio, desideri limitare l'accesso in lettura per i tuoi pool di Amazon VPC IP Address Manager (IPAM), che ti aiutano a gestire i tuoi indirizzi IP su larga scala. Puoi creare autorizzazioni gestite dal cliente per consentire ai tuoi sviluppatori di assegnare indirizzi IP, ma non visualizzare l'intervallo di indirizzi IP assegnati da altri account sviluppatore. Puoi seguire la best practice del privilegio minimo, concedendo solo le autorizzazioni necessarie per eseguire attività su risorse condivise.
>
> È possibile definire le proprie autorizzazioni per un tipo di risorsa in una condivisione di risorse con la possibilità di aggiungere condizioni come chiavi di contesto globali e chiavi specifiche

del servizio per specificare le condizioni in base alle quali i principali hanno accesso alla risorsa. Queste autorizzazioni possono essere utilizzate in una o più AWS RAM condivisioni. Le autorizzazioni gestite dal cliente sono specifiche della regione.

AWS RAM utilizza le autorizzazioni gestite come input per creare le politiche basate sulle risorse per le risorse condivise.

Versione con autorizzazione gestita

Qualsiasi modifica a un'autorizzazione gestita viene rappresentata come una nuova versione di tale autorizzazione gestita. La nuova versione è l'impostazione predefinita per tutte le nuove condivisioni di risorse. Ogni autorizzazione gestita ha sempre una versione designata come versione predefinita. Quando si AWS crea o si crea una nuova versione di autorizzazione gestita, è necessario aggiornare in modo esplicito l'autorizzazione gestita per ogni condivisione di risorse esistente. In questo passaggio puoi valutare le modifiche prima di applicarle alla tua condivisione di risorse. Tutte le nuove condivisioni di risorse utilizzeranno automaticamente la nuova versione dell'autorizzazione gestita per il tipo di risorsa corrispondente.

AWS versioni con autorizzazione gestita

AWS gestisce tutte le modifiche alle autorizzazioni AWS gestite. Tali modifiche risolvono nuove funzionalità o eliminano le carenze rilevate. Puoi applicare solo la versione di autorizzazione gestita predefinita alle tue condivisioni di risorse.

Versioni con autorizzazione gestita dal cliente

Gestisci tutte le modifiche alle autorizzazioni gestite dai clienti. Puoi creare una nuova versione predefinita, impostare una versione precedente come predefinita o eliminare versioni che non sono più associate a nessuna condivisione di risorse. Ogni autorizzazione gestita dal cliente può avere fino a cinque versioni.

Quando crei o aggiorni una condivisione di risorse, puoi allegare solo la versione predefinita dell'autorizzazione gestita specificata. Per ulteriori informazioni, consulta Aggiornamento delle autorizzazioniAWS gestite a una versione più recentissima.

Condivisione delle AWS risorse

Per condividere una risorsa di tua proprietà utilizzando AWS RAM, procedi come segue:

- Abilita la condivisione delle risorse all'interno AWS Organizations(opzionale)
- Creare una condivisione di risorse

> **Note**
>
> - La Account AWS condivisione di una risorsa con responsabili esterni al proprietario della risorsa non modifica le autorizzazioni o le quote applicabili alla risorsa all'interno dell'account che l'ha creata.
> - AWS RAM è un servizio regionale. I principali con cui condividi possono accedere alle condivisioni di risorse solo nelle aree Regioni AWS in cui sono state create.
> - Alcune risorse prevedono considerazioni e prerequisiti speciali per la condivisione. Per ulteriori informazioni, consulta Risorse condivisibili AWS.

Abilita la condivisione delle risorse all'interno AWS Organizations

Quando il tuo account è gestito da AWS Organizations, puoi trarne vantaggio per condividere le risorse più facilmente. Con o senza Organizations, un utente può condividere con account individuali. Tuttavia, se l'account si trova in un'organizzazione, è possibile condividerlo con singoli account o con tutti gli account dell'organizzazione o di un'unità organizzativa senza dover enumerare ogni account.

Per condividere le risorse all'interno di un'organizzazione, devi prima utilizzare la AWS RAM console o AWS Command Line Interface (AWS CLI) per abilitare la condivisione con. AWS Organizations Quando condividi risorse all'interno dell'organizzazione, AWS RAM non invia inviti ai dirigenti. I responsabili della tua organizzazione hanno accesso a risorse condivise senza scambiarsi inviti.

Quando abiliti la condivisione delle risorse all'interno dell'organizzazione, AWS RAM crea un ruolo collegato al servizio chiamato. **`AWSServiceRoleForResourceAccessManager`** Questo ruolo può essere assunto solo dal AWS RAM servizio e concede l' AWS RAM autorizzazione a recuperare informazioni sull'organizzazione di cui è membro, utilizzando la politica gestita. AWS `AWSResourceAccessManagerServiceRolePolicy`

Se non è più necessario condividere risorse con l'intera organizzazione oppure è possibile disabilitare OUs la condivisione delle risorse. Per ulteriori informazioni, consulta Disabilitazione della condivisione delle risorse con AWS Organizations.

Autorizzazioni minime

Per eseguire le procedure seguenti, devi accedere come responsabile all'account di gestione dell'organizzazione che dispone delle seguenti autorizzazioni:

- `ram:EnableSharingWithAwsOrganization`
- `iam:CreateServiceLinkedRole`
- `organizations:enableAWSServiceAccess`
- `organizations:DescribeOrganization`

Requisiti

- È possibile eseguire questi passaggi solo dopo aver effettuato l'accesso come responsabile nell'account di gestione dell'organizzazione.
- L'organizzazione deve avere tutte le funzionalità abilitate. Per ulteriori informazioni, vedere Abilitazione di tutte le funzionalità dell'organizzazione nella Guida per l'AWS Organizations utente.

> **Important**
>
> È necessario abilitare la condivisione con AWS Organizations utilizzando la AWS RAM console o il AWS CLI comando enable-sharing-with-aws-organization. Ciò garantisce la creazione del ruolo collegato ai servizi `AWSServiceRoleForResourceAccessManager`. Se abiliti l'accesso affidabile AWS Organizations utilizzando la AWS Organizations console o il enable-aws-service-access AWS CLI comando, il ruolo `AWSServiceRoleForResourceAccessManager` collegato al servizio non viene creato e non puoi condividere risorse all'interno dell'organizzazione.

Console

Per abilitare la condivisione delle risorse all'interno dell'organizzazione

1. Apri la pagina Impostazioni nella AWS RAM console.
2. Scegli Abilita condivisione con AWS Organizations, quindi scegli Salva impostazioni.

AWS CLI

Per abilitare la condivisione delle risorse all'interno dell'organizzazione

Utilizzate il comando enable-sharing-with-aws-organization.

Questo comando può essere utilizzato in qualsiasi Regione AWS ambiente e consente la condivisione AWS Organizations in tutte le regioni in cui AWS RAM è supportato.

```
$ aws ram enable-sharing-with-aws-organization
{
    "returnValue": true
}
```

Creare una condivisione di risorse

Per condividere le risorse di tua proprietà, crea una condivisione di risorse. Ecco una panoramica del processo:

1. Aggiungi le risorse che desideri condividere.
2. Per ogni tipo di risorsa che includi nella condivisione, specifica l'autorizzazione gestita da utilizzare per quel tipo di risorsa.
   - Puoi scegliere tra una delle autorizzazioni AWS gestite disponibili, un'autorizzazione gestita dal cliente esistente o creare una nuova autorizzazione gestita dal cliente.
   - AWS le autorizzazioni gestite vengono create AWS per coprire casi d'uso standard.
   - Le autorizzazioni gestite dai clienti ti consentono di personalizzare le tue autorizzazioni gestite per soddisfare le tue esigenze di sicurezza e aziendali.

   > **Note**
   >
   > Se l'autorizzazione gestita selezionata ha più versioni, allega AWS RAM automaticamente la versione predefinita. È possibile allegare solo la versione designata come predefinita.

3. Specificate i principali ai quali desiderate che abbiano accesso alle risorse.

Considerazioni

- Se in seguito devi eliminare una AWS risorsa inclusa in una condivisione, ti consigliamo di rimuovere prima la risorsa da qualsiasi condivisione di risorse che la include oppure di eliminare la condivisione di risorse.
- I tipi di risorse che puoi includere in una condivisione di risorse sono elencati inRisorse condivisibili AWS.
- Puoi condividere una risorsa solo se la possiedi. Non puoi condividere una risorsa condivisa con te.
- AWS RAM è un servizio regionale. Quando condividi una risorsa con i responsabili di altri Account AWS, tali principali devono accedere a ciascuna risorsa dalla stessa in Regione AWS cui è stata creata. Per le risorse globali supportate, puoi accedere a tali risorse da qualsiasi Regione AWS risorsa supportata dalla console di servizio e dagli strumenti di quella risorsa. È possibile visualizzare tali condivisioni di risorse e le relative risorse globali nella AWS RAM console e negli strumenti solo nella regione di origine designata, Stati Uniti orientali (Virginia settentrionale),`us-east-1`. Per ulteriori informazioni AWS RAM e risorse globali, vedereCondivisione delle risorse regionali rispetto alle risorse globali.
- Se l'account da cui condividi fa parte di un'organizzazione AWS Organizations e la condivisione all'interno dell'organizzazione è abilitata, a tutti i responsabili dell'organizzazione con cui condividi viene automaticamente concesso l'accesso alle condivisioni di risorse senza l'uso di inviti. Un responsabile di un account con cui condividi qualcosa al di fuori del contesto di un'organizzazione riceve un invito a partecipare alla condivisione di risorse e gli viene concesso l'accesso alle risorse condivise solo dopo aver accettato l'invito.
- Se condividi con un responsabile del servizio, non puoi associare nessun altro responsabile alla condivisione delle risorse.
- Se la condivisione avviene tra account o responsabili che fanno parte di un'organizzazione, qualsiasi modifica all'appartenenza all'organizzazione influirà dinamicamente sull'accesso alla condivisione delle risorse.
  - Se ne aggiungi un'altra Account AWS all'organizzazione o a un'unità organizzativa che ha accesso a una condivisione di risorse, il nuovo account membro ottiene automaticamente l'accesso alla condivisione di risorse. L'amministratore dell'account con cui hai condiviso l'account può quindi concedere ai singoli responsabili di quell'account l'accesso alle risorse di quella condivisione.
  - Se rimuovi un account dall'organizzazione o da un'unità organizzativa che ha accesso a una condivisione di risorse, tutti i responsabili di quell'account perderanno automaticamente l'accesso alle risorse a cui si accedeva tramite quella condivisione di risorse.

- Se hai condiviso direttamente con un account membro o con IAM ruoli o utenti dell'account membro e poi rimuovi tale account dall'organizzazione, tutti i responsabili di quell'account perderanno l'accesso alle risorse a cui accedeva tramite quella condivisione di risorse.

> **Important**
>
> Quando condividi con un'organizzazione o un'unità organizzativa e tale ambito include l'account proprietario della condivisione di risorse, tutti i responsabili dell'account di condivisione ottengono automaticamente l'accesso alle risorse della condivisione. L'accesso concesso è definito dalle autorizzazioni gestite associate alla condivisione. Questo perché la politica basata sulle risorse associata a ciascuna risorsa AWS RAM della condivisione utilizza. `"Principal": "*"` Per ulteriori informazioni, consulta Implicazioni dell'uso "Principal": "*" in una politica basata sulle risorse.
>
> I responsabili degli altri account di consumo non hanno accesso immediato alle risorse della condivisione. Gli amministratori degli altri account devono prima allegare politiche di autorizzazione basate sull'identità ai principali appropriati. Tali politiche devono consentire `Allow` l'accesso alle singole risorse ARNs della condivisione di risorse. Le autorizzazioni contenute in tali politiche non possono superare quelle specificate nell'autorizzazione gestita associata alla condivisione di risorse.

- Puoi aggiungere solo l'organizzazione di cui è membro l'account e quella OUs proveniente da tale organizzazione alle tue condivisioni di risorse. Non puoi aggiungere OUs organizzazioni esterne alla tua organizzazione a una condivisione di risorse come responsabili. Tuttavia, è possibile aggiungere IAM ruoli e utenti singoli Account AWS o, per i servizi supportati, esterni all'organizzazione come responsabili a una condivisione di risorse.

> **Note**
>
> Non tutti i tipi di risorse possono essere condivisi con IAM ruoli e utenti. Per informazioni sulle risorse che puoi condividere con questi responsabili, consultaRisorse condivisibili AWS.

- Per i seguenti tipi di risorse hai sette giorni di tempo per accettare l'invito a partecipare alla condivisione per i seguenti tipi di risorse. Se non accetti l'invito prima della scadenza, l'invito viene automaticamente rifiutato.

> **Important**
>
> Per i tipi di risorse condivise non presenti nell'elenco seguente, hai 12 ore per accettare l'invito a partecipare alla condivisione di risorse. Dopo 12 ore, l'invito scade e l'utente principale incluso nella condivisione delle risorse viene dissociato. L'invito non può più essere accettato dagli utenti finali.

- Amazon Aurora — cluster DB
- AmazonEC2: prenotazioni di capacità e host dedicati
- AWS License Manager — Configurazioni delle licenze
- AWS Outposts — Tabelle di routing, avamposti e siti dei gateway locali
- Amazon Route 53 — Regole di inoltro
- AmazonVPC: IPv4 indirizzi di proprietà del cliente, elenchi di prefissi, sottoreti, target Traffic Mirror, gateway di transito, domini multicast con gateway di transito

Console

Per creare una condivisione di risorse

1. Apri la AWS RAM console.
2. Poiché le condivisioni di AWS RAM risorse esistono in modo specifico Regioni AWS, scegli quella appropriata Regione AWS dall'elenco a discesa nell'angolo in alto a destra della console. Per visualizzare le condivisioni di risorse che contengono risorse globali, è necessario impostarle su Stati Uniti orientali (Virginia settentrionale), (). Regione AWS `us-east-1` Per ulteriori informazioni sulla condivisione di risorse globali, consultaCondivisione delle risorse regionali rispetto alle risorse globali. Se desideri includere risorse globali nella condivisione delle risorse, devi scegliere la regione di origine designata, Stati Uniti orientali (Virginia settentrionale),`us-east-1`.
3. Se sei nuovo AWS RAM, scegli Crea una condivisione di risorse dalla home page. Altrimenti, scegli Crea condivisione di risorse dalla pagina Condivisi da me: Condivisioni di risorse.
4. Nel Passaggio 1: Specificate i dettagli della condivisione delle risorse, effettuate le seguenti operazioni:

   a. In Nome, inserisci un nome descrittivo per la condivisione di risorse.

b. In Risorse, scegli le risorse da aggiungere alla condivisione di risorse come segue:

- Per Seleziona il tipo di risorsa, scegli il tipo di risorsa da condividere. In questo modo l'elenco delle risorse condivisibili viene filtrato solo in base alle risorse del tipo selezionato.
- Nell'elenco di risorse risultante, seleziona le caselle di controllo accanto alle singole risorse che desideri condividere. Le risorse selezionate vengono spostate in Risorse selezionate.

  Se condividi risorse associate a una zona di disponibilità specifica, l'utilizzo dell'ID della zona di disponibilità (ID AZ) ti aiuta a determinare la posizione relativa di queste risorse tra gli account. Per ulteriori informazioni, consulta ID delle zone di disponibilità perAWS le tue risorse.

c. (Facoltativo) Per allegare tag alla condivisione di risorse, in Tag, inserisci una chiave e un valore per il tag. Aggiungine altri selezionando Aggiungi nuovo tag. Ripeti questo passaggio se necessario. Questi tag si applicano solo alla condivisione di risorse stessa, non alle risorse incluse nella condivisione di risorse.

5. Scegli Next (Successivo).
6. Nel Passaggio 2: Associare un'autorizzazione gestita a ciascun tipo di risorsa, è possibile scegliere di associare un'autorizzazione gestita creata da AWS al tipo di risorsa, scegliere un'autorizzazione gestita dal cliente esistente oppure creare un'autorizzazione gestita dal cliente personalizzata per i tipi di risorse supportati. Per ulteriori informazioni, consulta Tipi di autorizzazioni gestite.

   Scegli Crea autorizzazione gestita dal cliente per creare un'autorizzazione gestita dal cliente che soddisfi i requisiti del tuo caso d'uso della condivisione. Per ulteriori informazioni, consulta Creazione di un'autorizzazione gestita dal cliente. Dopo aver completato il processo, scegli

   e poi puoi selezionare la tua nuova autorizzazione gestita dal cliente dall'elenco a discesa Autorizzazioni gestite.

> **Note**
>
> Se l'autorizzazione gestita selezionata ha più versioni, allega AWS RAM automaticamente la versione predefinita. È possibile allegare solo la versione designata come predefinita.

Per visualizzare le azioni consentite dall'autorizzazione gestita, espandi Visualizza il modello di policy per questa autorizzazione gestita.

7. Scegli Next (Successivo).
8. Nel passaggio 3: concedere l'accesso ai principali, procedi come segue:

   a. Per impostazione predefinita, è selezionata l'opzione Consenti la condivisione con chiunque, il che significa che, per i tipi di risorse Account AWS che la supportano, puoi condividere risorse con persone esterne all'organizzazione. Ciò non influisce sui tipi di risorse che possono essere condivise solo all'interno di un'organizzazione, come le VPC sottoreti Amazon. Puoi anche condividere alcuni tipi di risorse supportati con IAM ruoli e utenti.

      Per limitare la condivisione delle risorse solo agli account e ai responsabili dell'organizzazione, scegli Consenti la condivisione solo all'interno dell'organizzazione.

   b. Per i Responsabili, procedi come segue:

      - Per aggiungere l'organizzazione, un'unità organizzativa (OU) o una persona Account AWS che fa parte di un'organizzazione, attiva Mostra la struttura organizzativa. Viene visualizzata una visualizzazione ad albero dell'organizzazione. Quindi, seleziona la casella di controllo accanto a ciascun principale che desideri aggiungere.

        > **Important**
        >
        > Quando condividi con un'organizzazione o un'unità organizzativa e tale ambito include l'account proprietario della condivisione di risorse, tutti i responsabili dell'account di condivisione ottengono automaticamente l'accesso alle risorse della condivisione. L'accesso concesso è definito dalle autorizzazioni gestite associate alla condivisione. Questo perché la politica basata sulle risorse associata a ciascuna risorsa AWS RAM della condivisione utilizza.

`"Principal": "*"` Per ulteriori informazioni, consulta Implicazioni dell'uso "Principal": "*" in una politica basata sulle risorse.
I responsabili degli altri account di consumo non hanno accesso immediato alle risorse della condivisione. Gli amministratori degli altri account devono prima allegare politiche di autorizzazione basate sull'identità ai principali appropriati. Tali politiche devono consentire `Allow` l'accesso alle singole risorse ARNs della condivisione di risorse. Le autorizzazioni contenute in tali politiche non possono superare quelle specificate nell'autorizzazione gestita associata alla condivisione di risorse.

- Se si seleziona l'organizzazione (l'ID inizia cono-), tutti Account AWS i responsabili dell'organizzazione possono accedere alla condivisione delle risorse.
- Se si seleziona un'unità organizzativa (l'ID inizia conou-), tutti Account AWS gli amministratori dell'unità organizzativa e la relativa unità secondaria OUs possono accedere alla condivisione delle risorse.
- Se si seleziona una persona Account AWS, solo i responsabili di quell'account possono accedere alla condivisione delle risorse.

> **Note**
>
> L'interruttore Visualizza la struttura organizzativa viene visualizzato solo se la condivisione con AWS Organizations è abilitata e hai effettuato l'accesso all'account di gestione dell'organizzazione.
> Non puoi utilizzare questo metodo per specificare un IAM ruolo o un utente Account AWS esterno all'organizzazione. È invece necessario disattivare Visualizza la struttura organizzativa e utilizzare l'elenco a discesa e la casella di testo per inserire l'ID oARN.

- Per specificare un principale tramite ID oARN, compresi i responsabili esterni all'organizzazione, seleziona il tipo principale per ogni principale. Quindi, inserisci l'ID (per un' Account AWS organizzazione o unità organizzativa) o ARN (per un IAM ruolo o un utente), quindi scegli Aggiungi. I tipi principali, gli ID e i ARN formati disponibili sono i seguenti:
  - Account AWS— Per aggiungere un Account AWS, inserisci l'ID dell'account a 12 cifre. Per esempio:

```
123456789012
```

- Organizzazione: per aggiungere tutti i membri Account AWS della tua organizzazione, inserisci l'ID dell'organizzazione. Per esempio:

  ```
  o-abcd1234
  ```

- Unità organizzativa (OU): per aggiungere un'unità organizzativa, inserisci l'ID dell'unità organizzativa. Per esempio:

  ```
  ou-abcd-1234efgh
  ```

- IAMruolo: per aggiungere un IAM ruolo, immettere il ARN ruolo. Utilizzare la seguente sintassi:

  ```
  arn:partition:iam::account:role/role-name
  ```

  Per esempio:

  ```
  arn:aws:iam::123456789012:role/MyS3AccessRole
  ```

  > **Note**
  >
  > Per ottenere l'univoco ARN per un IAM ruolo, visualizza l'elenco dei ruoli nella IAM console, usa il AWS CLI comando get-role o l'azione GetRoleAPI.

- IAMutente: per aggiungere un IAM utente, inserisci il nome ARN dell'utente. Utilizzare la seguente sintassi:

  ```
  arn:partition:iam::account:user/user-name
  ```

  Per esempio:

  ```
  arn:aws:iam::123456789012:user/bob
  ```

  > **Note**
  >
  > Per ottenere l'univoco ARN di un IAM utente, visualizza l'elenco degli utenti nella IAM console, usa il get-user AWS CLI comando o GetUserAPIazione.

- Responsabile del servizio: per aggiungere un responsabile del servizio, scegli Responsabile del servizio dal dropbox Seleziona il tipo principale. Inserisci il nome del responsabile del AWS servizio. Utilizzare la seguente sintassi:
  - *service-id*.amazonaws.com

    Per esempio:

    pca-connector-ad.amazonaws.com

c. Per Principi selezionati, verifica che i principali specificati compaiano nell'elenco.

9. Scegli Next (Successivo).
10. Nel Passaggio 4: Revisione e creazione, rivedi i dettagli di configurazione per la condivisione delle risorse. Per modificare la configurazione per qualsiasi passaggio, scegli il link corrispondente al passaggio a cui desideri tornare e apporta le modifiche richieste.
11. Dopo aver esaminato la condivisione di risorse, scegli Crea condivisione di risorse.

    Il completamento dell'associazione tra la risorsa e il principale può richiedere alcuni minuti. Consenti il completamento di questo processo prima di provare a utilizzare la condivisione di risorse.
12. Puoi aggiungere e rimuovere risorse e principali o applicare tag personalizzati alla tua condivisione di risorse in qualsiasi momento. È possibile modificare l'autorizzazione gestita per i tipi di risorse inclusi nella condivisione delle risorse, per quei tipi che supportano più autorizzazioni gestite rispetto all'autorizzazione gestita predefinita. È possibile eliminare la condivisione di risorse quando non si desidera più condividere le risorse. Per ulteriori informazioni, consulta CondividiAWS le risorse di tua proprietà.

AWS CLI

Per creare una condivisione di risorse

Utilizzo dell'create-resource-sharecomando. Il comando seguente crea una condivisione di risorse condivisa con tutti i Account AWS membri dell'organizzazione. La condivisione contiene una configurazione di AWS License Manager licenza e concede le autorizzazioni gestite predefinite per quel tipo di risorsa.

> **Note**
>
> Se desideri utilizzare un'autorizzazione gestita dal cliente con un tipo di risorsa in questa condivisione di risorse, puoi utilizzare un'autorizzazione gestita dal cliente esistente o crearne una nuova. Prendi nota dell'ARNautorizzazione gestita dal cliente, quindi crea la condivisione di risorse. Per ulteriori informazioni, consulta Creazione di un'autorizzazione gestita dal cliente.

```
$ aws ram create-resource-share \
    --region us-east-1 \
    --name MyLicenseConfigShare \
    --permission-arns arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionLicenseConfiguration \
    --resource-arns arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-abc123 \
    --principals arn:aws:organizations::123456789012:organization/o-1234abcd
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
        "name": "MyLicenseConfigShare",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": true,
        "status": "ACTIVE",
        "creationTime": "2021-09-14T20:42:40.266000-07:00",
        "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00"
    }
}
```

Utilizzo diAWS risorse condivise

Per iniziare a utilizzare le risorse condivise con il tuo accountAWS Resource Access Manager, completa le seguenti attività.

Processi

- Rispondi all'invito alla condivisione della condivisione delle.
- Usa le risorse condivise con te

Rispondi all'invito alla condivisione della condivisione delle.

Se riceverai un invito a una condivisione, dovrai accettarlo per accedere alla condivisione.

Gli inviti non vengono utilizzati negli scenari riportati di seguito:

- Se fai parte di un'organizzazione inAWS Organizations e la condivisione nella tua organizzazione è abilitata, ai dirigenti nella tua organizzazione viene automaticamente concesso l'accesso all'elenco dei.
- Se condividi con ilAccount AWS proprietario della risorsa, i responsabili di quell'account accedono automaticamente alle risorse condivise senza inviti.

Console

Per rispondere agli inviti di

1. Apri la pagina Condiviso con me: condivisioni di risorse nellaAWS RAM console.

   > **Note**
   >
   > Una condivisione di risorse è visibile solo nel luogoRegione AWS in cui è stata creata. Se nella console non viene visualizzata una condivisione di risorse prevista, potrebbe essere necessario passare a un'altraRegione AWS utilizzando il menu a discesa nell'angolo in alto a destra.

2. Rivedi l'elenco delle condivisioni di risorse a cui ti è stato concesso l'accesso.

   La colonna Stato indica lo stato attuale della partecipazione alla condivisione di risorse. Lo`Pending` stato indica che sei stato aggiunto a una condivisione di risorse, ma non hai ancora accettato o rifiutato l'invito.

3. Per rispondere all'invito alla condivisione di risorse, seleziona l'ID di condivisione delle risorse e scegli Accetta condivisione di risorse per accettare l'invito o Rifiuta condivisione di risorse per rifiutare l'invito. Se rifiuti l'invito, non avrai accesso alle risorse. Se accetti l'invito, accedi alle risorse.

AWS CLI

Per iniziare, ottieni un elenco degli inviti alla condivisione delle risorse disponibili. Il seguente comando di esempio è stato eseguito nellaus-west-2 regione e mostra che una condivisione di risorse è disponibile nelloPENDING stato.

```
$ aws ram get-resource-share-invitations
{
    "resourceShareInvitations": [
        {
            "resourceShareInvitationArn": "arn:aws:ram:us-
west-2:111122223333:resource-share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111",
            "resourceShareName": "MyNewResourceShare",
            "resourceShareArn": "arn:aws:ram:us-west-2:111122223333:resource-
share/1234abcd-ef12-9876-5432-bbbbbb222222",
            "senderAccountId": "111122223333",
            "receiverAccountId": "444455556666",
            "invitationTimestamp": "2021-09-15T15:00:32.568000-07:00",
            "status": "PENDING"
        }
    ]
}
```

Puoi utilizzare l'Amazon Resource Name (ARN) dell'invito del comando precedente come parametro nel comando successivo per accettare quell'invito.

```
$ aws ram accept-resource-share-invitation \
    --resource-share-invitation-arn arn:aws:ram:us-west-2:111122223333:resource-
share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-west-2:111122223333:resource-
share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111",
        "resourceShareName": "MyNewResourceShare",
        "resourceShareArn": "arn:aws:ram:us-west-2:111122223333:resource-
share/1234abcd-ef12-9876-5432-bbbbbb222222",
        "senderAccountId": "111122223333",
        "receiverAccountId": "444455556666",
        "invitationTimestamp": "2021-09-15T15:14:12.580000-07:00",
        "status": "ACCEPTED"
    }
}
```

L'output mostra che `status` è cambiato in `ACCEPTED`. Le risorse incluse in quella quota di risorse sono ora disponibili per i dirigenti dell'account accettante.

Usa le risorse condivise con te

Dopo aver accettato l'invito a partecipare a una condivisione di risorse, puoi eseguire azioni specifiche sulle risorse condivise. Queste azioni possono variare a seconda del tipo di risorsa. Per ulteriori informazioni, consulta Risorse condivisibili AWS. Le risorse sono disponibili direttamente nella console di servizio e nelle operazioni API/CLI di ciascuna risorsa. Se la risorsa è regionale, è necessario utilizzare quella correttaRegione AWS nella console di servizio o nel comando API/CLI. Se la risorsa è globale, è necessario utilizzare la regione di origine designata, Stati Uniti orientali (Virginia settentrionale).`us-east-1` Per visualizzare la risorsa inAWS RAM, è necessario aprire laAWS RAM console inRegione AWS cui è stata creata la condivisione di risorse.

Lavorare conAWS risorse condivise

Puoi usareAWS Resource Access Manager (AWS RAM) per condividereAWS risorse di tua proprietà e accedere aAWS risorse condivise con te.

Indice

Condivisione delle risorse regionali rispetto alle risorse globali

Questo argomento illustra le differenze nel modo in cui AWS Resource Access Manager (AWS RAM) funziona con le risorse regionali e globali.

Le risorse sono regionali o globali. Puoi utilizzare il quarto campo in Amazon Resource Name (ARN) per identificare se una risorsa è regionale o globale. Le risorse regionali mostrano ilRegione AWS. Se è vuota, la risorsa è globale.

Quali sono le differenze tra risorse regionali e globali?

Risorse regionali

La maggior parte delle risorse con cui puoi condividere AWS RAM sono regionali. Li crei in una determinata Regione AWS regione e quindi esistono in quella regione. Per visualizzare o interagire con queste risorse, devi indirizzare le tue operazioni verso quella regione. Ad esempio, per creare un'istanza Amazon Elastic Compute Cloud (Amazon EC2) conAWS Management Console, scegli Regione AWS quella in cui desideri creare l'istanza. Se usi AWS Command Line Interface (AWS CLI) per creare l'istanza, includi il `--region` parametro. Gli AWS SDK hanno ciascuno il proprio meccanismo equivalente per specificare la regione utilizzata dall'operazione.

Esistono diversi motivi per utilizzare le risorse regionali. Una buona ragione è assicurarsi che le risorse e gli endpoint di servizio utilizzati per accedervi siano il più vicino possibile al cliente. Questo migliora le prestazioni riducendo al minimo la latenza. Un altro motivo è fornire un limite di isolamento. Ciò consente di creare copie indipendenti di risorse in più regioni per distribuire il carico e migliorare la scalabilità. Allo stesso tempo, isola le risorse l'una dall'altra per migliorare la disponibilità.

Se si specifica un valore diverso Regione AWS nella console o in un AWS CLI comando, non è più possibile visualizzare o interagire con le risorse visualizzate nella regione precedente.

Quando esamini l'Amazon Resource Name (ARN) per una risorsa regionale, la regione che contiene la risorsa viene specificata come quarto campo nell'ARN. Ad esempio, un'istanza Amazon EC2 è una risorsa regionale. Tali risorse hanno ARN simili all'esempio seguente per un VPC esistente nella `us-east-1` regione.

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

Risorse globali

Alcuni AWS servizi supportano risorse a cui è possibile accedere a livello globale, il che significa che è possibile utilizzare la risorsa da qualsiasi luogo. Non si specifica un Regione AWS nella console di un servizio globale. Per accedere a una risorsa globale, non è necessario specificare un `--region` parametro quando si utilizzano le operazioni del servizio AWS CLI e dell'AWSSDK.

Le risorse globali supportano i casi in cui è fondamentale che possa esistere solo un'istanza di una particolare risorsa alla volta. In tali scenari, la replica o la sincronizzazione tra copie in diverse regioni non è adeguata. La necessità di accedere a un unico endpoint globale, con il possibile aumento della latenza, è considerata accettabile per garantire che eventuali modifiche siano immediatamente visibili ai consumatori della risorsa. Ad esempio, quando crei una rete principale AWS Cloud WAN come risorsa globale, è coerente per tutti gli utenti. Si presenta come un'unica rete globale contigua in tutte le regioni.

L'Amazon Resource Name (ARN) per una risorsa globale non include una regione. Il quarto campo di tale ARN è vuoto, come il seguente esempio di ARN per una rete core Cloud WAN.

```
arn:aws:networkmanager::123456789012:core-network/core-network-0514d38fa6f796cea
```

Condivisioni di risorse e relative regioni

AWS RAMè un servizio regionale e una condivisione di risorse è regionale. Pertanto, una condivisione di risorse può contenere risorse provenienti dalla Regione AWS stessa condivisione di risorse e qualsiasi risorsa globale supportata. La regione in cui si crea la condivisione di risorse è la regione di origine della condivisione di risorse.

> **Important**
>
> Attualmente, puoi creare condivisioni di risorse con risorse globali solo nella regione di origine designata degli Stati Uniti orientali (Virginia settentrionale),`us-east-1`. Sebbene sia possibile creare la condivisione di risorse solo in quella singola regione di origine, qualsiasi risorsa globale condivisa appare come risorsa globale standard se visualizzata nella console o nelle operazioni CLI e SDK di quel servizio. La restrizione alla regione di origine si applica solo alla condivisione di risorse, non alle risorse in essa contenute.

Per condividere una risorsa regionale creata nella `us-west-2` regione, devi configurare la AWS RAM console per utilizzarla `us-west-2` e crearla. Non puoi creare una condivisione di risorse che includa risorse regionali diverseRegioni AWS. Ciò significa che per condividere le risorse di entrambe `us-west-2` le partie`u-north-1`, è necessario creare due diverse condivisioni di risorse. Non puoi combinare risorse di due regioni diverse in un'unica condivisione di risorse.

Per condividere una risorsa globale nella AWS RAM console, è necessario configurare la AWS RAM console per utilizzare la regione di origine designata, Stati Uniti orientali (Virginia settentrionale)`us-`

`east-1`. Quindi, crea la condivisione di risorse nella regione di origine designata. Puoi combinare risorse globali in una condivisione di risorse solo con risorse della `us-east-1` regione.

Anche se la risorsa globale è visualizzabile in una condivisione di AWS RAM risorse solo nella regione di origine designata, è comunque una risorsa globale dopo la condivisione. Puoi accedervi nella sezione condivisa Account AWS da qualsiasi regione dalla quale potevi accedervi nell'originaleAccount AWS.

Considerazioni

- Per creare una condivisione di risorse nella AWS RAM console, è necessario utilizzare la regione che contiene le risorse che si desidera condividere. Se desideri includere una risorsa globale, devi utilizzare la regione di origine designata per creare la condivisione. Ad esempio, per condividere una rete principale AWS Cloud WAN, è necessario creare la condivisione di risorse nella `us-east-1` regione.
- Per visualizzare o modificare una condivisione di risorse nella AWS RAM console, è necessario utilizzare la regione che contiene la condivisione di risorse. Allo stesso modo, le operazioni AWS RAM AWS CLI e SDK consentono di interagire solo con le condivisioni di risorse che si trovano nella regione specificata nell'operazione. Per visualizzare o modificare le condivisioni di risorse che contengono risorse globali, è necessario utilizzare la regione di origine designata, Stati Uniti orientali (Virginia settentrionale). `us-east-1`
- Per visualizzare una risorsa regionale nella AWS RAM console e includerla in una condivisione di risorse, è necessario utilizzare la regione che contiene la risorsa regionale.
- Per visualizzare una risorsa globale nella AWS RAM console e includerla in una condivisione di risorse, è necessario utilizzare la regione di origine designata, Stati Uniti orientali (Virginia settentrionale). `us-east-1`
- Puoi creare una condivisione di risorse con risorse regionali e globali solo nella regione di origine designata, Stati Uniti orientali (Virginia settentrionale). `us-east-1`

CondividiAWS le risorse di tua proprietà

Puoi usareAWS Resource Access Manager (AWS RAM) per condividere le risorse che specifichi con i principali che specifichi. Questa sezione descrive come creare nuove condivisioni di risorse, modificare le condivisioni di risorse esistenti ed eliminare le condivisioni di risorse che non sono più necessarie.

Argomenti

Visualizzazione delle condivisioni di risorse create inAWS RAM

Puoi visualizzare un elenco delle condivisioni di risorse che hai creato. Puoi vedere quali risorse stai condividendo e i responsabili con cui sono condivise.

Console

Per visualizzare le condivisioni di risorse

1. Apri la pagina Condiviso da me: condivisioni di risorse nellaAWS RAM console.
2. Poiché le condivisioni diAWS RAM risorse esistono in particolareRegioni AWS, scegliere la più appropriataRegione AWS dall'elenco a discesa nell'angolo in alto a destra della console. Per visualizzare le condivisioni che contengono risorse globali, è necessarioRegione AWS impostarle su Stati Uniti orientali (Virginia settentrionale), (`us-east-1`). Per ulteriori informazioni sulla condivisione di risorse globali, consultaCondivisione delle risorse regionali rispetto alle risorse globali.
3. Se una delle autorizzazioni gestite utilizzate dalle condivisioni di risorse nei risultati dispone di una nuova versione dell'autorizzazione gestita designata come predefinita, la pagina visualizza un banner per avvisare l'utente. Puoi scegliere di aggiornare tutte le versioni delle autorizzazioni gestite contemporaneamente scegliendo Rivedi e aggiorna tutto nella parte superiore della pagina.

   In alternativa, per le singole condivisioni di risorse con una o più nuove versioni delle autorizzazioni gestite, la colonna Stato mostra Aggiornamento disponibile. La scelta di quel collegamento avvia il processo di revisione delle versioni aggiornate delle autorizzazioni gestite e consente di assegnarle come versioni per i tipi di risorse pertinenti in quell'unica condivisione di risorse.
4. (Facoltativo) Applica un filtro per trovare condivisioni di risorse specifiche. È possibile applicare più filtri per limitare la ricerca. È possibile digitare una parola chiave, ad esempio

parte del nome di una condivisione di risorse, per elencare solo le condivisioni di risorse che includono quel testo nel nome. Scegli la casella di testo per visualizzare un elenco a discesa dei campi degli attributi suggeriti. Dopo averne scelto uno, puoi scegliere dall'elenco dei valori disponibili per quel campo. Puoi aggiungere altri attributi o parole chiave fino a trovare la risorsa desiderata.

5. scegliere il nome della condivisione della risorsa da esaminare. La console visualizza le seguenti informazioni sulla condivisione di risorse:

   - Riepilogo: elenca il nome della condivisione della risorsa, l'ID, il proprietario, il nome della risorsa Amazon (ARN), la data di creazione, se consente la condivisione con account esterni e il suo stato attuale.
   - Autorizzazioni gestite: elenca le autorizzazioni gestite allegate a questa condivisione di risorse. Può essere disponibile al massimo un'autorizzazione gestita per tipo di risorsa inclusa nella condivisione. Ogni autorizzazione gestita visualizza la versione dell'autorizzazione gestita associata alla condivisione di risorse. Se non è la versione predefinita, la console visualizza un collegamento Aggiorna alla versione predefinita. Se scegli quel link, ti viene offerta la possibilità di aggiornare la condivisione di risorse per utilizzare la versione predefinita.
   - Risorse condivise: elenca le singole risorse incluse nella condivisione di risorse. Scegli l'ID di una risorsa per aprire una nuova scheda del browser per visualizzare la risorsa nella console del servizio nativo.
   - Responsabili condivisi: elenca i responsabili con cui vengono condivise le risorse.
   - Tag: elenca le coppie chiave-valore del tag allegate alla condivisione di risorse stessa; queste non sono le etichette associate alle singole risorse incluse nella condivisione di risorse.

AWS CLI

Per visualizzare le condivisioni di risorse

Puoi utilizzare il get-resource-sharescomando con il parametro`--resource-owner` impostato`SELF` per visualizzare i dettagli delle condivisioni di risorse create nel tuoAccount AWS.

L'esempio seguente mostra le condivisioni di risorse condivise in currentRegione AWS (`us-east-1`) per la chiamataAccount AWS. Per ottenere le condivisioni di risorse create in una regione diversa, utilizza il`--region` *`<region-code>`* parametro. Per includere le condivisioni

di risorse che contengono risorse globali, è necessario specificare la regione Stati Uniti orientali (Virginia settentrionale),`us-east-1`.

```
$  aws ram get-resource-shares \
    --resource-owner SELF
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425",
            "name": "MySubnetShare",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-10T15:38:54.449000-07:00",
            "lastUpdatedTime": "2021-09-10T15:38:54.449000-07:00",
            "featureSet": "STANDARD"
        },
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/818d71dd-7512-4f71-99c6-2ae57aa010bc",
            "name": "MyLicenseConfigShare",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-14T20:42:40.266000-07:00",
            "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
```

Creazione di una condivisione di risorse in AWS RAM

Per condividere risorse di tua proprietà, crea una condivisione di risorse. Ecco una panoramica del processo:

1. Aggiungi le risorse che desideri condividere.
2. Per ogni tipo di risorsa che includi nella condivisione, specifica l'autorizzazione gestita da utilizzare per quel tipo di risorsa.

- Puoi scegliere tra una delle autorizzazioni AWS gestite disponibili, un'autorizzazione gestita dal cliente esistente o creare una nuova autorizzazione gestita dal cliente.
- AWS le autorizzazioni gestite vengono create AWS per coprire casi d'uso standard.
- Le autorizzazioni gestite dai clienti ti consentono di personalizzare le tue autorizzazioni gestite per soddisfare le tue esigenze di sicurezza e aziendali.

> **Note**
>
> Se l'autorizzazione gestita selezionata ha più versioni, allega AWS RAM automaticamente la versione predefinita. È possibile allegare solo la versione designata come predefinita.

3. Specificate i principali ai quali desiderate che abbiano accesso alle risorse.

Considerazioni

- Se in un secondo momento devi eliminare una AWS risorsa inclusa in una condivisione, ti consigliamo di rimuovere prima la risorsa da qualsiasi condivisione di risorse che la include oppure di eliminare la condivisione di risorse.
- I tipi di risorse che puoi includere in una condivisione di risorse sono elencati inRisorse condivisibili AWS.
- Puoi condividere una risorsa solo se la possiedi. Non puoi condividere una risorsa condivisa con te.
- AWS RAM è un servizio regionale. Quando condividi una risorsa con i responsabili di altri Account AWS, tali principali devono accedere a ciascuna risorsa dalla stessa in Regione AWS cui è stata creata. Per le risorse globali supportate, puoi accedere a tali risorse da qualsiasi Regione AWS risorsa supportata dalla console di servizio e dagli strumenti di quella risorsa. È possibile visualizzare tali condivisioni di risorse e le relative risorse globali nella AWS RAM console e negli strumenti solo nella regione di origine designata, Stati Uniti orientali (Virginia settentrionale),`us-east-1`. Per ulteriori informazioni AWS RAM e risorse globali, vedereCondivisione delle risorse regionali rispetto alle risorse globali.
- Se l'account da cui condividi fa parte di un'organizzazione AWS Organizations e la condivisione all'interno dell'organizzazione è abilitata, a tutti i responsabili dell'organizzazione con cui condividi viene automaticamente concesso l'accesso alle condivisioni di risorse senza l'uso di inviti. Un responsabile di un account con cui condividi qualcosa al di fuori del contesto di un'organizzazione riceve un invito a partecipare alla condivisione di risorse e gli viene concesso l'accesso alle risorse condivise solo dopo aver accettato l'invito.

- Se condividi con un responsabile del servizio, non puoi associare nessun altro responsabile alla condivisione delle risorse.
- Se la condivisione avviene tra account o responsabili che fanno parte di un'organizzazione, qualsiasi modifica all'appartenenza all'organizzazione influirà dinamicamente sull'accesso alla condivisione delle risorse.
  - Se ne aggiungi un'altra Account AWS all'organizzazione o a un'unità organizzativa che ha accesso a una condivisione di risorse, il nuovo account membro ottiene automaticamente l'accesso alla condivisione di risorse. L'amministratore dell'account con cui hai condiviso l'account può quindi concedere ai singoli responsabili di quell'account l'accesso alle risorse di quella condivisione.
  - Se rimuovi un account dall'organizzazione o da un'unità organizzativa che ha accesso a una condivisione di risorse, tutti i responsabili di quell'account perderanno automaticamente l'accesso alle risorse a cui si accedeva tramite quella condivisione di risorse.
  - Se hai condiviso direttamente con un account membro o con IAM ruoli o utenti nell'account membro e poi rimuovi tale account dall'organizzazione, tutti i responsabili di quell'account perderanno l'accesso alle risorse a cui accedeva tramite quella condivisione di risorse.

  Important

  Quando condividi con un'organizzazione o un'unità organizzativa e tale ambito include l'account proprietario della condivisione di risorse, tutti i responsabili dell'account di condivisione ottengono automaticamente l'accesso alle risorse della condivisione. L'accesso concesso è definito dalle autorizzazioni gestite associate alla condivisione. Ciò è dovuto al fatto che AWS RAM la politica basata sulle risorse associata a ciascuna risorsa della condivisione utilizza. `"Principal": "*"` Per ulteriori informazioni, consulta Implicazioni dell'uso "Principal": "*" in una politica basata sulle risorse.
  I responsabili degli altri account di consumo non hanno accesso immediato alle risorse della condivisione. Gli amministratori degli altri account devono prima allegare politiche di autorizzazione basate sull'identità ai principali appropriati. Tali politiche devono consentire `Allow` l'accesso alle singole risorse ARNs della condivisione di risorse. Le autorizzazioni contenute in tali politiche non possono superare quelle specificate nell'autorizzazione gestita associata alla condivisione di risorse.

- Puoi aggiungere solo l'organizzazione di cui è membro l'account e quella OUs proveniente da tale organizzazione alle tue condivisioni di risorse. Non puoi aggiungere OUs organizzazioni esterne alla tua organizzazione a una condivisione di risorse come responsabili. Tuttavia, è

possibile aggiungere IAM ruoli e utenti singoli Account AWS o, per i servizi supportati, esterni all'organizzazione come responsabili a una condivisione di risorse.

> **Note**
>
> Non tutti i tipi di risorse possono essere condivisi con IAM ruoli e utenti. Per informazioni sulle risorse che puoi condividere con questi responsabili, consultaRisorse condivisibili AWS.

- Per i seguenti tipi di risorse hai sette giorni di tempo per accettare l'invito a partecipare alla condivisione per i seguenti tipi di risorse. Se non accetti l'invito prima della scadenza, l'invito viene automaticamente rifiutato.

  > **Important**
  >
  > Per i tipi di risorse condivise non presenti nell'elenco seguente, hai 12 ore per accettare l'invito a partecipare alla condivisione di risorse. Dopo 12 ore, l'invito scade e l'utente principale incluso nella condivisione delle risorse viene dissociato. L'invito non può più essere accettato dagli utenti finali.

  - Amazon Aurora — cluster DB
  - AmazonEC2: prenotazioni di capacità e host dedicati
  - AWS License Manager — Configurazioni delle licenze
  - AWS Outposts — Tabelle di routing, avamposti e siti dei gateway locali
  - Amazon Route 53 — Regole di inoltro
  - AmazonVPC: IPv4 indirizzi di proprietà del cliente, elenchi di prefissi, sottoreti, target Traffic Mirror, gateway di transito, domini multicast con gateway di transito

Console

Per creare una condivisione di risorse

1. Apri la AWS RAM console.
2. Poiché le condivisioni di AWS RAM risorse esistono in modo specifico Regioni AWS, scegli quella appropriata Regione AWS dall'elenco a discesa nell'angolo in alto a destra

della console. Per visualizzare le condivisioni di risorse che contengono risorse globali, è necessario impostarle su Stati Uniti orientali (Virginia settentrionale), (). Regione AWS `us-east-1` Per ulteriori informazioni sulla condivisione di risorse globali, consultaCondivisione delle risorse regionali rispetto alle risorse globali. Se desideri includere risorse globali nella condivisione delle risorse, devi scegliere la regione di origine designata, Stati Uniti orientali (Virginia settentrionale),`us-east-1`.

3. Se sei nuovo AWS RAM, scegli Crea una condivisione di risorse dalla home page. Altrimenti, scegli Crea condivisione di risorse dalla pagina Condivisi da me: Condivisioni di risorse.
4. Nel Passaggio 1: Specificate i dettagli della condivisione delle risorse, effettuate le seguenti operazioni:

   a. In Nome, inserisci un nome descrittivo per la condivisione di risorse.

   b. In Risorse, scegli le risorse da aggiungere alla condivisione di risorse come segue:

      - Per Seleziona il tipo di risorsa, scegli il tipo di risorsa da condividere. In questo modo l'elenco delle risorse condivisibili viene filtrato solo in base alle risorse del tipo selezionato.
      - Nell'elenco di risorse risultante, seleziona le caselle di controllo accanto alle singole risorse che desideri condividere. Le risorse selezionate vengono spostate in Risorse selezionate.

        Se condividi risorse associate a una zona di disponibilità specifica, l'utilizzo dell'ID della zona di disponibilità (ID AZ) ti aiuta a determinare la posizione relativa di queste risorse tra gli account. Per ulteriori informazioni, consulta ID delle zone di disponibilità perAWS le tue risorse.

   c. (Facoltativo) Per allegare tag alla condivisione di risorse, in Tag, inserisci una chiave e un valore per il tag. Aggiungine altri selezionando Aggiungi nuovo tag. Ripeti questo passaggio se necessario. Questi tag si applicano solo alla condivisione di risorse stessa, non alle risorse incluse nella condivisione di risorse.
5. Scegli Next (Successivo).
6. Nel Passaggio 2: Associa un'autorizzazione gestita a ciascun tipo di risorsa, puoi scegliere di associare un'autorizzazione gestita creata da AWS al tipo di risorsa, scegliere un'autorizzazione gestita dal cliente esistente oppure creare un'autorizzazione gestita dal cliente personalizzata per i tipi di risorse supportati. Per ulteriori informazioni, consulta Tipi di autorizzazioni gestite.

Scegli Crea autorizzazione gestita dal cliente per creare un'autorizzazione gestita dal cliente che soddisfi i requisiti del tuo caso d'uso della condivisione. Per ulteriori informazioni, consulta Creazione di un'autorizzazione gestita dal cliente. Dopo aver completato il processo, scegli

e poi puoi selezionare la tua nuova autorizzazione gestita dal cliente dall'elenco a discesa Autorizzazioni gestite.

> **Note**
>
> Se l'autorizzazione gestita selezionata ha più versioni, allega AWS RAM automaticamente la versione predefinita. È possibile allegare solo la versione designata come predefinita.

Per visualizzare le azioni consentite dall'autorizzazione gestita, espandi Visualizza il modello di policy per questa autorizzazione gestita.

7. Scegli Next (Successivo).
8. Nel passaggio 3: concedere l'accesso ai principali, procedi come segue:

   a. Per impostazione predefinita, è selezionata l'opzione Consenti la condivisione con chiunque, il che significa che, per i tipi di risorse Account AWS che la supportano, puoi condividere risorse con persone esterne all'organizzazione. Ciò non influisce sui tipi di risorse che possono essere condivise solo all'interno di un'organizzazione, come le VPC sottoreti Amazon. Puoi anche condividere alcuni tipi di risorse supportati con IAM ruoli e utenti.

      Per limitare la condivisione delle risorse solo agli account e ai responsabili dell'organizzazione, scegli Consenti la condivisione solo all'interno dell'organizzazione.

   b. Per i Responsabili, procedi come segue:

      - Per aggiungere l'organizzazione, un'unità organizzativa (OU) o una persona Account AWS che fa parte di un'organizzazione, attiva Mostra la struttura organizzativa. Viene visualizzata una visualizzazione ad albero dell'organizzazione. Quindi, seleziona la casella di controllo accanto a ciascun principale che desideri aggiungere.

> **Important**
>
> Quando condividi con un'organizzazione o un'unità organizzativa e tale ambito include l'account proprietario della condivisione di risorse, tutti i responsabili dell'account di condivisione ottengono automaticamente l'accesso alle risorse della condivisione. L'accesso concesso è definito dalle autorizzazioni gestite associate alla condivisione. Ciò è dovuto al fatto che AWS RAM la politica basata sulle risorse associata a ciascuna risorsa della condivisione utilizza. `"Principal": "*"` Per ulteriori informazioni, consulta Implicazioni dell'uso "Principal": "*" in una politica basata sulle risorse.
>
> I responsabili degli altri account di consumo non hanno accesso immediato alle risorse della condivisione. Gli amministratori degli altri account devono prima allegare politiche di autorizzazione basate sull'identità ai principali appropriati. Tali politiche devono consentire `Allow` l'accesso alle singole risorse ARNs della condivisione di risorse. Le autorizzazioni contenute in tali politiche non possono superare quelle specificate nell'autorizzazione gestita associata alla condivisione di risorse.

- Se si seleziona l'organizzazione (l'ID inizia cono-), tutti Account AWS i responsabili dell'organizzazione possono accedere alla condivisione delle risorse.
- Se si seleziona un'unità organizzativa (l'ID inizia conou-), tutti Account AWS gli amministratori dell'unità organizzativa e la relativa unità secondaria OUs possono accedere alla condivisione delle risorse.
- Se si seleziona una persona Account AWS, solo i responsabili di quell'account possono accedere alla condivisione delle risorse.

> **Note**
>
> L'interruttore Visualizza la struttura organizzativa viene visualizzato solo se la condivisione con AWS Organizations è abilitata e hai effettuato l'accesso all'account di gestione dell'organizzazione.
>
> Non puoi utilizzare questo metodo per specificare un IAM ruolo o un utente Account AWS esterno all'organizzazione. È invece necessario disattivare

Visualizza la struttura organizzativa e utilizzare l'elenco a discesa e la casella di testo per inserire l'ID oARN.

- Per specificare un principale tramite ID oARN, compresi i responsabili esterni all'organizzazione, seleziona il tipo principale per ogni principale. Quindi, inserisci l'ID (per un' Account AWS organizzazione o unità organizzativa) o ARN (per un IAM ruolo o un utente), quindi scegli Aggiungi. I tipi principali, gli ID e i ARN formati disponibili sono i seguenti:
  - Account AWS— Per aggiungerne uno Account AWS, inserisci l'ID dell'account a 12 cifre. Per esempio:

    `123456789012`
  - Organizzazione: per aggiungere tutti i membri Account AWS della tua organizzazione, inserisci l'ID dell'organizzazione. Per esempio:

    `o-abcd1234`
  - Unità organizzativa (OU): per aggiungere un'unità organizzativa, inserisci l'ID dell'unità organizzativa. Per esempio:

    `ou-abcd-1234efgh`
  - IAMruolo: per aggiungere un IAM ruolo, immettere il ARN ruolo. Utilizzare la seguente sintassi:

    `arn:partition:iam::account:role/role-name`

    Per esempio:

    `arn:aws:iam::123456789012:role/MyS3AccessRole`

    > **Note**
    >
    > Per ottenere l'univoco ARN per un IAM ruolo, visualizza l'elenco dei ruoli nella IAM console, usa il AWS CLI comando get-role o l'azione GetRoleAPI.
  - IAMutente: per aggiungere un IAM utente, inserisci il nome ARN dell'utente. Utilizzare la seguente sintassi:

    `arn:partition:iam::account:user/user-name`

Per esempio:

```
arn:aws:iam::123456789012:user/bob
```

> **Note**
>
> Per ottenere l'univoco ARN di un IAM utente, visualizza l'elenco degli utenti nella IAM console, usa il get-user AWS CLI comando o GetUserAPIazione.

- Responsabile del servizio: per aggiungere un responsabile del servizio, scegli Responsabile del servizio dal dropbox Seleziona il tipo principale. Inserisci il nome del responsabile del AWS servizio. Utilizzare la seguente sintassi:
  - *service-id*.amazonaws.com

    Per esempio:

    ```
    pca-connector-ad.amazonaws.com
    ```

c. Per Principi selezionati, verifica che i principali specificati compaiano nell'elenco.

9. Scegli Next (Successivo).
10. Nel Passaggio 4: Revisione e creazione, rivedi i dettagli di configurazione per la condivisione delle risorse. Per modificare la configurazione per qualsiasi passaggio, scegli il link corrispondente al passaggio a cui desideri tornare e apporta le modifiche richieste.
11. Dopo aver esaminato la condivisione di risorse, scegli Crea condivisione di risorse.

    Il completamento dell'associazione tra la risorsa e il principale può richiedere alcuni minuti. Attendi il completamento di questo processo prima di provare a utilizzare la condivisione di risorse.
12. Puoi aggiungere e rimuovere risorse e principali o applicare tag personalizzati alla tua condivisione di risorse in qualsiasi momento. È possibile modificare l'autorizzazione gestita per i tipi di risorse inclusi nella condivisione delle risorse, per quei tipi che supportano più autorizzazioni gestite rispetto all'autorizzazione gestita predefinita. È possibile eliminare la condivisione di risorse quando non si desidera più condividere le risorse. Per ulteriori informazioni, consulta CondividiAWS le risorse di tua proprietà.

AWS CLI

Per creare una condivisione di risorse

Utilizzo dell'create-resource-sharecomando. Il comando seguente crea una condivisione di risorse condivisa con tutti i Account AWS membri dell'organizzazione. La condivisione contiene una configurazione di AWS License Manager licenza e concede le autorizzazioni gestite predefinite per quel tipo di risorsa.

> **Note**
>
> Se desideri utilizzare un'autorizzazione gestita dal cliente con un tipo di risorsa in questa condivisione di risorse, puoi utilizzare un'autorizzazione gestita dal cliente esistente o crearne una nuova. Prendi nota dell'ARNautorizzazione gestita dal cliente, quindi crea la condivisione di risorse. Per ulteriori informazioni, consulta Creazione di un'autorizzazione gestita dal cliente.

```
$ aws ram create-resource-share \
    --region us-east-1 \
    --name MyLicenseConfigShare \
    --permission-arns arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionLicenseConfiguration \
    --resource-arns arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-abc123 \
    --principals arn:aws:organizations::123456789012:organization/o-1234abcd
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
        "name": "MyLicenseConfigShare",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": true,
        "status": "ACTIVE",
        "creationTime": "2021-09-14T20:42:40.266000-07:00",
        "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00"
    }
}
```

Aggiornare una condivisione di risorse in AWS RAM

È possibile aggiornare una condivisione di risorse in qualsiasi AWS RAM momento nei seguenti modi:

- Puoi aggiungere principali, risorse o tag a una condivisione di risorse che hai creato.
- Per i tipi di risorse che supportano più autorizzazioni AWS gestite oltre a quelle predefinite, puoi scegliere quale autorizzazione gestita applicare alle risorse di ogni tipo.
- Quando un'autorizzazione gestita allegata alla condivisione di risorse ha una nuova versione predefinita, è possibile aggiornare l'autorizzazione gestita per utilizzare la nuova versione.
- È possibile revocare l'accesso alle risorse condivise rimuovendo i principali o le risorse da una condivisione di risorse. Se revochi l'accesso, i principali non avranno più accesso alle risorse condivise.

> **Note**
>
> I responsabili con cui condividi le risorse possono abbandonare la condivisione di risorse se la condivisione è vuota o contiene solo tipi di risorse che supportano l'abbandono di una condivisione di risorse. Se la condivisione di risorse contiene tipi di risorse che non supportano l'abbandono, viene visualizzato un messaggio per informare i responsabili della condivisione che devono contattare il proprietario della condivisione. In questo caso, in qualità di proprietario della condivisione di risorse, devi rimuovere i responsabili dalla condivisione di risorse. Per un elenco dei tipi di risorse che non supportano questa azione, consultaPrerequisiti per abbandonare una condivisione di risorse.

Console

Per aggiornare una condivisione di risorse

1. Vai alla pagina Condivisi da me: condivisioni di risorse nella AWS RAM console.
2. Poiché le condivisioni di AWS RAM risorse esistono in modo specifico Regioni AWS, scegli quella appropriata Regione AWS dall'elenco a discesa nell'angolo in alto a destra della console. Per visualizzare le condivisioni di risorse che contengono risorse globali, è necessario impostarle su Stati Uniti orientali (Virginia settentrionale), (). Regione AWS `us-east-1` Per ulteriori informazioni sulla condivisione di risorse globali, consultaCondivisione delle risorse regionali rispetto alle risorse globali.

3. Seleziona la condivisione di risorse, quindi scegli Modifica.
4. Nel passaggio 1: Specificate i dettagli della condivisione delle risorse, esaminate i dettagli della condivisione delle risorse e, se necessario, aggiornate uno dei seguenti elementi:

   a. (Facoltativo) Per modificare il nome della condivisione di risorse, modifica Nome.

   b. (Facoltativo) Per aggiungere una risorsa alla condivisione di risorse, in Risorse, scegli il tipo di risorsa, quindi seleziona la casella di controllo accanto alla risorsa per aggiungerla alla condivisione di risorse. Le risorse globali vengono visualizzate solo se imposti la regione su Stati Uniti orientali (Virginia settentrionale), (`us-east-1`) nel. AWS Management Console

   c. (Facoltativo) Per rimuovere una risorsa dalla condivisione di risorse, individua la risorsa in Risorse selezionate, quindi scegli la X accanto all'ID della risorsa.

   d. (Facoltativo) Per aggiungere un tag alla condivisione di risorse, in Tag, inserisci una chiave e un valore per il tag nelle caselle di testo vuote. Per aggiungere più di una coppia chiave-valore di tag, scegli Aggiungi nuovo tag. Puoi aggiungere fino a 50 tag.

   e. Per rimuovere un tag dalla condivisione di risorse, in Tag, individua il tag e scegli Rimuovi accanto ad esso.
5. Scegli Next (Successivo).
6. (Facoltativo) Nel Passaggio 2: Associa un'autorizzazione gestita a ciascun tipo di risorsa, puoi scegliere di associare un'autorizzazione gestita creata da AWS al tipo di risorsa, scegliere un'autorizzazione gestita dal cliente esistente oppure creare un'autorizzazione gestita dal cliente personalizzata. Per ulteriori informazioni, consulta Tipi di autorizzazioni gestite.

   Puoi anche scegliere Crea autorizzazione gestita dal cliente per creare un'autorizzazione gestita dal cliente che soddisfi i requisiti del tuo caso d'uso della condivisione. Per ulteriori informazioni, consulta Creazione di un'autorizzazione gestita dal cliente. Dopo aver completato il processo,

   scegli 
   quindi puoi selezionare la tua nuova autorizzazione gestita dal cliente dall'elenco a discesa Autorizzazioni gestite.

   Per visualizzare le azioni consentite dall'autorizzazione gestita, espandi Visualizza il modello di policy per questa autorizzazione gestita.

7. Se la versione dell'autorizzazione gestita attualmente assegnata alla condivisione di risorse non è la versione predefinita corrente, puoi eseguire l'aggiornamento alla versione predefinita scegliendo Aggiorna alla versione predefinita.

> **Note**
>
> Finché non salvi le modifiche alla condivisione di risorse dopo il passaggio finale, puoi annullare l'aggiornamento della versione scegliendo Ripristina alla versione precedente. Tuttavia, per le autorizzazioni AWS gestite, dopo aver salvato la condivisione di risorse, la modifica è definitiva e non è più possibile tornare alla versione precedente.

8. Scegli Next (Successivo).
9. Nel passaggio 3: scegli i principali a cui è consentito l'accesso, rivedi i principali selezionati e, se necessario, aggiorna uno dei seguenti elementi:

   a. (Facoltativo) Per modificare se la condivisione è abilitata con i responsabili interni o esterni all'organizzazione, scegli una delle seguenti opzioni:

      - Per condividere risorse Account AWS o singoli IAM ruoli o utenti esterni all'organizzazione, scegli Consenti la condivisione con responsabili esterni.
      - Per limitare la condivisione delle risorse ai soli responsabili della tua organizzazione in AWS Organizations, scegli Consenti la condivisione solo con i responsabili della tua organizzazione.

   b. Per i dirigenti, procedi come segue:

      - (Facoltativo) Per aggiungere un'organizzazione, un'unità organizzativa (OU) o un membro Account AWS all'interno dell'organizzazione, attiva Mostra struttura organizzativa per visualizzare una visualizzazione ad albero dell'organizzazione. Quindi seleziona la casella di controllo accanto a ciascun principale che desideri aggiungere.

> **Important**
>
> Quando condividi con un'organizzazione o un'unità organizzativa e tale ambito include l'account proprietario della condivisione di risorse, tutti i responsabili dell'account di condivisione ottengono automaticamente l'accesso alle risorse della condivisione. L'accesso concesso è definito dalle autorizzazioni

gestite associate alla condivisione. Questo perché la politica basata sulle risorse associata a ciascuna risorsa AWS RAM della condivisione utilizza. `"Principal": "*"` Per ulteriori informazioni, consulta Implicazioni dell'uso "Principal": "*" in una politica basata sulle risorse.
I responsabili degli altri account di consumo non hanno accesso immediato alle risorse della condivisione. Gli amministratori degli altri account devono prima allegare politiche di autorizzazione basate sull'identità ai principali appropriati. Tali politiche devono consentire `Allow` l'accesso alle singole risorse ARNs della condivisione di risorse. Le autorizzazioni contenute in tali politiche non possono superare quelle specificate nell'autorizzazione gestita associata alla condivisione di risorse.

> **Note**
>
> L'interruttore Visualizza la struttura organizzativa viene visualizzato solo se la condivisione con AWS Organizations è abilitata e se hai effettuato l'accesso come responsabile nell'account di gestione dell'organizzazione.
> Non puoi utilizzare questo metodo per specificare un IAM ruolo o un utente Account AWS esterno all'organizzazione. È invece necessario aggiungere questi principali inserendo i relativi identificatori, visualizzati nella casella di testo sotto l'interruttore Visualizza la struttura organizzativa. Vedi il prossimo bullet point.

- (Facoltativo) Per aggiungere un principale tramite il relativo identificatore, scegli il tipo principale dall'elenco a discesa, quindi inserisci l'ID o ARN il principale. Infine, scegli Aggiungi.

  Se selezioni una persona Account AWS, solo quell'account può accedere alla condivisione delle risorse. Puoi scegliere una delle seguenti opzioni.

  - Altro Account AWS (diverso dal proprietario della risorsa): rende la risorsa disponibile per l'altro account. L'amministratore di tale account deve completare il processo concedendo l'accesso alla risorsa condivisa utilizzando politiche di autorizzazione basate sull'identità a singoli ruoli e utenti. Tali autorizzazioni non possono superare quelle definite nelle autorizzazioni gestite allegate alla condivisione di risorse.

- Questo Account AWS (proprietario della risorsa): tutti i ruoli e gli utenti dell'account proprietario delle risorse ricevono automaticamente l'accesso definito dalle autorizzazioni gestite allegate alla condivisione delle risorse.
- L'aggiunta viene immediatamente visualizzata nell'elenco Principi selezionati.

  Puoi quindi aggiungere altri account o OUs la tua organizzazione ripetendo questo passaggio.
- (Facoltativo) Per rimuovere un principale, individualo in Responsabili selezionati, seleziona la relativa casella di controllo, quindi scegli Deseleziona.

10. Scegli Next (Successivo).
11. Nel passaggio 4: Rivedi e aggiorna, esamina i dettagli di configurazione per la condivisione delle risorse.
12. Per modificare la configurazione per qualsiasi passaggio, scegli il link corrispondente al passaggio a cui desideri tornare, quindi apporta le modifiche richieste.

    Se alcune autorizzazioni gestite utilizzano ancora versioni diverse da quella predefinita, hai un'altra opportunità per risolvere il problema scegliendo Aggiorna alla versione predefinita.
13. Scegli Aggiorna condivisione risorse quando hai finito di apportare le modifiche.

AWS CLI

Per aggiornare una condivisione di risorse

È possibile utilizzare i seguenti AWS CLI comandi per modificare una condivisione di risorse:

- Per rinominare una condivisione di risorse o modificare se sono consentiti i principali esterni, usa il comando update-resource-share. L'esempio seguente rinomina la condivisione di risorse specificata e la imposta in modo da consentire solo i principali membri della relativa organizzazione. È necessario utilizzare l'endpoint di servizio per la condivisione di risorse Regione AWS che contiene la condivisione di risorse.

```
$ aws ram update-resource-share \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
    --name "my-renamed-resource-share" \
    --no-allow-external-principals
{
```

```
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
        "name": "my-renamed-resource-share",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": false,
        "status": "ACTIVE",
        "creationTime": 1565295733.282,
        "lastUpdatedTime": 1565303080.023
    }
}
```

- Per aggiungere una risorsa a una condivisione di risorse, usa il comando associate-resource-share. L'esempio seguente aggiunge una sottorete alla condivisione di risorse specificata.

```
$ aws ram associate-resource-share \
    --region us-east-1 \
    --resource-arns arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
{
    "resourceShareAssociations": [
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
        "associatedEntity": "arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235",
        "associationType": "RESOURCE",
        "status": "ASSOCIATING",
        "external": false
    ]
}
```

- Per aggiungere o sostituire un'autorizzazione gestita per un tipo di risorsa in una condivisione di risorse, utilizzare i comandi list-permissions e associate-resource-share-permission. È possibile assegnare solo un'autorizzazione gestita per tipo di risorsa in una condivisione di risorse. Se si tenta di aggiungere un'autorizzazione gestita a un tipo di risorsa che dispone già di un'autorizzazione gestita, è necessario includere l'`--replace`opzione o il comando ha esito negativo e viene generato un errore.

  Il comando di esempio seguente elenca le ARNs autorizzazioni gestite disponibili per una sottorete Amazon Elastic Compute Cloud EC2 (Amazon), quindi utilizza una di queste ARNs

per sostituire l'autorizzazione AWS gestita attualmente assegnata per quel tipo di risorsa nella condivisione di risorse specificata.

```
$ aws ram list-permissions \
    --resource-type ec2:Subnet
{
    "permissions": [
        {
            "arn": "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionSubnet",
            "version": "1",
            "defaultVersion": true,
            "name": "AWSRAMDefaultPermissionSubnet",
            "resourceType": "ec2:Subnet",
            "creationTime": "2020-02-27T11:38:26.727000-08:00",
            "lastUpdatedTime": "2020-02-27T11:38:26.727000-08:00"
        }
    ]
}
$ aws ram associate-resource-share-permission \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
    --permission-arn arn:aws:ram::aws:permission/AWSRAMDefaultPermissionSubnet
{
    "returnValue": true
}
```

- Per rimuovere una risorsa da una condivisione di risorse, usa il comando disassociate-resource-share. L'esempio seguente rimuove la EC2 sottorete Amazon con la condivisione di risorse specificata ARN dalla condivisione di risorse specificata.

```
$ aws ram disassociate-resource-share \
    --region us-east-1 \
    --resource-arns arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
{
    "resourceShareAssociations": [
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
        "associatedEntity": "arn:aws:ec2:us-east-1:ubnet/
subnet-0250c25a1f4e15235",
```

```
        "associationType": "RESOURCE",
        "status": "DISASSOCIATING",
        "external": false
    ]
}
```

- Per modificare i tag allegati a una condivisione di risorse, usa i comandi tag-resource e untag-resource. L'esempio seguente aggiunge il tag `project=lima` alla condivisione di risorse specificata.

```
$ aws ram tag-resource \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
    --tags key=project,value=lima
```

L'esempio seguente rimuove il tag con una chiave di `project` dalla condivisione di risorse specificata.

```
$ aws ram untag-resource \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
    --tag-keys=project
```

I comandi di tagging non producono alcun risultato in caso di successo.

Visualizzazione delle risorse condivise inAWS RAM

Puoi visualizzare l'elenco delle singole risorse che hai condiviso, in tutte le condivisioni di risorse. L'elenco ti aiuta a determinare quali risorse stai attualmente condividendo, il numero di condivisioni di risorse in cui sono incluse e il numero di responsabili che vi hanno accesso.

Console

Per visualizzare le risorse che stai attualmente condividendo

1. Apri la pagina Condivise da me: risorse condivise nellaAWS RAM console.
2. Poiché le condivisioni diAWS RAM risorse esistono in particolareRegioni AWS, scegliere la più appropriataRegione AWS dall'elenco a discesa nell'angolo in alto a destra della console.

Per visualizzare le condivisioni di risorse globali, è necessario impostarle su Stati Uniti orientali (Virginia settentrionale), (`us-east-1`).Regione AWS Per ulteriori informazioni sulla condivisione di risorse globali, consultaCondivisione delle risorse regionali rispetto alle risorse globali.

3. Per ogni risorsa condivisa, sono disponibili le seguenti informazioni:

   - ID risorsa: l'ID della risorsa. Scegli l'ID di una risorsa per aprire una nuova scheda del browser per visualizzare la risorsa nella console di servizio nativa.
   - Il tipo di risorsa: il tipo di risorsa.
   - Data ultima condivisione: la data in cui la risorsa è stata condivisa l'ultima volta.
   - Condivisioni di risorse: il numero di condivisioni di risorse che includono la risorsa. Per visualizzare l'elenco delle condivisioni di risorse, scegli il numero.
   - Responsabili: il numero di dirigenti che possono accedere alla risorsa. Scegli il valore per visualizzare i principali.

AWS CLI

Per visualizzare le risorse che stai attualmente condividendo

È possibile utilizzare il comando list-resources con il parametro`--resource-owner` impostato`SELF` per visualizzare i dettagli delle risorse attualmente condivise.

L'esempio seguente mostra le risorse incluse nelle condivisioni di risorse inRegione AWS (`us-east-1`) per la chiamataAccount AWS. Per ottenere le risorse che condividi in una regione diversa, usa il`--region` *`<region-code>`* parametro.

```
$ aws ram list-resources \
    --region us-east-1 \
    --resource-owner SELF
{
    "resources": [
        {
            "arn": "arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-ecbd5574fd92cb0d312baea260e4cece",
            "type": "license-manager:LicenseConfiguration",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/818d71dd-7512-4f71-99c6-2ae57aa010bc",
            "creationTime": "2021-09-14T20:42:40.266000-07:00",
            "lastUpdatedTime": "2021-09-14T20:42:41.081000-07:00"
```

```
        },
        {
            "arn": "arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-ecbd5574fd92cb0d312baea260e4cece",
            "type": "license-manager:LicenseConfiguration",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-share/
a477f3b2-4001-4dcb-bd54-7c8d23b4f07d",
            "creationTime": "2021-07-22T11:48:11.104000-07:00",
            "lastUpdatedTime": "2021-07-22T11:48:11.971000-07:00"
        }
    ]
}
```

Visualizzazione dei dirigenti con cui condividi le risorse inAWS RAM

Puoi visualizzare i principali con cui condividi le risorse in tutte le condivisioni di risorse. Visualizzare questo elenco di principali consente di determinare chi ha accesso alle risorse condivise.

Console

Per visualizzare i responsabili con cui stai condividendo le risorse

1. Vai alla pagina Condivisi da me: Responsabili nellaAWS RAM console.
2. Poiché le condivisioni diAWS RAM risorse esistono in particolareRegioni AWS, scegliere la più appropriataRegione AWS dall'elenco in alto a destra della console. Per visualizzare le condivisioni di risorse che contengono risorse globali, è necessarioRegione AWS impostarle su Stati Uniti orientali (Virginia settentrionale), (`us-east-1`). Per ulteriori informazioni sulla condivisione di risorse globali, consultaCondivisione delle risorse regionali rispetto alle risorse globali.
3. Applica un filtro per trovare soggetti specifici. È possibile applicare più filtri per limitare la ricerca. Scegli la casella di testo per visualizzare un elenco a discesa dei campi degli attributi suggeriti. Dopo averne scelto uno, puoi scegliere dall'elenco dei valori disponibili per quel campo. Puoi aggiungere altri attributi o parole chiave fino a trovare la risorsa desiderata.
4. Per ogni committente dell'elenco, la console visualizza le seguenti informazioni:
   - ID principale: l'ID del committente. Scegli l'ID per aprire una nuova scheda del browser per visualizzare il principale nella sua console nativa.

- Condivisioni di risorse: il numero di condivisioni di risorse che hai condiviso con il committente specificato. Selezionare il numero per visualizzare l'elenco delle condivisioni di risorse.
- Risorse: il numero di risorse che hai condiviso con il preside. Selezionare il numero per visualizzare l'elenco delle risorse condivise.

AWS CLI

Per visualizzare i responsabili con cui stai condividendo le risorse

È possibile utilizzare il comando list-principals per ottenere un elenco dei responsabili a cui si fa riferimento nelle condivisioni di risorse create nella correnteRegione AWS per l'account chiamante.

L'esempio seguente elenca i committenti che hanno accesso alle condivisioni create nella regione predefinita per l'account chiamante. In questo esempio, i responsabili sono l'organizzazione dell'account chiamante e un'organizzazione separataAccount AWS, nell'ambito di due diverse condivisioni di risorse. È necessario utilizzare l'endpoint del servizio perRegione AWS ciò che contiene la condivisione di risorse.

```
$ aws ram list-principals \
    --region us-east-1 \
    --resource-owner SELF
{
    "principals": [
        {
            "id": "arn:aws:organizations::123456789012:organization/o-a1b2c3dr",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-share/
a477f3b2-4001-4dcb-bd54-7c8d23b4f07d",
            "creationTime": "2021-09-14T20:40:58.532000-07:00",
            "lastUpdatedTime": "2021-09-14T20:40:59.610000-07:00",
            "external": false
        },
        {
            "id": "111111111111",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/6405fa7c-0786-4e15-8c9f-8aec02802f18",
            "creationTime": "2021-09-15T15:00:31.601000-07:00",
            "lastUpdatedTime": "2021-09-15T15:14:13.618000-07:00",
            "external": true
        }
```

```
    ]
}
```

Eliminazione di una condivisione di risorse inAWS RAM

È possibile eliminare una condivisione delle risorse in qualsiasi momento. Quando si elimina una condivisione di risorse, tutti i principali associati alla condivisione di risorse perdono l'accesso alle risorse condivise. L'eliminazione di una condivisione di risorse non comporta l'eliminazione delle risorse condivise.

> **Per eliminare unaAWS risorsa**
>
> Se è necessario eliminare unaAWS risorsa inclusa in una condivisione di risorse,AWS si consiglia innanzitutto di assicurarsi di rimuovere la risorsa da qualsiasi condivisione di risorse che la include o di eliminare la condivisione di risorse.

La condivisione di risorse eliminata rimane visibile nellaAWS RAM console per un breve periodo dopo l'eliminazione, ma il suo stato cambia in`Deleted`.

Console

Come Come eliminare una condivisione delle risorse

1. Apri la pagina Condiviso da me: condivisioni di risorse nellaAWS RAM console.
2. Poiché le condivisioniAWS RAM delle risorse esistono specificatamenteRegioni AWS, scegliere quella appropriataRegione AWS dall'elenco a discesa nell'angolo superiore destro della console. Per visualizzare le condivisioni delle risorse che contengono risorse globali, è necessarioRegione AWS impostarle su Stati Uniti orientali (Virginia settentrionale), (`us-east-1`). Per ulteriori informazioni sulla condivisione delle risorse globali, consultaCondivisione delle risorse regionali rispetto alle risorse globali.
3. Seleziona la condivisione delle risorse che desideri eliminare.

> **Warning**
>
> Assicurarsi di selezionare la condivisione delle risorse corretta. Non è possibile, tuttavia, tuttavia, tuttavia, tuttavia, tuttavia, recuperare una condivisione delle risorse dopo averla eliminata.

4. Scegli Elimina, quindi nel messaggio di conferma scegli Elimina.
5. La condivisione di risorse eliminata scompare dopo due ore. Fino ad allora, rimarrà visibile nella console con uno stato eliminato.

AWS CLI

Come Come eliminare una condivisione delle risorse

È possibile utilizzare il delete-resource-sharecomando per eliminare una condivisione delle risorse che non serve più.

L'esempio seguente utilizza innanzitutto il get-resource-sharescomando per ottenere il nome della risorsa Amazon (ARN) della condivisione di risorse che desideri eliminare. Quindi viene utilizzata delete-resource-shareper eliminare la condivisione di risorse specificata.

```
$  aws ram get-resource-shares \
    --region us-east-1 \
    --resource-owner SELF
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425",
            "name": "MySubnetShare",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-10T15:38:54.449000-07:00",
            "lastUpdatedTime": "2021-09-10T15:38:54.449000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
$ aws ram delete-resource-share \
```

```
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425
{
    "returnValue": true
}
```

Accedi alle AWS risorse condivise con te

Con AWS Resource Access Manager (AWS RAM), puoi visualizzare le condivisioni di risorse a cui sei stato aggiunto, le risorse condivise a cui puoi accedere e quelle Account AWS che hanno condiviso risorse con te. Puoi anche lasciare una condivisione di risorse quando non hai più bisogno dell'accesso alle relative risorse condivise.

Indice

Accettazione e rifiuto degli inviti alla condivisione di risorse

Per accedere alle risorse condivise, il proprietario della condivisione di risorse deve aggiungerti come principale. Il proprietario può aggiungere uno dei seguenti elementi come principale alla condivisione di risorse.

- L'organizzazione a cui appartiene il tuo account
- Un'unità organizzativa (OU) che contiene il tuo account
- Il tuo account individuale
- Per i tipi di risorse supportati, il tuo ruolo o utente IAM specifico

Se vieni aggiunto alla condivisione di risorse tramite un membro di un'organizzazione e la condivisione all'interno dell'organizzazione è abilitata, avrai automaticamente accesso alle risorse condivise senza dover accettare un invito. Account AWS AWS Organizations I responsabili del

servizio ottengono inoltre l'accesso automatico alle risorse condivise senza accettare un invito. Se l'account tramite il quale si ottiene l'accesso viene successivamente rimosso dall'organizzazione, tutti i responsabili dell'account perderanno automaticamente l'accesso alle risorse a cui si accedeva tramite quella condivisione di risorse.

Se vieni aggiunto a una condivisione di risorse da una delle seguenti persone, riceverai un invito a partecipare alla condivisione di risorse:

- Un account esterno alla tua organizzazione in AWS Organizations
- Un account interno all'organizzazione con cui è possibile condividere non AWS Organizations è abilitato

Se ricevi un invito a partecipare a una condivisione di risorse, devi accettarlo per accedere alle relative risorse condivise. Se rifiuti l'invito, non puoi accedere alle risorse condivise.

Per i seguenti tipi di risorse hai sette giorni di tempo per accettare l'invito a partecipare alla condivisione per i seguenti tipi di risorse. Se non accetti l'invito prima della scadenza, l'invito viene automaticamente rifiutato.

> **Important**
>
> Per i tipi di risorse condivise non presenti nell'elenco seguente, hai 12 ore per accettare l'invito a partecipare alla condivisione di risorse. Dopo 12 ore, l'invito scade e l'utente principale incluso nella condivisione delle risorse viene dissociato. L'invito non può più essere accettato dagli utenti finali.

- Amazon Aurora — cluster DB
- Amazon EC2: prenotazioni di capacità e host dedicati
- AWS License Manager — Configurazioni delle licenze
- AWS Outposts — Tabelle di routing, avamposti e siti dei gateway locali
- Amazon Route 53 — Regole di inoltro
- Amazon VPC: indirizzi IPv4 di proprietà del cliente, elenchi di prefissi, sottoreti, target Traffic Mirror, gateway di transito, domini multicast con gateway di transito

Console

Per rispondere a un invito alla condivisione di risorse

1. Vai alla pagina Condivisi con me: condivisioni di risorse nella AWS RAM console.
2. Poiché le condivisioni di AWS RAM risorse esistono in modo specifico Regioni AWS, scegli quella appropriata Regione AWS dall'elenco a discesa nell'angolo in alto a destra della console. Per visualizzare le condivisioni di risorse che contengono risorse globali, è necessario impostarle su Stati Uniti orientali (Virginia settentrionale), (). Regione AWS `us-east-1` Per ulteriori informazioni sulla condivisione di risorse globali, consultaCondivisione delle risorse regionali rispetto alle risorse globali.
3. Controlla l'elenco delle condivisioni di risorse a cui sei stato aggiunto.

   La colonna Stato indica il tuo attuale stato di partecipazione alla condivisione di risorse. Lo `Pending` stato indica che sei stato aggiunto a una condivisione di risorse, ma non hai ancora accettato o rifiutato l'invito.
4. Per rispondere all'invito alla condivisione delle risorse, seleziona l'ID di condivisione delle risorse e scegli Accetta la condivisione delle risorse per accettare l'invito oppure Rifiuta la condivisione delle risorse per rifiutare l'invito. Se rifiuti l'invito, non avrai accesso alle risorse. Se accetti l'invito, avrai accesso alle risorse.

AWS CLI

Per rispondere a un invito alla condivisione di risorse

È possibile utilizzare i seguenti comandi per accettare o rifiutare gli inviti a una condivisione di risorse:

- get-resource-share-invitations
- accept-resource-share-invitation
- reject-resource-share-invitation

1. L'esempio seguente inizia utilizzando il get-resource-share-invitationscomando per recuperare un elenco di tutti gli inviti disponibili per l'utente. Account AWS Il AWS CLI `query` parametro consente di limitare l'output solo agli inviti impostati su. `status` `PENDING` Questo esempio mostra che un invito dall'account 1111 è attualmente `PENDING` per l'account corrente `123456789012` specificato. Regione AWS

```
$ aws ram get-resource-share-invitations \
    --region us-east-1 \
    --query 'resourceShareInvitations[?status==`PENDING`]'
{
    "resourceShareInvitations": [
        {
            "resourceShareInvitationArn": "arn:aws:ram:us-
east-1:111111111111:resource-share-invitation/3b3bc051-
fbf6-4336-8377-06c559dfee49",
            "resourceShareName": "Test TrngAcct Resource Share",
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/c4506c70-df75-4e6c-ac30-42ca03295a37",
            "senderAccountId": "111111111111",
            "receiverAccountId": "123456789012",
            "invitationTimestamp": "2021-09-21T08:56:24.977000-07:00",
            "status": "PENDING"
        }
    ]
}
```

2. Dopo aver trovato l'invito che desideri accettare, prendi nota dell'`resourceShareInvitationArn`output da utilizzare nel comando successivo per accettare l'invito.

```
$ aws ram accept-resource-share-invitation \
    --region us-east-1 \
    --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-
east-1:111111111111:resource-share-invitation/3b3bc051-
fbf6-4336-8377-06c559dfee49",
        "resourceShareName": "Test TrngAcct Resource Share",
        "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
        "senderAccountId": "111111111111",
        "receiverAccountId": "123456789012",
        "invitationTimestamp": "2021-09-21T09:18:24.545000-07:00",
        "status": "ACCEPTED"
    }
```

```
}
```

In caso di successo, nota che la risposta mostra che `status` è cambiato da `PENDING` a`ACCEPTED`.

Se invece desideri rifiutare l'invito, esegui il reject-resource-share-invitationcomando con gli stessi parametri.

```
$ aws ram reject-resource-share-invitation \
    --region us-east-1 \
    --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49",
        "resourceShareName": "Test TrngAcct Resource Share",
        "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
        "senderAccountId": "111111111111",
        "receiverAccountId": "123456789012",
        "invitationTimestamp": "2021-09-21T09:18:24.545000-07:00",
        "status": "REJECTED"
    }
}
```

Visualizzazione delle condivisioni di risorse condivise con te

Puoi visualizzare le condivisioni di risorse a cui hai accesso. Puoi vedere quali dirigenti condividono risorse con te e quali risorse condividono.

Console

Per visualizzare le condivisioni di risorse

1. Vai alla pagina Condiviso con me: condivisioni di risorse nellaAWS RAM console.
2. Poiché le condivisioni diAWS RAM risorse esistono in particolareRegioni AWS, scegliere la più appropriataRegione AWS dall'elenco a discesa nell'angolo in alto a destra della console. Per visualizzare le condivisioni di risorse che contengono risorse globali, è

necessarioRegione AWS impostarle su Stati Uniti orientali (Virginia settentrionale), (`us-east-1`). Per ulteriori informazioni sulla condivisione di risorse globali, consultaCondivisione delle risorse regionali rispetto alle risorse globali.

3. (Facoltativo) Applica un filtro per trovare condivisioni di risorse specifiche. È possibile applicare più filtri per limitare la ricerca. È possibile digitare una parola chiave, ad esempio parte del nome di una condivisione di risorse, per elencare solo le condivisioni di risorse che includono quel testo nel nome. Scegli la casella di testo per visualizzare un elenco a discesa dei campi degli attributi suggeriti. Dopo averne scelto uno, puoi scegliere dall'elenco dei valori disponibili per quel campo. Puoi aggiungere altri attributi o parole chiave fino a trovare la risorsa desiderata.
4. LaAWS RAM console visualizza le informazioni riportate di seguito.

   - Nome: il nome della condivisione di risorse.
   - ID: l'ID della condivisione di risorse. Scegliere l'ID per visualizzare la pagina dei dettagli della condivisione di risorse.
   - Proprietario: l'ID di chiAccount AWS ha creato la condivisione di risorse.
   - Stato: lo stato corrente della condivisione di risorse. I valori possibili includono:
     - `Active`— La condivisione di risorse è attiva e disponibile per l'utilizzo.
     - `Deleted`— La condivisione di risorse viene eliminata e non è più disponibile per l'utilizzo.
     - `Pending`— Un invito ad accettare la condivisione di risorse è in attesa di risposta.

AWS CLI

Per visualizzare le condivisioni di risorse

Utilizzate il get-resource-sharescomando con il`--resource-owner` parametro impostato su`OTHER-ACCOUNTS`.

L'esempio seguente mostra l'elenco delle condivisioni di risorse condivise nell'account specificatoRegione AWS con l'account chiamante da un altroAccount AWS.

```
$ aws ram get-resource-shares \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "resourceShares": [
```

```
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "name": "Prod Env Shared Licenses",
            "owningAccountId": "111111111111",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T08:50:41.308000-07:00",
            "featureSet": "STANDARD"
        },
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:222222222222:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
            "name": "Prod Env Shared Subnets",
            "owningAccountId": "222222222222",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-21T08:56:24.737000-07:00",
            "lastUpdatedTime": "2021-09-21T08:56:24.737000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
```


Visualizzazione delle risorse condivise con te

Puoi visualizzare le risorse condivise a cui puoi accedere. Puoi vedere quali responsabili hanno condiviso le risorse con te e quali condivisioni di risorse includono le risorse.

Console

Per visualizzare le risorse condivise con te

1. Vai alla pagina Condivise con me: risorse condivise nellaAWS RAM console.
2. Poiché le condivisioni diAWS RAM risorse esistono in particolareRegioni AWS, scegliere la più appropriataRegione AWS dall'elenco in alto a destra della console, scegliere la più appropriata dall'elenco in alto a destra della console. Per visualizzare le condivisioni di risorse che contengono risorse globali, è necessario impostarle su Stati UnitiRegione AWS`us-east-1` Per ulteriori

informazioni sulla condivisione di risorse globali, consultaCondivisione delle risorse regionali rispetto alle risorse globali.

3. Applicare un filtro per trovare risorse condivise specifiche. È possibile applicare più filtri per limitare la ricerca.
4. Sono disponibili le seguenti informazioni:

   - ID risorsa: l'ID della risorsa. Scegliere l'ID della risorsa per visualizzarlo nella relativa console di servizio.
   - Il tipo di risorsa: il tipo di risorsa.
   - Data ultima condivisione: la data in cui la risorsa è stata condivisa con te.
   - Condivisioni di risorse: il numero di condivisioni di risorse in cui è inclusa la risorsa. Scegli il valore per visualizzare le condivisioni di risorse.
   - ID proprietario: l'ID del committente proprietario della risorsa.

AWS CLI

Per visualizzare le risorse condivise con te

Puoi usare il comando list-resources per visualizzare le risorse condivise con te.

Il seguente comando di esempio visualizza i dettagli sulla risorsa accessibile tramite una condivisione di risorse in quella specificataRegione AWS da un'altraAccount AWS.

```
$ aws ram list-resources \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "resources": [
        {
            "arn": "arn:aws:license-manager:us-east-1:111111111111:license-
configuration:lic-36be0485f5ae379cc74cf8e9242ab143",
            "type": "license-manager:LicenseConfiguration",
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "status": "AVAILABLE",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T08:50:42.517000-07:00"
        }
    ]
```

```
}
```

Visualizza i dirigenti che condividono con te

Puoi visualizzare un elenco di tutti i principali che condividono risorse con l'utente. Puoi vedere le risorse e le condivisioni di risorse con l'utente.

Console

Per visualizzare i principali che condividono risorse con l'utente

1. Aprire la console AWS RAM all'indirizzo https://console.aws.amazon.com/ram.
2. Poiché le condivisioni diAWS RAM risorse esistono in particolareRegioni AWS, scegliere la più appropriataRegione AWS dall'elenco a discesa nell'angolo in alto a destra della console. Per visualizzare le condivisioni di risorse globali, è necessario impostarle su Stati Uniti orientali (Virginia settentrionale), (`us-east-1`).Regione AWS Per ulteriori informazioni sulla condivisione di risorse globali, consultaCondivisione delle risorse regionali rispetto alle risorse globali.
3. Nel riquadro di navigazione, scegliere Shared with me (Condivise con me), Principals (Principali).
4. (Facoltativo) È possibile applicare un filtro per trovare principali. È possibile applicare più filtri per limitare la ricerca.
5. La console mostra le seguenti informazioni:
   - ID principale: l'ID del committente che condivide con te.
   - Condivisioni di risorse: il numero di condivisioni di risorse a cui il committente ti ha aggiunto. Scegliere il numero per visualizzare l'elenco delle condivisioni di risorse.
   - Risorse: il numero di risorse che il preside condivide con te. Scegli il valore per visualizzare l'elenco delle risorse.

AWS CLI

Per visualizzare i principali che condividono risorse con l'utente

Puoi usare il comando list-principals per recuperare l'elenco dei responsabili che condividono risorse con il tuoAccount AWS.

Il seguente comando di esempio visualizza i dettagli relativi aAccount AWS chi ha condiviso una condivisione di risorse con l'account utilizzato per chiamare l'operazione nell'oggetto specificatoRegione AWS.

```
$  aws ram list-principals \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "principals": [
        {
            "id": "111111111111",
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T09:06:25.545000-07:00",
            "external": true
        }
    ]
}
```

Lasciare una condivisione di risorse

Se non hai più bisogno di accedere alle risorse condivise con te, puoi lasciare una condivisione di risorse in qualsiasi momento. Quando abbandoni una condivisione di risorse, perdi l'accesso alle risorse condivise.

Prerequisiti per abbandonare una condivisione di risorse

- Puoi lasciare una condivisione di risorse solo se è stata condivisa con te come individuo Account AWS e non nel contesto di un'organizzazione. Non puoi abbandonare una condivisione di risorse se sei stato aggiunto da un Account AWS membro dell'organizzazione e la condivisione con AWS Organizations è abilitata. L'accesso alle condivisioni di risorse all'interno di un'organizzazione è automatico.
- Per abbandonare una condivisione di risorse, verifica che la condivisione di risorse sia vuota o che contenga solo tipi di risorse che supportano l'abbandono di una condivisione.

  Di seguito sono riportati gli unici tipi di risorse che supportano l'abbandono di una condivisione di risorse.

Servizio	Tipo di risorsa
Amazon Aurora	`rds:Cluster`
Amazon EC2	`ec2:CapacityReservation` `ec2:DedicatedHost`
AWS License Manager	`license-manager:LicenseConfiguration`

AWS Outposts	`ec2:LocalGatewayRouteTable`
	`outposts:Outpost`
	`outposts:Site`

Amazon Route 53	`route53resolver:ResolverRule`

Amazon VPC	`ec2:CoipPool`
	`ec2:PrefixList`
	`ec2:Subnet`
	`ec2:TrafficMirrorTarget`
	`ec2:TransitGateway`
	`ec2:TransitGatewayMulticastDomain`

Come abbandonare una condivisione di risorse

Console

Per lasciare una condivisione di risorse

1. Vai alla pagina Condivisi con me: condivisioni di risorse nella AWS RAM console.

2. Poiché le condivisioni di AWS RAM risorse esistono in modo specificoRegioni AWS, scegli quella appropriata Regione AWS dall'elenco a discesa nell'angolo in alto a destra della console. Per visualizzare le condivisioni di risorse che contengono risorse globali, è necessario impostarle su Stati Uniti orientali (Virginia settentrionale), (). Regione AWS `us-east-1` Per ulteriori informazioni sulla condivisione di risorse globali, consultaCondivisione delle risorse regionali rispetto alle risorse globali.
3. Seleziona la condivisione di risorse che desideri abbandonare.
4. Scegli Lascia la condivisione delle risorse e nella finestra di dialogo di conferma scegli Abbandona.

AWS CLI

Per lasciare una condivisione di risorse

È possibile utilizzare il disassociate-resource-sharecomando per lasciare una condivisione di risorse.

I seguenti comandi di esempio fanno sì Account AWS che chi chiama il comando perda l'accesso alle risorse condivise dalla condivisione di risorse specificata dall'ARN. È necessario indirizzare la richiesta all'endpoint del servizio Regione AWS che contiene la condivisione di risorse che si desidera abbandonare.

1. Innanzitutto, recupera l'elenco delle condivisioni di risorse per recuperare l'ARN della condivisione di risorse che desideri lasciare.

```
$ aws ram get-resource-shares \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "name": "Prod Environment Shared Licenses",
            "owningAccountId": "111111111111",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T08:50:41.308000-07:00",
            "featureSet": "STANDARD"
```

```
        }
    ]
}
```

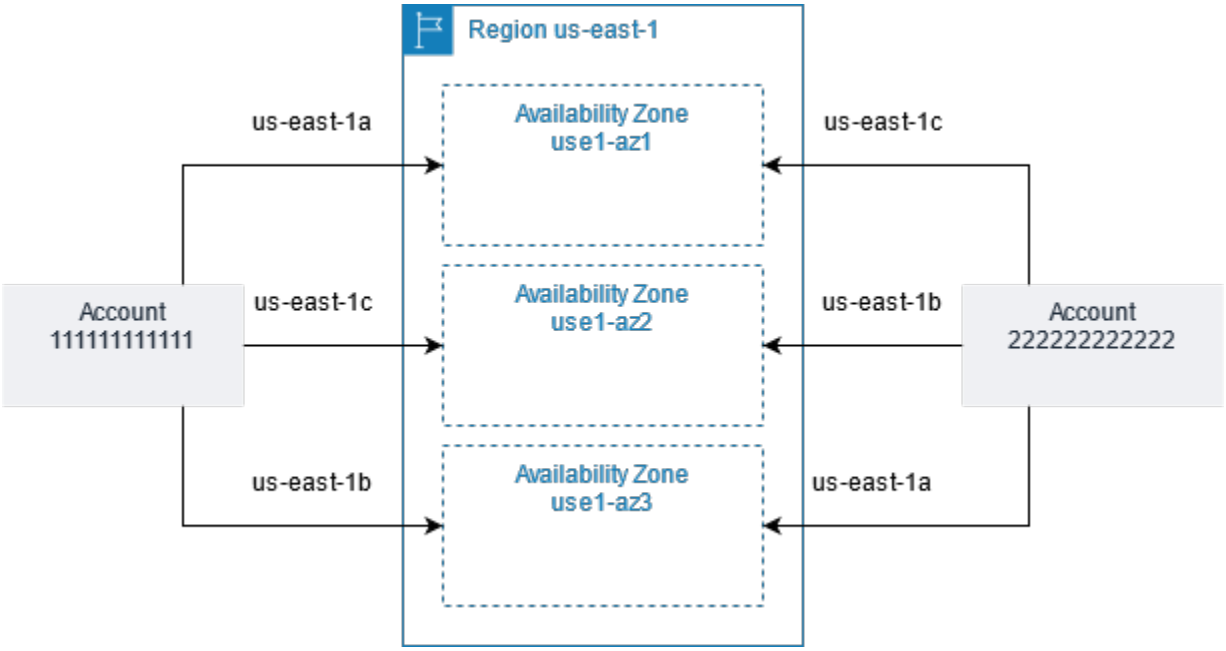
2. Quindi, puoi eseguire il comando per lasciare quella condivisione di risorse. Tieni presente che devi anche specificare l'ID del tuo account`123456789012`, come principale da dissociare dalla condivisione di risorse specificata, che è condivisa per account`111111111111`.

```
$ aws ram disassociate-resource-share \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e \
    --principals 123456789012
                        {
    "resourceShareAssociations": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "associatedEntity": "123456789012",
            "associationType": "PRINCIPAL",
            "status": "DISASSOCIATING",
            "external": false
        }
    ]
}
```

ID delle zone di disponibilità perAWS le tue risorse

AWSassocia le zone di disponibilità fisiche in modo casuale ai nomi delle zone di disponibilità per ciascunaAccount AWS. Questo approccio consente di distribuire le risorse tra le zone di disponibilità in unaRegione AWS, anziché concentrare le risorse nella zona di disponibilità «a» per ciascuna regione. Di conseguenza, la zona`us-east-1a` di disponibilità del tuoAWS account potrebbe non rappresentare la stessa posizione fisica`us-east-1a` di un altroAWS account. Per ulteriori informazioni, consulta Regioni e zone di disponibilità nella Guida per l'utente di Amazon EC2.

La figura seguente mostra come gli ID AZ siano gli stessi per ogni account anche se i nomi delle zone di disponibilità possono essere mappati in modo diverso per ogni account.



Per alcune risorse, è necessario identificare non solo la zona di disponibilitàRegione AWS, ma anche la zona di disponibilità. Ad esempio, una sottorete Amazon VPC. All'interno di un singolo account, la mappatura di una zona di disponibilità a un nome specifico non è importante. Tuttavia, quando siAWS RAM condivide una risorsa del genere con altriAccount AWS, la mappatura è importante. Questa mappatura casuale complica la capacità dell'account che accede alla risorsa condivisa di sapere a quale zona di disponibilità fare riferimento. A tale scopo, tali risorse consentono anche di identificare l'ubicazione effettiva delle risorse rispetto ai propri account utilizzando l'ID AZ. Un ID AZ è univoco ed è lo stesso identificatore di una zona di disponibilità per tutta la zona di disponibilitàAccount AWS. Ad esempio,`use1-az1` è un ID della zona di disponibilità nella`us-east-1` Regione e rappresenta la stessa posizione fisica in ogniAWS account.

È possibile utilizzare gli ID AZ per stabilire la posizione delle risorse in un account rispetto alle risorse in un altro account. Ad esempio, se condividi una sottorete nella zona di disponibilità con l'ID AZ `use1-az2` con un altro account, questa sottorete è disponibile per tale account nella zona di disponibilità il cui ID AZ è anche `use1-az2`. L'ID AZ per ogni sottorete è visualizzato nella console Amazon VPC e può essere interrogato utilizzando ilAWS CLI.

Console

Per visualizzare gli ID AZ per le zone di disponibilità nell'account

1. Vai alla pagina della AWS RAMconsole nellaAWS RAM console.
2. Puoi visualizzare gli ID AZ correnti nellaRegione AWS sezione Il tuo ID AZ.

AWS CLI

Per visualizzare gli ID AZ per le zone di disponibilità nell'account

Il seguente comando di esempio mostra gli ID AZ per le zone di disponibilità nella regione us-west-2 e come vengono mappati per la chiamataAccount AWS.

```
$ aws ec2 describe-availability-zones \
    --region us-west-2
{
    "AvailabilityZones": [
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2a",
            "ZoneId": "usw2-az2",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2b",
            "ZoneId": "usw2-az1",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2c",
            "ZoneId": "usw2-az3",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        },
```

```
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2d",
            "ZoneId": "usw2-az4",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        }
    ]
}
```

Risorse condivisibili AWS

Con AWS Resource Access Manager (AWS RAM), puoi condividere risorse create e gestite da altri Servizi AWS. È possibile condividere risorse con singoli utenti Account AWS. È inoltre possibile condividere risorse con gli account di un'organizzazione o delle unità organizzative (OUs) in AWS Organizations. Alcuni tipi di risorse supportati consentono inoltre di condividere risorse con singoli AWS Identity and Access Management (IAM) ruoli e utenti.

Nelle sezioni seguenti sono elencati i tipi di risorse, raggruppati per Servizio AWS, che è possibile condividere utilizzando AWS RAM. Le colonne delle tabelle specificano le funzionalità supportate da ciascun tipo di risorsa:

Può condividere con IAM utenti e ruoli	 puoi condividere risorse di questo tipo con singoli AWS Identity and Access Management (IAM) ruoli e utenti, oltre agli account.	Sì,
	 puoi condividere risorse di questo tipo solo con account.	No,
Può condividere con account esterni alla propria organizzazione	 puoi condividere risorse di questo tipo solo con singoli account, interni o esterni all'organizzazione. Per ulteriori informazioni, consulta Considerazioni.	Sì,
	 puoi condividere risorse di questo tipo solo con account membri della stessa organizzazione.	No,

Può utilizzare le autorizzazioni gestite dal cliente	Tutti i tipi di risorse supportati dal AWS RAM supporto supportano le autorizzazioni AWS gestite, ma un Sì in questa colonna significa che le autorizzazioni gestite dal cliente sono supportate anche per questo tipo di risorsa.	Sì, le risorse di questo tipo supportano l'uso di autorizzazioni gestite dal cliente. No, le risorse di questo tipo non supportano l'uso di autorizzazioni gestite dal cliente.
Può condividere con i responsabili del servizio		Sì, puoi condividere risorse di questo tipo con Servizi AWS. No, non puoi condividere risorse di questo tipo con Servizi AWS.

Amazon API Gateway

Puoi condividere le seguenti risorse Amazon API Gateway utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Nome dominio `apigateway:Domainnames`	Crea e gestisci i nomi di dominio centralmente e condividili con altri Account AWS o con la tua organizzazione. Ciò consente a più account di richiamare i tuoi nomi di dominio mappati come privati. APIs Per ulteriori informazioni, consulta la sezione Nomi di dominio personalizzati per uso privato APIs in API Gateway nella Amazon API Gateway Developer Guide.	N	S Può condividere con chiunque Account AWS.	N	No

AWS App Mesh

È possibile condividere le seguenti AWS App Mesh risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Mesh `appmesh:Mesh`	Crea e gestisci una rete mesh centralmente e condividila con altri Account AWS o con la tua organizzazione. Una rete condivisa consente alle risorse create da Account AWS persone diverse di comunicare tra loro nella stessa mesh. Per ulteriori informazioni, consultate Lavorare con le mesh condivise nella Guida per l'AWS App Mesh utente.	 S	 S Può condividere con chiunque Account AWS.	 N	 No

AWS AppSync GraphQL API

È possibile condividere le seguenti API risorse AWS AppSync GraphQL utilizzando. AWS RAM

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
GraphyQL API `appsync:APIs`	Gestisci AWS AppSync GraphQL APIs centralmente e condividili con altri Account AWS o con la tua organizzazione. Ciò consente la condivisione di più account AWS AppSync APIs come parte della creazione di un sistema AWS AppSync Merged unificato API che può accedere ai dati di più sottoschemi APIs su diversi account nella stessa regione. Per ulteriori informazioni, consulta Merged APIs nella Developer Guide. AWS AppSync	 S	 S Può condividere con chiunque Account AWS.	 S	 No

Amazon Aurora

Puoi condividere le seguenti risorse Amazon Aurora utilizzando. AWS RAM

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Cluster database `rds:Cluster`	Crea e gestisci un cluster DB centralmente e condividilo con altri Account AWS o con la tua organizzazione. Ciò consente di Account AWS clonare più volte un cluster DB condiviso e gestito centralmente. Per ulteriori informazioni, consulta la sezione Clonazione tra account AWS RAM e Amazon Aurora nella Guida per l'utente di Amazon Aurora.	N	S Può condividere con chiunque. Account AWS	N	No

AWS Backup

È possibile condividere le seguenti AWS Backup risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
BackupVault `backup:BackupVault`	Crea e gestisci casseforti logicamente isolati centralmente e condividili con altri o con la tua organizzazione. Account AWS Questa opzione consente a più account di accedere e ripristinare i backup dai vault. Per ulteriori informazioni, consulta Panoramica dei vault con intercapedine logiche nella Guida per gli sviluppatori.AWS Backup	S	S Può condividere con chiunque. Account AWS	S	No

Amazon Bedrock

Puoi condividere le seguenti risorse Amazon Bedrock utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Modello personalizzato `bedrock:CustomModel`	Crea e gestisci un modello personalizzato centralmente e condividilo con altri Account AWS o con la tua organizzazione. Ciò consente a più account di utilizzare lo stesso modello personalizzato per applicazioni di intelligenza artificiale generativa. Per ulteriori informazioni, consulta Condividere un modello per un altro account nella Amazon Bedrock User Guide.	 S	 N Può condividere solo con Account AWS la propria organizzazione.	 S	 No

AWS Billing Visualizza servizio

È possibile condividere le seguenti risorse di AWS Billing View Service utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Visualizzazione di fatturazione `billing:billingview`	Crea e gestisci visualizzazioni di fatturazione personalizzate centralmente e condividile con altri Account AWS o con la tua organizzazione. Ciò consente ai proprietari di applicazioni e unità aziendali di accedere alla AWS spesa a livello di unità aziendale da un account membro. Per ulteriori informazioni, consulta Controllare l'accesso ai dati di gestione dei costi con Billing View nella Guida per l'AWS Cost Management utente.	N	N Può condividere solo con Account AWS la propria organizzazione.	S	No

AWS Private Certificate Authority

È possibile condividere le seguenti CA privata AWS risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Autorità di certificazione privata (CA) `acm-pca:CertificateAuthority`	Crea e gestisci autorità di certificazione private (CAs) per l'infrastruttura a chiave pubblica interna della tua organizzazione (PKI) e condividile CAs con altri Account AWS o con la tua organizzazione. Ciò consente AWS Certificate Manager agli utenti di altri account di emettere certificati X.509 firmati dalla CA condivisa. Per ulteriori informazioni, consulta Controllare l'accesso a una CA privata nella Guida per l'AWS Private Certificate Authority utente.	 S	 S Può condividere con chiunque Account AWS.	 N	 Sì

Amazon DataZone

Puoi condividere le seguenti DataZone risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
DataZone Dominio `datazone:Domain`	Crea e gestisci i domini centralmente e condividili con altri Account AWS o con la tua organizzazione. Ciò consente a più account di creare DataZone domini Amazon. Per ulteriori informazioni, consulta What is Amazon DataZone nella Amazon DataZone User Guide.	N	S Può condividere con chiunque Account AWS.	N	No

AWS CloudHSM

È possibile condividere le seguenti AWS CloudHSM risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
AWS CloudHSM Backup `cloudhsm:Backup`	Gestisci i AWS CloudHSM backup centralmente e condividili con altri Account AWS o con la tua organizzazione. Ciò consente a più Account AWS utenti di visualizzare le informazioni sul Backup e utilizzarle per ripristinare un AWS CloudHSM cluster. Per ulteriori informazioni, consulta la sezione Gestione dei AWS CloudHSM backup nella Guida per l'AWS CloudHSM utente.	S	S	S	No

AWS CodeBuild

È possibile condividere le seguenti AWS CodeBuild risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Progetto `codebuild:Project`	Crea un progetto e usalo per eseguire build. Condividi il progetto con altri Account AWS o con la tua organizzazione. Ciò consente a più Account AWS utenti di visualizzare le informazioni su un progetto e analizzarne le build. Per ulteriori informazioni, consulta Lavorare con progetti condivisi nella Guida per l' AWS CodeBuild utente.	 S	 S Può condividere con chiunque Account AWS.	 S	 No
Gruppo di report `codebuild:ReportGroup`	Crea un gruppo di report e usalo per creare report quando crei un progetto. Condividi il gruppo di report con altri Account AWS o con la tua organizzazione. Ciò consente a più Account	 S	 S Può condividere con chiunque Account AWS.	 S	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	AWS utenti di visualizzare il gruppo di report e i relativi report, nonché i risultati del test case per ogni rapporto. Un report può essere visualizzato per 30 giorni dopo la creazione, quindi scade e non è più disponibile per la visualizzazione. Per ulteriori informazioni, consulta Lavorare con progetti condivisi nella Guida per l'AWS CodeBuild utente.				

Amazon EC2

Puoi condividere le seguenti EC2 risorse Amazon utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Prenotazioni della capacità `ec2:CapacityReservation`	Crea e gestisci le prenotazioni di capacità centralmente e condividi la capacità riservata con altri Account AWS o con la tua organizzazione. Ciò consente a più istanze Amazon di Account AWS lanciare le proprie EC2 istanze Amazon in una capacità riservata gestita centralmente. Per ulteriori informazioni, consulta Lavorare con le prenotazioni di capacità condivise nella Amazon EC2 User Guide. **Important** Se non soddisfi tutti i prerequisiti per condividere una prenotazi	 N	 S Può condividere con chiunque. Account AWS	 N	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	one di capacità, l'operazione di condivisione potrebbe fallire. Se ciò accade e un utente tenta di avviare un'EC2istanza Amazon con quella prenotazione di capacità, viene avviata come istanza on-demand che può generare costi più elevati. Ti consigliamo di verificare di poter accedere alla prenotazione di capacità condivisa tentando di visualizzarla nella EC2 console Amazon.				

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	Puoi anche monitorare e eventuali condivisioni di risorse non riuscite in modo da intraprendere azioni correttive prima che gli utenti avviino le istanze in modo da aumentare i costi. Per ulteriori informazioni, consulta Esempio: avvisi in caso di errori di condivisione delle risorse.				

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Host dedicati `ec2:DedicatedHost`	Alloca e gestisci gli host EC2 dedicati Amazon centralmente e condividi la capacità dell'istanza dell'host con altri Account AWS o con la tua organizzazione. Ciò consente a più istanze Amazon di Account AWS lanciare le proprie EC2 istanze Amazon su host dedicati gestiti centralmente. Per ulteriori informazioni, consulta Lavorare con host dedicati condivisi nella Amazon EC2 User Guide.	 N	 S Può condividere con chiunque Account AWS.	 N	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Gruppi di collocamento `ec2:PlacementGroup`	Condividi i gruppi di collocamento di cui sei proprietario all'interno e all'esterno dell'organizzazione. Account AWS Puoi avviare EC2 istanze Amazon da qualsiasi account con cui condividi le istanze in un gruppo di collocamento condiviso. Per ulteriori informazioni, consulta Condividi un gruppo di collocamento nella Amazon EC2 User Guide.	 S	 S Può condividere con chiunque Account AWS.	 N	 No

EC2Image Builder

È possibile condividere le seguenti risorse di EC2 Image Builder utilizzando. AWS RAM

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Componenti `imagebuilder:Component`	Crea e gestisci i componenti centralmente e condividili con altri Account AWS o con la tua organizzazione. Definisci chi può utilizzare componenti di compilazione e test predefiniti nelle proprie ricette di immagini. Per ulteriori informazioni, consulta Share EC2 Image Builder resources nella Guida per l'utente di Image EC2 Builder.	 S	 S Può condividere con chiunque. Account AWS	 S	 No
Ricette container `imagebuilder:ContainerRecipe`	Crea e gestisci le tue ricette in contenitore centralmente e condividile con altri Account AWS o con la tua organizzazione. Ciò consente di gestire chi può utilizzare documenti predefiniti	 S	 S Può condividere con chiunque. Account AWS	 S	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	per duplicare le build di immagini dei contenitori. Per ulteriori informazioni, consulta Share EC2 Image Builder resources nella Guida per l'utente di Image EC2 Builder.				
Immagini `imagebuilder:Image`	Crea e gestisci le tue immagini dorate centralmente e condividile con altri Account AWS o con la tua organizzazione. Gestisci chi può utilizzare le immagini create con EC2 Image Builder in tutta l'organizzazione. Per ulteriori informazioni, consulta Share EC2 Image Builder resources nella Guida per l'utente di Image EC2 Builder.	 S	 S Può condividere con chiunque. Account AWS	 S	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Ricette immagine `imagebuilder:ImageRecipe`	Crea e gestisci le tue ricette di immagini centralmente e condividile con altri Account AWS o con la tua organizzazione. Ciò consente di gestire chi può utilizzare documenti predefiniti per duplicare le build. AMI Per ulteriori informazioni, consulta Share EC2 Image Builder resources nella Guida per l'utente di Image EC2 Builder.	 S	 S Può condividere con chiunque. Account AWS	 S	 No

AWS End User Messaging SMS

È possibile condividere la seguente AWS End User Messaging SMS risorsa utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
OptOutList `sms-voice:opt-out-list`	Creane uno OptOutList e condividilo con altri membri Account AWS della tua organizzazione. Puoi condividerli OptOutList in modo che le altre applicazioni possano disattivare i numeri di telefono dell'utente da diversi numeri di telefono Account AWS oppure possano controllare lo stato del numero di telefono dell'utente. Per ulteriori informazioni, consulta Lavorare con risorse condivise nella Guida AWS End User Messaging SMS per l'utente.	N	S Può condividere con chiunque Account AWS.	S	No
PhoneNumber `sms-voice:phone-number`	Crea e gestisci numeri di telefono per condividerli con altri Account AWS o	N	S	S	Sì

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	con la tua organizzazione. Ciò consente l' Account AWS invio di più messaggi utilizzando il numero di telefono condiviso. Per ulteriori informazioni, consulta Lavorare con risorse condivise nella Guida AWS End User Messaging SMS per l'utente.		Può condividere con chiunque Account AWS.		
Pool `sms-voice:pool`	Crea e gestisci pool per condividerli con altri Account AWS o con la tua organizzazione. Ciò consente l' Account AWS invio di più messaggi utilizzando il pool condiviso. Per ulteriori informazioni, consulta Lavorare con risorse condivise nella Guida AWS End User Messaging SMS per l'utente.	 N	 S Può condividere con chiunque Account AWS.	 S	 Sì

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
SenderId `sms-voice:sender-id`	Crea e gestisci SenderId e condividili con altri Account AWS o con la tua organizzazione. Ciò consente l' Account AWS invio di più messaggi utilizzando quelli condivisi SenderId. Per ulteriori informazioni, consulta Lavorare con risorse condivise nella Guida AWS End User Messaging SMS per l'utente.	N	S Può condividere con chiunque Account AWS.	S	Sì

Amazon FSx per Open ZFS

Puoi condividere le seguenti ZFS risorse di Amazon FSx for Open utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Volume FSx `fsx:Volume`	Crea e gestisci FSx ZFS volumi aperti in modo centralizzato e condividili con altri Account AWS o con la tua organizzazione. Ciò consente a più account di eseguire la replica dei dati utilizzando OpenZfs istantanee in volumi condivisi tramite FSx APIs `CreateVolume` o. `CopySnapshotAndUpdateVolume` Per ulteriori informazioni, consulta la replica dei dati su richiesta nella Amazon FSx for Open ZFS User Guide.	S	S Può condividere con chiunque. Account AWS	S	No

AWS Glue

È possibile condividere le seguenti AWS Glue risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Cataloghi di dati `glue:Catalog`	Gestisci un catalogo di dati centralizzato e condividi i metadati su database e tabelle con la Account AWS nostra organizzazione. Ciò consente agli utenti di eseguire query sui dati su più account. Per ulteriori informazioni, consulta Condivisione delle tabelle e dei database del catalogo dati tra AWS account nella Guida per gli AWS Lake Formation sviluppatori.	N	S Può condividere con chiunque Account AWS.	N	No
Database `glue:Database`	Crea e gestisci database di cataloghi di dati in modo centralizzato e condividili con Account AWS la tua organizzazione. I database sono raccolte di tabelle di cataloghi di	N	S Può condividere con chiunque	N	No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	dati. Ciò consente agli utenti di eseguire query ed estrarre, trasformare e caricare (ETL) lavori che possono unire e interrogare dati su più account. Per ulteriori informazioni, consulta Condivisione delle tabelle e dei database del catalogo dati tra AWS account nella Guida per gli AWS Lake Formation sviluppatori.		Account AWS.		

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Tabelle `glue:Table`	Crea e gestisci le tabelle del catalogo dati in modo centralizzato e condividile con Account AWS la tua organizzazione. Le tabelle del catalogo dati contengono metadati sulle tabelle di dati in Amazon S3JDBC, sorgenti di dati, Amazon Redshift, sorgenti di streaming e altri archivi di dati. Ciò consente agli utenti di eseguire query e ETL lavori in grado di unire e interrogare dati su più account. Per ulteriori informazioni, consulta Condivisione delle tabelle e dei database del catalogo dati tra AWS account nella Guida per gli AWS Lake Formation sviluppatori.	 N	 S Può condividere con chiunque Account AWS.	 N	 No

AWS License Manager

È possibile condividere le seguenti AWS License Manager risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Configurazioni di licenza `license-manager:LicenseConfiguration`	Crea e gestisci le configurazioni delle licenze in modo centralizzato e condividile con altri Account AWS o con la tua organizzazione. Ciò consente di applicare regole di licenza gestite centralmente e basate sui termini dei contratti aziendali su più livelli. Account AWS Per ulteriori informazioni, vedere Configurazioni delle licenze in License Manager nella Guida per l'utente di License Manager.	 N	 S Può condividere con chiunque Account AWS.	 N	 No

Marketplace AWS

È possibile condividere le seguenti Marketplace AWS risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Entità del catalogo Marketplace `aws-marketplace:Entity`	Crea, gestisci e condividi entità all'interno Account AWS o all'interno della tua organizzazione in Marketplace AWS. Per ulteriori informazioni, consulta Condivisione delle risorse AWS RAM nella Guida AWS Marketplace Catalog API di riferimento.	 S	 S Può condividere con chiunque Account AWS.	 N	 No

AWS Migration Hub Refactor Spaces

È possibile condividere le seguenti AWS Migration Hub Refactor Spaces risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Ambiente Refactor Spaces `refactor-spaces:Environment`	Crea un ambiente Refactor Spaces e usalo per contenere le tue applicazioni Refactor Spaces. Condividi l'ambiente con altri Account AWS o tutti gli account della tua organizzazione. Ciò consente a più Account AWS utenti di visualizzare le informazioni sull'ambiente e sulle applicazioni in esso contenute. Per ulteriori informazioni, consulta Condivisione degli ambienti Refactor Spaces AWS RAM nella Guida per l'AWS Migration Hub Refactor Spaces utente.	 S	 S Può condividere con chiunque Account AWS.	 S	 No

AWS Network Firewall

È possibile condividere le seguenti AWS Network Firewall risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Policy firewall `network-firewall:FirewallPolicy`	Crea e gestisci le politiche firewall in modo centralizzato e condividile con altri Account AWS o con la tua organizzazione. Ciò consente a più account di un'organizzazione di condividere un insieme comune di comportamenti di monitoraggio, protezione e filtraggio della rete. Per ulteriori informazioni, consulta Condivisione delle politiche e dei gruppi di regole del firewall nella Guida per gli AWS Network Firewall sviluppatori.	 S	 S Può condividere con chiunque Account AWS.	 N	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio

Gruppi di regole
 	
`network-firewall:StatefulRuleGroup`
 	
`network-firewall:StatelessRuleGroup`
	Crea e gestisci centralmente gruppi di regole stateless e stateless e condividili con altri Account AWS o con la tua organizzazione. Ciò consente a più account di un'organizzazione di AWS Organizations condividere una serie di criteri per l'ispezione e la gestione del traffico di rete. Per ulteriori informazioni, consulta Condivisione delle politiche e dei gruppi di regole del firewall nella Guida per gli AWS Network Firewall sviluppatori.	 S	 S
			
			Può condividere con chiunque Account AWS.
				 N	 No

AWS Outposts

È possibile condividere le seguenti AWS Outposts risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Outposts `outposts:Outpost`	Crea e gestisci Outposts centralmente e condividili con altri membri della tua Account AWS organizzazione. Ciò consente a più account di creare sottoreti e EBS volumi sui tuoi Outposts condivisi e gestiti centralmente. Per ulteriori informazioni, consulta Lavorare con le risorse AWS Outposts condivise nella Guida per l'AWS Outposts utente.	 N	 N Può condividere solo con Account AWS la propria organizzazione.	 S	 No
Tabella di routing del gateway locale `ec2:LocalGatewayRouteTable`	Crea e gestisci centralmente VPC le associazioni verso un gateway locale e condividile con altri Account AWS membri dell'organizzazione. Ciò consente a più account	 N	 N Può condividere solo Account AWS con	 N	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	di creare VPC associazioni a un gateway locale e visualizzare la tabella di routing e la configurazione dell'interfaccia virtuale. Per ulteriori informazioni, consulta le risorse di Shareable Outpost nella Guida per l'AWS Outposts utente.		la propria organizzazione.		

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Siti `outposts:Site`	Crea e gestisci siti Outpost e condividili con altri membri Account AWS dell'organizzazione. Ciò consente a più account di creare e gestire Outposts sul sito condiviso e supporta il controllo suddiviso tra le risorse Outpost e il sito. Per ulteriori informazioni, consulta Lavorare con le risorse AWS Outposts condivise nella Guida per l'AWS Outposts utente.	 N	 S Può condividere con chiunque Account AWS.	 N	 No

Amazon S3 su Outposts

Puoi condividere la seguente risorsa Amazon S3 on Outposts utilizzando. AWS RAM

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
S3 su Outpost `s3-outposts:Outpost`	Crea e gestisci bucket, access point ed endpoint Amazon S3 su Outpost. Ciò consente a più account di creare e gestire Outposts sul sito condiviso e supporta il controllo suddiviso tra le risorse Outpost e il sito. Per ulteriori informazioni, consulta Lavorare con le risorse AWS Outposts condivise nella Guida per l'AWS Outposts utente.	N	N Può condividere solo con Account AWS la propria organizzazione.	S	No

Esploratore di risorse AWS

È possibile condividere le seguenti Esploratore di risorse AWS risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Visualizzazioni `resource-explorer-2:View`	Crea e configura le visualizzazioni di Resource Explorer Account AWS in modo centralizzato e condividile con altri membri dell'organizzazione. Ciò consente ai ruoli e agli utenti Account AWS di cercare e scoprire più risorse accessibili tramite la visualizzazione. Per ulteriori informazioni, consulta Sharing Resource Explorer views nella Guida Esploratore di risorse AWS per l'utente.	N	N Può condividere solo Account AWS con la propria organizzazione.	N	No

AWS Resource Groups

È possibile condividere le seguenti AWS Resource Groups risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Gruppi di risorse `resource-groups:Group`	Crea e gestisci centralmente un gruppo di risorse host e condividilo con altri membri Account AWS dell'organizzazione. Ciò consente la Account AWS condivisione multipla di un gruppo di host EC2 dedicati Amazon creati utilizzando AWS License Manager. Per ulteriori informazioni, consulta Host resource groups AWS License Manager nella Guida AWS License Manager per l'utente.	N	S Può condividere con chiunque Account AWS.	N	No

Amazon Route 53

Puoi condividere le seguenti risorse Amazon Route 53 utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Gruppi di regole Route 53 Resolver Firewall DNS `route53resolver:FirewallRuleGroup`	Crea e gestisci centralmente i gruppi di regole di Route 53 Resolver DNS Firewall e condividili con altri Account AWS o con la tua organizzazione. Ciò consente a più account di condividere una serie di criteri per l'ispezione e la gestione delle DNS query in uscita che passano attraverso Route 53 Resolver. Per ulteriori informazioni, consulta la sezione Condivisione dei gruppi di regole del DNS firewall di Route 53 Resolver Account AWS nella Amazon Route 53 Developer Guide.	S	S Può condividere con chiunque. Account AWS	N	No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Route 53 Profiles `route53profiles:Profile`	Crea e gestisci Route 53 Profiles centralmente e condividili con altri Account AWS o con la tua organizzazione. Ciò consente a più account di applicare le DNS configurazioni specificate nella Route 53 Profiles a piùVPCs. Per ulteriori informazioni, consulta Amazon Route 53 Profilesnella Amazon Route 53 Developer Guide.	 S	 S Può condividere con chiunque Account AWS.	 S	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Regole del resolver `route53resolver:ResolverRule`	Crea e gestisci le regole Resolver centralmente e condividile con altri Account AWS o con la tua organizzazione. Ciò consente a più account di inoltrare DNS le query dai propri cloud privati virtuali (VPCs) agli indirizzi IP di destinazione definiti nelle regole Resolver condivise e gestite centralmente. Per ulteriori informazioni, consulta Condivisione delle regole del Resolver con altri Account AWS e utilizzo di regole condivise nella Amazon Route 53 Developer Guide.	 N	 S Può condividere con chiunque. Account AWS	 N	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Registri delle interrogazioni `route53resolver:ResolverQueryLogConfig`	Crea e gestisci i registri delle interrogazioni centralmente e condividili con altri utenti Account AWS o con la tua organizzazione. Ciò consente di Account AWS registrare più DNS interrogazioni che hanno VPCs origine in un registro delle query gestito centralmente. Per ulteriori informazioni, consulta Condivisione delle configurazioni di registrazione delle query di Resolver con altre nella Amazon Route 53 Account AWS Developer Guide.	 S	 S Può condividere con chiunque. Account AWS	 S	 No

Controller di ripristino delle applicazioni Amazon (ARC)

Puoi condividere le seguenti risorse di Amazon Application Recovery Controller (ARC) utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
ARC cluster `route53-recovery-control:Cluster`	Crea e gestisci ARC i cluster centralmente e condividili con altri Account AWS o con la tua organizzazione. Ciò consente a più account di creare pannelli di controllo e controlli di routing in un unico cluster condiviso, riducendo la complessità e il numero totale di cluster richiesti da un'organizzazione. Per ulteriori informazioni, consulta la sezione Condivisione di cluster tra account nella Amazon Application Recovery Controller (ARC) Developer Guide.	S	S Può condividere con chiunque Account AWS.	S	No

Amazon Simple Storage Service

È possibile condividere le seguenti Amazon Simple Storage Service risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Sovvenzioni di accesso `s3:AccessGrants`	Crea e gestisci le istanze S3 Access Grants centralmente e condividile con altri Account AWS o con la tua organizzazione. Ciò consente a più account di visualizzare ed eliminare le risorse condivise. Per ulteriori informazioni, consulta S3 Access Grants Cross-Access Cross-Access nella Guida per l' Amazon Simple Storage Service utente.	 S	 S Può condividere con chiunque. Account AWS	 S	 Sì

Amazon SageMaker AI

Puoi condividere le seguenti risorse Amazon SageMaker AI utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
SageMaker Catalogo AI `sagemaker:SagemakerCatalog`	Per la rilevabilità: consente ai proprietari degli account di concedere autorizzazioni di reperibilità ad altri account, per tutte le risorse dei gruppi di funzionalità nel SageMaker catalogo AI. Una volta concesso l'accesso, gli utenti di tali account possono visualizzare i gruppi di funzionalità che sono stati condivisi con loro dal catalogo. Per ulteriori informazioni, consulta la ricerca e l'accesso ai gruppi di funzionalità tra account nella Amazon SageMaker AI Developer Guide.	N	S Può condividere con chiunque. Account AWS	S	No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	Note La rilevabilità e l'accesso sono autorizzazioni separate in AI. SageMaker				

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
SageMaker Gruppo AI Feature `sagemaker:FeatureGroup`	Per l'accesso: consente ai proprietari di account di concedere le autorizzazioni di accesso ad altri account, per determinate risorse del gruppo di funzionalità. Una volta concesso l'accesso, gli utenti di tali account possono utilizzare i gruppi di funzionalità che sono stati condivisi con loro. Per ulteriori informazioni, consulta la ricerca e l'accesso ai gruppi di funzionalità tra account nella Amazon SageMaker AI Developer Guide. **Note** La rilevabilità e l'accesso sono autorizzazioni	 S	 S Può condividere con chiunque. Account AWS	 S	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	separate in AI. SageMaker				
SageMaker INTELLIGENZA ARTIFICIALE JumpStart `sagemaker:Hub`	Con Amazon SageMaker AI JumpStart, puoi crearli e gestirli `sagemaker:Hub` centralmente e condividerli con altri Account AWS membri della stessa organizzazione. Per ulteriori informazioni, consulta Controllare l'accesso al modello Foundation utilizzando hub privati curati in Amazon SageMaker AI JumpStart nella Amazon SageMaker AI Developer Guide.	 S	 S Può condividere con chiunque. Account AWS	 S	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Gruppo di lignaggio `sagemaker:LineageGroup`	Amazon SageMaker AI ti consente di creare gruppi di derivazione dei metadati della tua pipeline per comprenderne più a fondo la storia e le relazioni. Condividi il gruppo di discendenza con altri Account AWS o con gli account della tua organizzazione. Ciò consente a più Account AWS utenti di visualizzare le informazioni sul gruppo di discendenza e di interrogare le entità di tracciamento al suo interno. Per ulteriori informazioni, consulta la sezione Cross-Account Lineage Tracking nella Amazon SageMaker AI Developer Guide.	 S	 S Può condividere con chiunque. Account AWS	 N	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
SageMaker Schede modello AI `sagemaker:ModelCard`	Amazon SageMaker AI crea Model Cards per documentare dettagli critici sui tuoi modelli di machine learning (ML) in un unico posto per una governance e un reporting semplificati. Condividi le tue Model Cards con altri Account AWS account della tua organizzazione per realizzare una strategia multi-account per le tue operazioni di machine learning. Ciò consente di Account AWS condividere l'accesso alle schede modello per le loro attività di machine learning con altri account. Per ulteriori informazioni, consulta Amazon SageMaker AI Model Cards nella	 S	 S Può condividere con chiunque Account AWS.	 N	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	Amazon SageMaker AI Developer Guide.				
SageMaker Gruppo di pacchetti di modelli AI Model Registry `sagemaker:model-package-group`	Con Amazon SageMaker AI Model Registry, puoi creare e gestire `sagemaker:model-package-group` centralmente e condividerli con altri Account AWS per registrare le versioni dei modelli. Per ulteriori informazioni, consulta Amazon SageMaker AI Model Registry nella Amazon SageMaker AI Developer Guide.	 S	 S	 S	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
SageMaker Pipeline di intelligenza artificiale `sagemaker:Pipeline`	Con Amazon SageMaker AI Model Building Pipelines, puoi creare, automatizzare e gestire flussi di lavoro di end-to-end machine learning su larga scala. Condividi le tue pipeline con altri Account AWS o con gli account della tua organizzazione per realizzare una strategia multi-account per le tue operazioni di apprendimento automatico. Ciò consente a più Account AWS utenti di visualizzare le informazioni su una pipeline e sulle sue esecuzioni con accesso opzionale per avviare, interrompere e riprovare le pipeline da altri account. Per ulteriori informazioni, consulta Cross-Account	 S	 S Può condividere con chiunque. Account AWS	 S	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	Support for SageMaker AI Pipelines nella Amazon SageMaker AI Developer Guide.				

AWS Service Catalog AppRegistry

È possibile condividere le seguenti AWS Service Catalog AppRegistry risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Applicazione `servicecatalog:Application`	Crea un'applicazione e usala per tenere traccia delle risorse che appartengono a quell'applicazione in tutto l' AWS ambiente. Condividi l'applicazione	N	N Può condividere solo	S	No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	con altri Account AWS o con la tua organizzazione. Ciò consente a più Account AWS utenti di visualizzare localmente le informazioni sull'applicazione e le risorse associate. Per ulteriori informazioni, vedere Creazione di applicazioni nella Service Catalog User Guide.		Account AWS con la propria organizzazione.		

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Gruppo di attributi `servicecatalog:AttributeGroup`	Crea un gruppo di attributi e utilizzalo per archiviare i metadati relativi alle tue applicazioni. Condividi i gruppi di attributi con altri Account AWS o con la tua organizzazione. Ciò consente a più Account AWS utenti di visualizzare le informazioni sui gruppi di attributi. Per ulteriori informazioni, vedere Creazione di gruppi di attributi nella Service Catalog User Guide.	N	N Può condividere solo Account AWS con la propria organizzazione.	S	No

AWS Systems Manager Incident Manager

È possibile condividere le seguenti AWS Systems Manager Incident Manager risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Contatti `ssm-contacts:Contact`	Crea e gestisci i contatti e i piani di escalation centralmente e condividi i dettagli di contatto con altri Account AWS o con la tua organizzazione. Ciò consente a molti di Account AWS visualizzare gli impegni che si verificano durante un incidente. Per ulteriori informazioni, vedere Utilizzo dei contatti condivisi e dei piani di risposta nella Guida per l'utente di AWS Systems Manager Incident Manager.	 S	 S Può condividere con chiunque Account AWS.	 S	 No
Piani di risposta `ssm-incidents:ResponsePlan`	Crea e gestisci i piani di risposta centralmente e condividili con altri Account AWS o con la tua organizzazione. Ciò consente di	 S	 S Può condividere con	 S	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	Account AWS collegare gli CloudWatch allarmi di Amazon e le regole EventBridge degli eventi di Amazon ai piani di risposta, creando automaticamente un incidente quando viene rilevato. L'incidente ha anche accesso alle metriche di questi altri. Account AWS Per ulteriori informazioni, vedere Utilizzo dei contatti condivisi e dei piani di risposta nella Guida per l'utente di AWS Systems Manager Incident Manager.		chiunque Account AWS.		

AWS Systems Manager Parameter Store

È possibile condividere le seguenti risorse di AWS Systems Manager Parameter Store utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Parametro `ssm:Parameter`	Crea un parametro e utilizzalo per archiviare i dati di configurazione a cui puoi fare riferimento negli script, nei comandi, nei SSM documenti e nei flussi di lavoro di configurazione e automazione. Condividi il parametro con altri Account AWS o con la tua organizzazione. Ciò consente a più Account AWS utenti di visualizzare le informazioni sulla stringa e di migliorare la sicurezza separando i dati dal codice. Per ulteriori informazioni, consulta Lavorare con i parametri condivisi nella Guida per l'AWS Systems Manager utente.	 S	 S Può condividere con chiunque Account AWS.	 S	 No

Amazon VPC

Puoi condividere le seguenti risorse Amazon Virtual Private Cloud (AmazonVPC) utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Indirizzi di proprietà del cliente IPv4 `ec2:CoipPool`	Durante il processo di AWS Outposts installazione, AWS crea un pool di indirizzi, noto come pool di indirizzi IP di proprietà del cliente, in base alle informazioni fornite dall'utente sulla rete locale. Gli indirizzi IP di proprietà del cliente forniscono connettività locale o esterna alle risorse nelle sottoreti Outposts attraverso la rete locale. Puoi assegnare questi indirizzi alle risorse di Outpost, ad esempio le EC2 istanze, utilizzando indirizzi IP elastici	 N	 N Può condividere solo con la propria organizzazione. Account AWS	 N	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	o utilizzando l'impostazione della sottorete che assegna automaticamente gli indirizzi IP di proprietà del cliente. Per ulteriori informazioni, consulta Indirizzi IP di proprietà del cliente nella Guida per l'utente di AWS Outposts .				

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Pool di IP Address Manager (IPAM) `ec2:IpamPool`	Condividi i VPC IPAM pool Amazon centralmente con altri Account AWS IAM ruoli o utenti o con un'intera organizzazione o unità organizzativa (OU) in AWS Organizations. Ciò consente a tali responsabili di allocare CIDRs dal pool AWS le risorse, ad esempio VPCs nei rispettivi account. Per ulteriori informazioni, consulta Condividi un IPAM pool utilizzando AWS RAM nella Guida per l'utente di Amazon VPC IP Address Manager.	 S	 S Può condividere con chiunque Account AWS.	 S	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Individuazione delle risorse di IP Address Manager (IPAM) `ec2:IpamResourceDiscovery`	Condividi le scoperte di risorse con altri. Account AWS Un resource discovery è un VPC IPAM component e di Amazon che consente IPAM di gestire e monitorare le risorse che appartengono all'account proprietario. Per ulteriori informazioni, consulta Work with resource discoveries nella Amazon VPC IPAM User Guide.	 N	 S Può condividere con chiunque Account AWS.	 N	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Elenchi di prefissi `ec2:PrefixList`	Crea e gestisci elenchi di prefissi centralmente e condividili con altri Account AWS o con la tua organizzazione. Ciò consente di inserire più elenchi Account AWS di prefissi di riferimento nelle rispettive risorse, ad esempio gruppi di VPC sicurezza e tabelle di routing delle sottoreti. Per ulteriori informazioni, consulta Lavorare con gli elenchi di prefissi condivisi nella Amazon VPC User Guide.	 N	 S Può condividere con chiunque Account AWS.	 N	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Sottoreti `ec2:Subnet`	Crea e gestisci le sottoreti centralmente e condividile all' Account AWS interno della tua organizzazione. Ciò consente a più utenti di Account AWS avviare le proprie risorse applicative e di gestirle centralmente. VPCs Queste risorse includono EC2 istanze Amazon, database Amazon Relational Database Service RDS (), cluster Amazon Redshift e funzioni. AWS Lambda Per ulteriori informazioni, consulta Working with VPC sharing nella Amazon VPC User Guide.	N	N Può condividere solo Account AWS con la propria organizzazione.	N	No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	Note Per includere una sottorete quando crei una condivisione di risorse, devi disporre delle `ec2:DescribeVpcs` autorizzazioni `ec2:DescribeSubnets` e, oltre a. `ram:CreateResourceShare` Le sottoreti predefinite non sono condivisibili. È possibile condividere solo le sottoreti create dall'utente.				

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Gruppi di sicurezza `ec2:SecurityGroup`	Crea e gestisci gruppi di sicurezza centralmente e condividili con altri Account AWS o con la tua organizzazione. Ciò consente Account AWS a più utenti di associare il gruppo di sicurezza alle proprie interfacce di rete elastiche. Per ulteriori informazioni, consulta Condividi un gruppo di sicurezza nella Amazon VPC User Guide.	 S	 N Può condividere solo Account AWS con la propria organizzazione.	 S	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Traffic Mirror, obiettivi `ec2:TrafficMirrorTarget`	Crea e gestisci centralmente gli obiettivi Traffic Mirror e condividili con altri utenti Account AWS o con la tua organizzazione. Ciò consente a più utenti di Account AWS inviare traffico di rete in mirroring dalle sorgenti mirror del traffico presenti nei propri account a un target di mirroring del traffico condiviso e gestito centralmente. Per ulteriori informazioni, consulta Targets di mirroring del traffico tra account nella Traffic Mirroring Guide.	 N	 S Può condividere con chiunque. Account AWS	 N	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Gateway di transito `ec2:TransitGateway`	Crea e gestisci i gateway di transito centralmente e condividili con altri Account AWS o con la tua organizzazione. Ciò consente di Account AWS instradare il traffico multiplo tra le proprie reti VPCs e quelle locali attraverso un gateway di transito condiviso e gestito centralmente. Per ulteriori informazioni, consulta Condivisione di un gateway di transito in Amazon VPC Transit Gateways. **Note** Per includere un gateway di transito quando crei una condivisi	 N	 S Può condividere con chiunque Account AWS.	 N	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	one di risorse, devi disporre dell'`ec2:DescribeTransitGateway` autorizzazione oltre `aram:CreateResourceShare` .				

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Domini multicast Transit Gateway `ec2:TransitGatewayMulticastDomain`	Crea e gestisci centralmente i domini multicast del gateway di transito e condividili con altri Account AWS o con la tua organizzazione. In questo modo è Account AWS possibile registrare e annullare la registrazione di più membri del gruppo o sorgenti di gruppo nel dominio multicast. Per ulteriori informazioni, consulta Lavorare con domini multicast condivisi nella Transit Gateways Guide.	 N	 S Può condividere con chiunque. Account AWS	 N	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Accesso verificato da AWS gruppo `ec2:VerifiedAccessGroup`	Crea e gestisci Accesso verificato da AWS gruppi centralmente, quindi condividili con altri Account AWS o con la tua organizzazione. Ciò consente alle applicazioni con più account di utilizzare un unico set condiviso di Accesso verificato da AWS endpoint. Per ulteriori informazioni, consulta Condividi il tuo Accesso verificato da AWS gruppo AWS Resource Access Manager nella Guida per l'Accesso verificato da AWS utente.	 S	 S Può condividere con chiunque Account AWS.	 N	 No

Amazon VPC Lattice

Puoi condividere le seguenti risorse Amazon VPC Lattice utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Servizio Amazon VPC Lattice `vpc-lattice:Service`	Crea e gestisci i servizi Amazon VPC Lattice centralmente e condividili con singoli utenti Account AWS o con la tua organizzazione. Ciò consente ai proprietari dei servizi di connettersi, proteggere e osservare la service-to-service comunicazione in un ambiente con più account. Per ulteriori informazioni, consulta Lavorare con risorse condivise nella Guida per l'utente di VPC Lattice.	 N	 S Può condividere con chiunque Account AWS.	 S	 No
Rete di servizi Amazon VPC Lattice `vpc-lattice:ServiceNetwork`	Crea e gestisci reti di servizi Amazon VPC Lattice centralmente e condividile con singoli utenti Account AWS o con la tua organizzazione. Ciò consente	 N	 S Può condividere con chiunque	 S	 No

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	ai proprietari di reti di servizi di connettersi, proteggere e osservare la service-to-service comunicazione in un ambiente con più account. Per ulteriori informazioni, consulta Lavorare con risorse condivise nella Amazon VPC Lattice User Guide.		Account AWS.		

AWS Cloud WAN

Puoi condividere le seguenti WAN risorse AWS Cloud utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può essere condiviso con IAM utenti e ruoli	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Rete WAN centrale cloud `networkmanager:CoreNetwork`	Crea e gestisci una rete WAN centrale Cloud centralmente e condividila con altri Account AWS. Ciò consente Account AWS l'accesso e il provisioning di più host su un'unica rete WAN centrale Cloud. Per ulteriori informazioni, consulta Share a core network in the AWS Cloud WAN User Guide.	 S	 S Può condividere con chiunque Account AWS.	 N	 No

Gestione delle autorizzazioni inAWS RAM

InAWS RAM, esistono due tipi di autorizzazioni gestite, autorizzazioniAWS gestite e autorizzazioni gestite dal cliente.

Le autorizzazioni gestite definiscono il modo in cui un consumatore può agire sulle risorse in una condivisione di risorse. Quando si crea una condivisione di risorse, è necessario specificare quale autorizzazione gestita utilizzare per ogni tipo di risorsa incluso nella condivisione di risorse. Il modello di policy nell'autorizzazione gestita contiene tutto il necessario per una politica basata sulle risorse tranne il principale e la risorsa. L'Amazon Resource Name (ARN) della risorsa e l'ARN dei principali associati alla condivisione di risorse completano gli elementi di una politica basata sulle risorse. AWS RAMquindi crea la politica basata sulle risorse che associa a tutte le risorse in quella condivisione di risorse.

Ogni autorizzazione gestita può avere una o più versioni. Una versione è designata come versione predefinita per tale autorizzazione gestita. Occasionalmente,AWS aggiorna un'autorizzazioneAWS gestita per un tipo di risorsa creando una nuova versione e designandola come predefinita. Puoi anche aggiornare le autorizzazioni gestite dai clienti creando nuove versioni. Le autorizzazioni gestite già associate a una condivisione di risorse non vengono aggiornate automaticamente. LaAWS RAM console indica quando è disponibile una nuova versione predefinita ed è possibile rivedere le modifiche nella nuova versione predefinita rispetto a quella precedente.

> **Note**
>
> Ti consigliamo di eseguire l'aggiornamento alla nuova versione dell'autorizzazioneAWS gestita il prima possibile. Questi aggiornamenti in genere aggiungono il supporto per i nuovi o gli aggiornamentiServizi AWS che possono utilizzare per condividere altri tipi di risorseAWS RAM. Una nuova versione predefinita può anche risolvere e correggere le vulnerabilità di sicurezza.

> **Important**
>
> È possibile allegare la versione predefinita dell'autorizzazione gestita solo a una nuova condivisione di risorse.

Puoi recuperare l'elenco delle autorizzazioni gestite disponibili in qualsiasi momento. Per ulteriori informazioni, consulta Visualizzazione delle autorizzazioni gestite.

Argomenti

Visualizzazione delle autorizzazioni gestite

Puoi visualizzare i dettagli sulle autorizzazioni gestite disponibili per l'assegnazione ai tipi di risorse nelle tue condivisioni di risorse. È possibile identificare le autorizzazioni gestite assegnate alle condivisioni di risorse. Per visualizzare questi dettagli, usa la libreria delle autorizzazioni gestite nellaAWS RAM console.

Console

Per visualizzare i dettagli sulle autorizzazioni gestite disponibili inAWS RAM

1. Accedere alla pagina della libreria delle autorizzazioni gestite nellaAWS RAM console.
2. Poiché le condivisioni diAWS RAM risorse esistono in modo specificoRegioni AWS, scegli quella appropriataRegione AWS dall'elenco a discesa nell'angolo in alto a destra della console. Per visualizzare le condivisioni di risorse che contengono risorse globali, è necessarioRegione AWS impostarle su Stati Uniti orientali (Virginia settentrionale), (`us-east-1`). Per ulteriori informazioni sulla condivisione di risorse globali, consultaCondivisione delle risorse regionali rispetto alle risorse globali. Sebbene tutte le regioni condividano le stesse autorizzazioniAWS gestite disponibili, ciò influisce sul numero di condivisioni di risorse associate visualizzate per ciascuna autorizzazione gestita inStep 5. Le autorizzazioni gestite dal cliente sono disponibili solo nella regione in cui sono state create.
3. Nell'elenco Autorizzazioni gestite, scegli l'autorizzazione gestita di cui desideri visualizzare i dettagli. È possibile utilizzare la casella di ricerca per filtrare l'elenco delle autorizzazioni gestite immettendo parte del nome o del tipo di risorsa, oppure scegliendo un tipo di autorizzazione gestita dall'elenco a discesa.

4. (Facoltativo) Per modificare le preferenze di visualizzazione, scegli l'icona a forma di ingranaggio in alto a destra del pannello Autorizzazioni gestite da. È possibile modificare le seguenti preferenze:

   - Dimensione della pagina: il numero di risorse visualizzate in ogni pagina.
   - Linee di avvolgimento: indica se disporre le righe nelle righe della tabella.
   - Colonne: indica se visualizzare o nascondere le informazioni sul tipo di risorsa e sulle condivisioni associate.

   Dopo aver impostato le preferenze di visualizzazione, scegli Conferma.

5. Per ogni autorizzazione gestita, l'elenco contiene le seguenti informazioni:

   - Nome dell'autorizzazione gestita: il nome dell'autorizzazione gestita.
   - Tipo di risorsa: il tipo di risorsa associato all'autorizzazione gestita.
   - Tipo di autorizzazione gestita: se l'autorizzazione gestita è un'autorizzazioneAWS gestita o un'autorizzazione gestita dal cliente.
   - Condivisioni associate: il numero di condivisioni di risorse associate all'autorizzazione gestita. Se viene visualizzato un numero, puoi scegliere il numero per visualizzare una tabella di condivisioni di risorse con le seguenti informazioni:
     - Nome della condivisione di risorse: il nome della condivisione di risorse associata all'autorizzazione gestita.
     - Versione delle autorizzazioni gestite: la versione dell'autorizzazione gestita allegata a questa condivisione di risorse.
     - Proprietario: ilAccount AWS numero del proprietario della condivisione di risorse.
     - Consenti responsabili esterni: se tale condivisione di risorse consente la condivisione con dirigenti esterni all'organizzazioneAWS Organizations.
     - Stato: lo stato corrente dell'associazione tra la condivisione di risorse e l'autorizzazione gestita.
   - Stato: descrive se l'autorizzazione gestita è:
     - Allegabile: puoi allegare l'autorizzazione gestita alle tue condivisioni di risorse.
     - Non allegabile: non puoi allegare l'autorizzazione gestita alle tue condivisioni di risorse.
     - Eliminazione: l'autorizzazione gestita non è più attiva e verrà presto eliminata.
     - Eliminata: l'autorizzazione gestita è stata eliminata. Rimane visibile per due ore prima di scomparire dalla libreria delle autorizzazioni gestite.

È possibile scegliere il nome dell'autorizzazione gestita per visualizzare ulteriori informazioni su tale autorizzazione gestita. Nella pagina Dettagli di un'autorizzazione gestita sono visualizzate le seguenti informazioni:

- Tipo di risorsa: il tipo diAWS risorsa a cui si applica questa autorizzazione gestita.
- Numero di versioni: è possibile avere fino a cinque versioni di un'autorizzazione gestita dal cliente.
- Versione predefinita: specifica quale versione è quella predefinita e quindi assegnata automaticamente a tutte le nuove condivisioni di risorse che utilizzano questa autorizzazione gestita. Tutte le condivisioni di risorse esistenti che utilizzano versioni diverse visualizzano una richiesta per aggiornare la condivisione di risorse alla versione predefinita.
- ARN: il nome della risorsa Amazon (ARN) dell'autorizzazione gestita. Gli ARN per le autorizzazioniAWS gestite utilizzano il seguente formato:

  ```
  arn:aws:ram::aws:permission/
  AWSRAM[DefaultPermission]ShareableResourceType
  ```

  La sottostringa*[DefaultPermission]* (senza le parentesi in un ARN effettivo) è presente nel nome di una sola autorizzazione gestita per quel tipo di risorsa designata come predefinita.
- Versioni di autorizzazioni gestite: puoi scegliere quali informazioni sulla versione visualizzare nelle schede sotto questo elenco a discesa.
  - Scheda Dettagli:
    - Ora di creazione: la data e l'ora in cui è stata creata questa versione dell'autorizzazione gestita.
    - Ora dell'ultimo aggiornamento: la data e l'ora dell'ultimo aggiornamento di questa versione dell'autorizzazione gestita.
  - Scheda modello di policy: l'elenco delle azioni e delle condizioni del servizio, se applicabile, che questa versione dell'autorizzazione gestita consente ai committenti di eseguire sul tipo di risorsa associato.
  - Condivisioni di risorse associate: l'elenco delle condivisioni di risorse che utilizzano questa versione dell'autorizzazione gestita.

AWS CLI

Per visualizzare i dettagli sulle autorizzazioni gestite disponibili inAWS RAM

È possibile utilizzare il list-permissionscomando per ottenere un elenco delle autorizzazioni gestite disponibili per le condivisioni di risorse attualmente disponibiliRegione AWS per l'account chiamante.

```
$ aws ram list-permissions
{
    "permissions": [
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority",
            "version": "1",
            "defaultVersion": true,
            "name":
 "AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority",
            "resourceType": "acm-pca:CertificateAuthority",
            "status": "ATTACHABLE",
            "creationTime": "2022-06-30T13:03:31.732000-07:00",
            "lastUpdatedTime": "2022-06-30T13:03:31.732000-07:00",
            "isResourceTypeDefault": false,
            "permissionType": "AWS_MANAGED"
        },
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMBlankEndEntityCertificateAPIPassthroughIssuanceCertificateAuthority",
            "version": "1",
            "defaultVersion": true,
            "name":
 "AWSRAMBlankEndEntityCertificateAPIPassthroughIssuanceCertificateAuthority",
            "resourceType": "acm-pca:CertificateAuthority",
            "status": "ATTACHABLE",
            "creationTime": "2022-11-18T07:05:46.976000-08:00",
            "lastUpdatedTime": "2022-11-18T07:05:46.976000-08:00",
            "isResourceTypeDefault": false,
            "permissionType": "AWS_MANAGED"
        },

        ... TRUNCATED FOR BREVITY ... RUN COMMAND TO SEE COMPLETE LIST OF
 PERMISSIONS ...
```

```
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMVPCPermissionsNetworkManagerCoreNetwork",
            "version": "1",
            "defaultVersion": true,
            "name": "AWSRAMVPCPermissionsNetworkManagerCoreNetwork",
            "resourceType": "networkmanager:CoreNetwork",
            "status": "ATTACHABLE",
            "creationTime": "2022-06-30T13:03:46.557000-07:00",
            "lastUpdatedTime": "2022-06-30T13:03:46.557000-07:00",
            "isResourceTypeDefault": false,
            "permissionType": "AWS_MANAGED"
        },        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP",
            "version": "1",
            "defaultVersion": true,
            "name": "My-Test-CMP",
            "resourceType": "ec2:IpamPool",
            "status": "ATTACHABLE",
            "creationTime": "2023-03-08T06:54:10.038000-08:00",
            "lastUpdatedTime": "2023-03-08T06:54:10.038000-08:00",
            "isResourceTypeDefault": false,
            "permissionType": "CUSTOMER_MANAGED"
        }
    ]
}
```

È inoltre possibile trovare l'ARN di una specifica autorizzazione gestita in base al suo nome nel`--query` parametro del`list-permissions`AWS CLI comando. L'esempio seguente filtra l'output per includere solo gli elementi nei risultati dell'`permissions`array che corrispondono al nome specificato. Specifichiamo inoltre che vogliamo vedere solo il campo ARN nei risultati e in formato testo normale anziché nel JSON predefinito.

```
$ aws ram list-permissions \
    --query "permissions[?name == 'My-Test-CMP'].arn \
    --output text
arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP
```

Dopo aver trovato l'ARN dell'autorizzazione gestita specifica che ti interessa, puoi recuperarne i dettagli, incluso il testo della politica JSON, eseguendo il comando get-permission.

```
$ aws ram get-permission \
```

```
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP
{
    "permission": {
        "arn": "arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP",
        "version": "1",
        "defaultVersion": true,
        "name": "My-Test-CMP",
        "resourceType": "ec2:IpamPool",
        "permission": "{\n\t\"Effect\": \"Allow\",\n\t\"Action\": [\n
\t\t\"ec2:GetIpamPoolAllocations\",\n\t\t\"ec2:GetIpamPoolCidrs\",\n\t
\t\"ec2:AllocateIpamPoolCidr\",\n\t\t\"ec2:AssociateVpcCidrBlock\",\n
\t\t\"ec2:CreateVpc\",\n\t\t\"ec2:ProvisionPublicIpv4PoolCidr\",\n\t\t
\"ec2:ReleaseIpamPoolAllocation\"\n\t]\n}",
        "creationTime": "2023-03-08T06:54:10.038000-08:00",
        "lastUpdatedTime": "2023-03-08T06:54:10.038000-08:00",
        "isResourceTypeDefault": false,
        "permissionType": "CUSTOMER_MANAGED",
        "featureSet": "STANDARD",
        "status": "ATTACHABLE"
    }
}
```

Creazione e utilizzo delle autorizzazioni gestite dai clienti inAWS RAM

AWS Resource Access Manager(AWS RAM) fornisce almeno un'autorizzazioneAWS gestita per ogni tipo di risorsa che puoi condividere. Tuttavia, tali autorizzazioni gestite potrebbero non fornire l'accesso con privilegi minimi per il caso d'uso della condivisione. Quando una delle autorizzazioniAWS gestite fornite non funziona, puoi creare la tua autorizzazione gestita dal cliente.

Le autorizzazioni gestite dai clienti sono autorizzazioni gestite che crei e gestisci specificando con precisione quali azioni possono essere eseguite e in quali condizioni con l'utilizzo condiviso delle risorseAWS RAM. Ad esempio, desideri limitare l'accesso in lettura per i tuoi pool Amazon VPC IP Address Manager (IPAM), che ti aiutano a gestire i tuoi indirizzi IP su larga scala. Puoi creare autorizzazioni gestite dai clienti per consentire agli sviluppatori di assegnare indirizzi IP, ma non visualizzare l'intervallo di indirizzi IP assegnati da altri account sviluppatore. È possibile seguire la best practice sulla concessione di privilegi minimi, concedono solo le autorizzazioni richieste per eseguire le attività su risorse condivise.

Inoltre, puoi aggiornare o eliminare le autorizzazioni gestite dai clienti in base alle necessità.

Argomenti

Creazione di un'autorizzazione gestita dal cliente

Le autorizzazioni gestite dal cliente sono specifiche di unRegione AWS. Assicurati di creare questa autorizzazione gestita dal cliente nella regione appropriata.

Console

Per creare un'autorizzazione gestita dal cliente

1. Completa una delle seguenti operazioni:
   - Vai alla libreria delle autorizzazioni gestite e scegli Crea un'autorizzazione gestita dal cliente.
   - Passa direttamente alla pagina Crea un'autorizzazione gestita dal cliente nella console.
2. Per i dettagli delle autorizzazioni gestite dal cliente, inserisci un nome di autorizzazione gestita dal cliente.
3. Scegli il tipo di risorsa a cui si applica questa autorizzazione gestita.
4. Per il modello di policy, definisci quali operazioni possono essere eseguite su questo tipo di risorsa.
   - Puoi scegliere Importa autorizzazione gestita per utilizzare le azioni di un'autorizzazione gestita esistente.
   - Seleziona o deseleziona le informazioni sul livello di accesso per soddisfare i tuoi requisiti nell'editor visivo.
   - Aggiungi o modifica le condizioni utilizzando l'editor JSON.
5. (Facoltativo) Per allegare tag all'autorizzazione gestita, per Tag, inserisci una chiave e un valore per il tag. Aggiungi altri tag scegliendo Aggiungi nuovo tag. Ripetere ere ere ere ere ere ere ere ere ere.

6. Al termine, scegli Crea autorizzazione gestita dal cliente.

AWS CLI

Per creare un'autorizzazione gestita dal cliente

- Esegui il comando create-permission e specifica un nome, il tipo di risorsa a cui si applica l'autorizzazione gestita dal cliente e il testo del corpo del modello di policy.

  Il seguente comando di esempio crea un'autorizzazione gestita per il tipo di`imagebuilder:Component` risorsa.

```
$ aws ram create-permission \
    --name TestCMP \
    --resource-type imagebuilder:Component \
    --policy-template "{\"Effect\":\"Allow\",\"Action\":
[\"imagebuilder:ListComponents\"]}"
{
    "permission": {
        "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
        "version": "1",
        "defaultVersion": true,
        "isResourceTypeDefault": false,
        "name": "TestCMP",
        "resourceType": "imagebuilder:Component",
        "status": "ATTACHABLE",
        "creationTime": 1680033769.401,
        "lastUpdatedTime": 1680033769.401
    }
}
```

Crea una nuova versione di un'autorizzazione gestita dal cliente

Se il caso d'uso dell'autorizzazione gestita dal cliente cambia, puoi creare una nuova versione dell'autorizzazione gestita. Ciò non influisce sulle condivisioni di risorse esistenti, ma solo sulle nuove condivisioni di risorse future che utilizzano questa autorizzazione gestita dal cliente.

Ogni autorizzazione gestita può avere fino a cinque versioni, ma è possibile associare solo la versione predefinita.

Console

Per creare una nuova versione di un'autorizzazione gestita dal cliente

1. Accedere alla libreria delle autorizzazioni gestite.
2. Filtra l'elenco delle autorizzazioni gestite dal cliente o cerca il nome dell'autorizzazione gestita dal cliente che desideri modificare.
3. Nella pagina dei dettagli delle autorizzazioni gestite, nella sezione Versioni di autorizzazioni gestite, scegli Crea versione.
4. Per il modello Policy, puoi aggiungere o rimuovere azioni e condizioni con l'editor visivo o l'editor JSON.

   È inoltre possibile scegliere Importa autorizzazione gestita per utilizzare un modello di policy esistente.
5. Al termine, scegli Crea versione nella parte inferiore della pagina.

AWS CLI

Per creare una nuova versione di un'autorizzazione gestita dal cliente

1. Trova l'ARN (Amazon Resource Name) dell'autorizzazione gestita per la quale desideri creare una nuova versione. Esegui questa operazione chiamando list-permissions con il`--permission-type CUSTOMER_MANAGED` parametro per includere solo le autorizzazioni gestite dal cliente.

```
$ aws ram-cmp list-permissions --permission-type CUSTOMER_MANAGED
{
    "permissions": [
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "2",
            "defaultVersion": true,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "resourceType": "imagebuilder:Component",
            "status": "ATTACHABLE",
            "creationTime": 1680035597.346,
            "lastUpdatedTime": 1680035597.346
```

```
        }
    ]
}
```

2. Dopo aver ottenuto l'ARN, è possibile chiamare l'create-permission-versionoperazione e fornire il modello di policy aggiornato.

```
$ aws ram create-permission-version \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
    --policy-template {"Effect":"Allow","Action":
["imagebuilder:ListComponents"]}
{
    "permission": {
        "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
        "version": "2",
        "defaultVersion": true,
        "isResourceTypeDefault": false,
        "name": "TestCMP",
        "status": "ATTACHABLE",
        "resourceType": "imagebuilder:Component",
        "permission": "{\"Effect\":\"Allow\",\"Action\":
[\"imagebuilder:ListComponents\"]}",
        "creationTime": 1680038973.79,
        "lastUpdatedTime": 1680038973.79
    }
}
```

L'output include il numero di versione della nuova versione.

Scegli una versione diversa come predefinita per un'autorizzazione gestita dal cliente

È possibile impostare un'altra versione delle autorizzazioni gestite dal cliente come nuova versione predefinita.

Console

Per impostare una nuova versione predefinita per un'autorizzazione gestita dal cliente

1. Accedere alla libreria delle autorizzazioni gestite.

2. Filtra l'elenco delle autorizzazioni gestite dal cliente o cerca il nome dell'autorizzazione gestita dal cliente che desideri modificare.
3. Dalla pagina dei dettagli delle autorizzazioni gestite dal cliente, nella sezione Versioni di autorizzazioni gestite, utilizza l'elenco a discesa per scegliere la versione che desideri impostare come nuova impostazione predefinita.
4. Scegli Imposta come versione predefinita.
5. Quando viene visualizzata la finestra di dialogo, conferma che desideri che questa versione sia l'impostazione predefinita per tutte le nuove condivisioni di risorse che utilizzano questa autorizzazione gestita dal cliente. Se sei d'accordo, scegli Imposta come versione predefinita.

AWS CLI

Per impostare una nuova versione predefinita per un'autorizzazione gestita dal cliente

1. Trova il numero di versione che desideri impostare come versione predefinita chiamando list-permission-versions.

   Il seguente comando di esempio recupera le versioni correnti per l'autorizzazione gestita specificata.

```
$ aws ram list-permission-versions \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP
{
    "permissions": [
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "1",
            "defaultVersion": false,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "featureSet": "STANDARD",
            "resourceType": "imagebuilder:Component",
            "status": "UNATTACHABLE",
            "creationTime": 1680033769.401,
            "lastUpdatedTime": 1680035597.345
        },
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
```

```
            "version": "2",
            "defaultVersion": true,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "featureSet": "STANDARD",
            "resourceType": "imagebuilder:Component",
            "status": "ATTACHABLE",
            "creationTime": 1680035597.346,
            "lastUpdatedTime": 1680035597.346
        }
    ]
}
```


2. Dopo aver impostato il numero di versione come predefinito, è possibile chiamare l'set-default-permission-versionoperazione.

```
$ aws ram-cmp set-default-permission-version \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
    --version 2
```

Se il comando viene eseguito correttamente, non restituisce alcun output. Puoi eseguire di list-permission-versionsnuovo e verificare che il`defaultVersion` campo della versione scelta sia ora impostato su`true`.

Eliminare una versione di autorizzazione gestita dal cliente

Puoi avere fino a cinque versioni di ogni autorizzazione gestita dal cliente. Quando una versione non è più necessaria e non è più utilizzata, è possibile eliminarla. Non è possibile eliminare la versione predefinita di un'autorizzazione gestita dal cliente. Le versioni eliminate rimangono visibili nella console per un massimo di due ore con uno stato di eliminazione prima di essere completamente rimosse.

Console

Per eliminare una versione di autorizzazione gestita dal cliente

1. Accedere alla libreria delle autorizzazioni gestite.
2. Filtra l'elenco delle autorizzazioni gestite dal cliente o cerca il nome dell'autorizzazione gestita dal cliente con la versione che desideri eliminare.

3. Assicurati che la versione che desideri eliminare non sia attualmente quella predefinita.
4. Per la sezione Versioni della pagina, scegli la scheda Condivisioni di risorse associate per vedere se alcune condivisioni utilizzano questa versione.

   Se sono associate delle condivisioni, è necessario modificare la versione delle autorizzazioni gestite dal cliente prima di poter eliminare questa versione.
5. Scegli Elimina versione sul lato destro della sezione Versione.
6. Nella finestra di dialogo di conferma, seleziona Elimina per disabilitare questa versione dell'autorizzazione gestita dal cliente.

   Scegli Annulla se non desideri eliminare questa versione dell'autorizzazione gestita dal cliente.

AWS CLI

Per eliminare una versione di un'autorizzazione gestita dal cliente

1. Chiama l'list-permission-versionsoperazione per recuperare i numeri di versione disponibili.
2. Dopo aver ottenuto il numero di versione, forniscilo come parametro a delete-permission-version.

```
$ aws ram-cmp delete-permission-version \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
    --version 1
```

   Se il comando viene eseguito correttamente, non restituisce alcun output. È possibile eseguire list-permission-versionsnuovamente e verificare che la versione non sia più inclusa nell'output.

Eliminare un'autorizzazione gestita dal cliente

Se un'autorizzazione gestita dal cliente non è più necessaria e non è in uso, puoi eliminarla. Non è possibile eliminare un'autorizzazione gestita dal cliente associata a una condivisione di risorse. L'autorizzazione gestita dal cliente eliminata scompare dopo due ore. Fino ad allora, rimane visibile nella libreria delle autorizzazioni gestite con uno stato eliminato.

Console

Per eliminare un'autorizzazione gestita dal cliente

1. Accedere alla libreria delle autorizzazioni gestite.
2. Filtra l'elenco delle autorizzazioni gestite dal cliente o cerca il nome dell'autorizzazione gestita dal cliente che desideri eliminare.
3. Verifica che vi siano 0 condivisioni associate nell'elenco delle autorizzazioni gestite prima di selezionare l'autorizzazione gestita dal cliente.

   Se esistono ancora condivisioni di risorse associate all'autorizzazione gestita, è necessario assegnare un'altra autorizzazione gestita a tutte le condivisioni di risorse prima di poter continuare.
4. Nell'angolo in alto a destra della pagina dei dettagli delle autorizzazioni gestite dal cliente, scegliere Elimina autorizzazione gestita.
5. Quando viene visualizzata la finestra di dialogo di conferma, scegli Elimina per eliminare l'autorizzazione gestita.

AWS CLI

Per eliminare un'autorizzazione gestita dal cliente

1. Trova l'ARN dell'autorizzazione gestita che desideri eliminare chiamando list-permissions con il`--permission-type CUSTOMER_MANAGED` parametro per includere solo le autorizzazioni gestite dal cliente.

```
$ aws ram-cmp list-permissions --permission-type CUSTOMER_MANAGED
{
    "permissions": [
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "2",
            "defaultVersion": true,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "resourceType": "imagebuilder:Component",
            "status": "ATTACHABLE",
            "creationTime": 1680035597.346,
```

```
            "lastUpdatedTime": 1680035597.346
        }
    ]
}
```

2. Dopo aver ottenuto l'ARN dell'autorizzazione gestita per l'eliminazione, forniscila come parametro per l'autorizzazione all'eliminazione.

```
$ aws ram delete-permission \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP
{
    "returnValue": true,
    "permissionStatus": "DELETING"
}
```

Aggiornamento delle autorizzazioniAWS gestite a una versione più recentissima

Occasionalmente,AWS aggiorna le autorizzazioniAWS gestite disponibili da allegare a una condivisione di risorse per un tipo di risorsa specifico. Quando loAWS fa, crea una nuova versione dell'autorizzazioneAWS gestita. Le condivisioni di risorse che includono il tipo di risorsa specificato non vengono aggiornate automaticamente per utilizzare la versione più recente dell'autorizzazione gestita. È necessario aggiornare in modo esplicito l'autorizzazione gestita per ogni condivisione di risorse. Questo passaggio aggiuntivo è necessario per poter valutare le modifiche prima di applicarle alle condivisioni di risorse.

Console

Ogni volta che la console visualizza una pagina che elenca le autorizzazioni associate a una condivisione di risorse e una o più di queste autorizzazioni utilizzano una versione diversa da quella predefinita per l'autorizzazione, la console visualizza un banner nella parte superiore della pagina della console. Il banner indica che la condivisione di risorse utilizza una versione diversa da quella predefinita.

Inoltre, le autorizzazioni individuali possono visualizzare un pulsante Aggiorna alla versione predefinita accanto al numero di versione corrente quando quella versione non è quella predefinita.

La scelta di quel pulsante avvia la procedura guidata di condivisione delle risorse di aggiornamento. Nella fase 2 della procedura guidata è possibile aggiornare la versione di tutte le autorizzazioni non predefinite per utilizzare le versioni predefinite.

Le modifiche non vengono salvate finché non si completa la procedura guidata scegliendo Invia nell'ultima pagina della procedura guidata.

> **Note**
>
> Puoi allegare solo la versione predefinita e non puoi tornare a un'altra versione. Per le autorizzazioni gestite dai clienti, dopo aver aggiornato le autorizzazioni alla versione predefinita, non è possibile applicare un'altra versione a una condivisione di risorse a meno che non si imposti prima l'altra versione come predefinita. Ad esempio, se hai aggiornato un'autorizzazione alla versione predefinita e poi hai trovato un errore che desideri ripristinare, puoi designare la versione precedente come predefinita. In alternativa, è possibile creare una nuova versione diversa e quindi designarla come predefinita. Dopo aver eseguito una di queste opzioni, è necessario aggiornare le condivisioni di risorse per utilizzare quella che ora è la versione predefinita.

AWS CLI

Per aggiornare la versione di un'autorizzazioneAWS gestita

1. Esegui il comando get-resource-sharescon il`--permission-arn` parametro per specificare l'Amazon Resource Name (ARN) dell'autorizzazione gestita che desideri aggiornare. Ciò fa sì che il comando restituisca solo le condivisioni di risorse che utilizzano tale autorizzazione gestita.

   Ad esempio, il seguente comando di esempio restituisce i dettagli per ogni condivisione di risorse che utilizza l'autorizzazioneAWS gestita predefinita per le prenotazioni di capacità di Amazon EC2.

   ```
   $ aws ram get-resource-shares \
       --resource-owner SELF \
       --permission-arn arn:aws:ram::aws:permission/
   AWSRAMDefaultPermissionCapacityReservation
   ```

L'output include l'ARN di ogni condivisione di risorse con almeno una risorsa il cui accesso è controllato da tale autorizzazione gestita.

2. Per ogni condivisione di risorse specificata nel comando precedente, esegui il comando associate-resource-share-permission. Includi il parametro `--resource-share-arn` per specificare la condivisione di risorse da aggiornare, il parametro `--permission-arn` per specificare quale autorizzazioneAWS gestita stai aggiornando e il `--replace` parametro per specificare che desideri aggiornare la condivisione per utilizzare la versione più recente di tale autorizzazione gestita. Non è necessario specificare il numero di versione; la versione predefinita viene utilizzata automaticamente.

```
$ aws ram associate-resource-share-permission \
    --resource-share-arn < ARN of one of the shares from the output of the
 previous command > \
    --permission-arn arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionCapacityReservation \
    --replace
```

3. Ripeti il comando nel passaggio precedente per ogni`ResourceShareArn` oggetto che hai ricevuto nei risultati del comando del passaggio 1.

Considerazioni sull'utilizzo delle autorizzazioni gestite dal cliente in AWS RAM

Le autorizzazioni gestite dal cliente sono disponibili solo nella versione in Regione AWS cui le crei. Non tutti i tipi di risorse supportano le autorizzazioni gestite dai clienti. Per un elenco dei tipi di risorse supportati in AWS Resource Access Manager, vedereRisorse condivisibili AWS.

Le autorizzazioni gestite dal cliente con più istruzioni non sono supportate. Puoi utilizzare solo singoli operatori senza negazione nelle autorizzazioni gestite dai clienti.

Le seguenti condizioni non sono supportate nelle autorizzazioni gestite dai clienti:

- Chiavi condizionali utilizzate per abbinare le proprietà del principale:
  - `aws:PrincipalOrgId`
  - `aws:PrincipalOrgPaths`
  - `aws:PrincipalAccount`

- Chiavi condizionali utilizzate per limitare l'accesso ai responsabili del servizio:
  - `aws:SourceArn`
  - `aws:SourceAccount`
  - `aws:SourceOrgPaths`
  - `aws:SourceOrgID`
- Tag di sistema:
  - `aws:PrincipalTag/aws:`
  - `aws:ResourceTag/aws:`
  - `aws:RequestTag/aws:`

> **Note**
>
> Il `aws:SourceAccount` valore viene compilato automaticamente durante la condivisione con i responsabili del servizio.

Come funzionano le autorizzazioni gestite

Per una rapida panoramica, guarda il video seguente che dimostra come le autorizzazioni gestite consentono di applicare la best practice di accesso con privilegi minimi alleAWS risorse.

In questo video viene illustrato come creare e associare le autorizzazioni gestite dai clienti seguendo la best practice dei privilegi minimi. Per ulteriori informazioni, consultare ???.

Quando si crea una condivisione di risorse, si associa un'autorizzazioneAWS gestita a ogni tipo di risorsa che si desidera condividere. Se l'autorizzazione gestita ha più di una versione, la nuova condivisione di risorse utilizza sempre la versione designata come predefinita.

Dopo aver creato la condivisione di risorse,AWS RAM utilizza l'autorizzazione gestita per generare una politica basata sulle risorse allegata a ciascuna risorsa condivisa.

Il modello di policy in un'autorizzazione gestita specifica quanto segue:

Effetto

Indica se eseguire un'operazione su una risorsa condivisa`Allow` o`Deny` l'autorizzazione principale. Per un'autorizzazione gestita, l'effetto è sempre`Allow`. Per ulteriori informazioni, consulta Effect nella Guida per l'utente IAM.

Operazione

L'elenco delle operazioni che il committente è autorizzato a eseguire. Può trattarsi di un'azione inAWS Management Console o di un'operazione inAWS Command Line Interface (AWS CLI) o nell'AWSAPI. Le azioni sono definite dall'AWSautorizzazione. Per ulteriori informazioni, consulta Azione nella Guida per l'utente IAM.

Condition

Quando e come un preside può interagire con una risorsa in una condivisione di risorse. Le condizioni aggiungono un ulteriore livello di sicurezza alle risorse condivise. Usali per limitare l'accesso alle tue risorse condivise per azioni sensibili. Ad esempio, è possibile includere condizioni che richiedono che le azioni provengano da uno specifico intervallo di indirizzi IP aziendali o che le azioni devono essere eseguite da utenti autenticati con l'autenticazione a più fattori. Per ulteriori informazioni sulle condizioni, consulta Chiavi di contesto delle condizioniAWS globali nella Guida per l'utente IAM. Per ulteriori informazioni sulle condizioni specifiche dei servizi, consulta Operazioni, risorse e chiavi di condizione per iAWS servizi in Service Authorization Reference.

> **Note**
>
> Le condizioni sono disponibili per le autorizzazioni gestite dai clienti e i tipi di risorse supportati per le autorizzazioniAWS gestite.
> Per informazioni sulle condizioni che sono escluse dall'uso con autorizzazioni gestite dal cliente, vedereConsiderazioni sull'utilizzo delle autorizzazioni gestite dal cliente in AWS RAM.

Tipi di autorizzazioni gestite

Quando si crea una condivisione di risorse, si sceglie un'autorizzazione gestita da associare a ogni tipo di risorsa che si include nella condivisione di risorse. AWSle autorizzazioni gestite sono definite dal servizioAWS proprietario delle risorse e gestite daAWS RAM. Tu crei e gestisci le tue autorizzazioni gestite dai clienti.

- AWSautorizzazione gestita: è disponibile un'autorizzazione gestita predefinita per ogni tipo di risorsaAWS RAM supportata. L'autorizzazione gestita predefinita è quella utilizzata per un tipo di risorsa a meno che non si scelga esplicitamente una delle autorizzazioni gestite aggiuntive. L'autorizzazione gestita predefinita è destinata a supportare gli scenari più comuni dei clienti per la condivisione di risorse del tipo specificato. L'autorizzazione gestita predefinita consente ai responsabili di eseguire azioni specifiche definite dal servizio per il tipo di risorsa. Ad esempio, per il tipo di`ec2:Subnet` risorsa Amazon VPC, l'autorizzazione gestita predefinita consente ai committenti di eseguire le seguenti azioni:
  - `ec2:RunInstances`
  - `ec2:CreateNetworkInterface`
  - `ec2:DescribeSubnets`

  I nomi delle autorizzazioniAWS gestite predefinite utilizzano il seguente formato:`AWSRAMDefaultPermission`*`ShareableResourceType`*. Ad esempio, per il tipo di`ec2:Subnet` risorsa, il nome dell'autorizzazioneAWS gestita predefinita è`AWSRAMDefaultPermissionSubnet`.

  > **Note**
  >
  > L'autorizzazione gestita predefinita è separata dalla versione predefinita di un'autorizzazione gestita. Tutte le autorizzazioni gestite, predefinite o una delle autorizzazioni gestite aggiuntive supportate da alcuni tipi di risorse, sono autorizzazioni separate e complete con effetti e azioni diversi che supportano diversi scenari di condivisione, ad esempio l'accesso in lettura e scrittura rispetto all'accesso di sola lettura. Qualsiasi autorizzazione gestita, indipendentemente dal fatto cheAWS sia gestita dal cliente, può avere più versioni, una delle quali è la versione predefinita per tale autorizzazione.

  Ad esempio, quando si condivide un tipo di risorsa che supporta sia l'accesso completo (`ReadeWrite`) l'autorizzazione gestita sia un'autorizzazione gestita di sola lettura, è possibile creare una condivisione di risorse per l'amministratore con l'autorizzazione gestita ad accesso completo. È quindi possibile creare una condivisione di risorse separata per altri sviluppatori utilizzando l'autorizzazione gestita di sola lettura per seguire la pratica della concessione del privilegio minimo.

> **Note**
>
> Tutti iAWS servizi che funzionano conAWS RAM supportano almeno un'autorizzazione gestita predefinita. È possibile visualizzare le autorizzazioni disponibili per ciascuna nellaServizio AWS pagina della libreria delle autorizzazioni gestite. Questa pagina fornisce dettagli su ogni autorizzazione gestita disponibile, comprese eventuali condivisioni di risorse attualmente associate all'autorizzazione e se è consentita la condivisione con responsabili esterni, se applicabile. Per ulteriori informazioni, consulta Visualizzazione delle autorizzazioni gestite.
>
> Per i servizi che non supportano autorizzazioni gestite aggiuntive, quando si crea una condivisione di risorse, si applicaAWS RAM automaticamente l'autorizzazione predefinita definita per il tipo di risorsa scelto. Se supportato, avrai anche la possibilità di scegliere Crea autorizzazione gestita dal cliente nella pagina Associa autorizzazioni gestite.

- Autorizzazioni gestite dal cliente: le autorizzazioni gestite dal cliente sono autorizzazioni gestite che crei e gestisci specificando con precisione quali azioni possono essere eseguite e in quali condizioni con l'utilizzo condiviso delle risorseAWS RAM. Ad esempio, desideri limitare l'accesso in lettura per i tuoi pool Amazon VPC IP Address Manager (IPAM), che ti aiutano a gestire i tuoi indirizzi IP su larga scala. Puoi creare autorizzazioni gestite dai clienti per consentire agli sviluppatori di assegnare indirizzi IP, ma non visualizzare l'intervallo di indirizzi IP assegnati da altri account sviluppatore. Puoi seguire la best practice dei privilegi minimi, concedendo solo le autorizzazioni richieste per eseguire attività su risorse condivise.

Sicurezza in AWS RAM

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

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

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per ulteriori informazioni sui programmi di conformità che si applicano ad AWS Resource Access Manager 8 AWS RAM), consulta Servizi coperti dal programma di conformitàAWS.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS RAM. I seguenti argomenti mostrano come configurare per AWS RAM soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere AWS RAM le tue risorse.

Argomenti

Protezione dei dati in AWS RAM

Il modello di responsabilità AWS condivisa modello di di si applica alla protezione dei dati in AWS Resource Access Manager. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, consulta la sezione Privacy dei dati FAQ. Per informazioni sulla protezione dei dati in Europa, consulta il Modello di responsabilitàAWS condivisa e GDPR il post sul blog sulla AWS sicurezza.

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

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

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

Gestione delle identità e degli accessi per AWS RAM

AWS Identity and Access Management (IAM) è un AWS servizio che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori hanno IAM il controllo su chi può essere autenticato (effettuato l'accesso) e autorizzato (dispone delle autorizzazioni) a utilizzare le risorse. AWS UtilizzandoIAM, crei i principali, come ruoli, utenti e gruppi, all'interno del tuo. Account AWS Sei tu a controllare le autorizzazioni di cui dispongono tali responsabili per eseguire attività utilizzando le risorse. AWS È possibile utilizzare IAM senza costi aggiuntivi. Per ulteriori informazioni sulla gestione e la creazione IAM di politiche personalizzate, vedere Gestione delle IAM politiche nella Guida per l'IAMutente.

Argomenti

Come AWS RAM funziona con IAM

Per impostazione predefinita, IAM i mandanti non sono autorizzati a creare o modificare AWS RAM risorse. Per consentire IAM ai responsabili di creare o modificare risorse ed eseguire attività, è necessario eseguire una delle seguenti operazioni. Queste azioni concedono il permesso di utilizzare risorse e API azioni specifiche.

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .
- Utenti gestiti IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate in Creare un ruolo per un provider di identità di terze parti (federazione) nella Guida per l'IAMutente.

- IAMutenti:
  - Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate in Creare un ruolo per un IAM utente nella Guida per l'IAMutente.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate in Aggiungere autorizzazioni a un utente (console) nella Guida per l'IAMutente.

AWS RAM fornisce diverse politiche AWS gestite che puoi utilizzare per soddisfare le esigenze di molti utenti. Per ulteriori informazioni su queste impostazioni, consulta AWS Policy gestite da per AWS RAM.

Se hai bisogno di un controllo più preciso sulle autorizzazioni concesse ai tuoi utenti, puoi creare le tue politiche nella console. IAM Per informazioni sulla creazione di politiche e sulla loro associazione ai IAM ruoli e agli utenti, consulta Politiche e autorizzazioni nella IAM Guida per l'utente.AWS Identity and Access Management

Le seguenti sezioni forniscono i dettagli AWS RAM specifici per la creazione di una politica di IAM autorizzazione.

Indice

Struttura delle policy

Una politica di IAM autorizzazione è un JSON documento che include le seguenti dichiarazioni: Effetto, Azione, Risorsa e Condizione. Una IAM politica assume in genere la forma seguente.

```
{
    "Statement":[{
        "Effect":"<effect>",
        "Action":"<action>",
        "Resource":"<arn>",
        "Condition":{
```

```
            "<comparison-operator>":{
                "<key>":"<value>"
            }
        }
    }]
}
```

Effetto

L'istruzione Effect indica se la politica consente o nega l'autorizzazione principale per eseguire un'azione. I valori possibili includono: `Allow` e`Deny`.

Azione

La dichiarazione Action specifica le AWS RAM API azioni per le quali la politica consente o nega l'autorizzazione. Per un elenco completo delle azioni consentite, vedere Azioni definite da AWS Resource Access Manager nella Guida per l'IAMutente.

Risorsa

L'informativa Resource specifica le AWS RAM risorse interessate dalla politica. Per specificare una risorsa nell'istruzione, devi utilizzare il relativo Amazon Resource Name univoco (ARN). Per un elenco completo delle risorse consentite, consulta la sezione Risorse definite da AWS Resource Access Manager nella Guida per l'IAMutente.

Condizione

Le istruzioni sulle condizioni sono facoltative. Possono essere utilizzate per perfezionare ulteriormente le condizioni alle quali si applica la politica. AWS RAM supporta le seguenti chiavi di condizione:

- `aws:RequestTag/${TagKey}`— Verifica se la richiesta di servizio include un tag con la chiave di tag specificata esiste e ha il valore specificato.
- `aws:ResourceTag/${TagKey}`— Verifica se alla risorsa su cui si basa la richiesta di servizio è associata un'etichetta con una chiave di tag specificata nella policy.

  La condizione di esempio seguente verifica che la risorsa a cui si fa riferimento nella richiesta di servizio abbia un tag allegato con il nome chiave «Owner» e il valore «Dev Team».

  ```
  "Condition" : {
      "StringEquals" : {
  ```

```
        "aws:ResourceTag/Owner" : "Dev Team"
    }
}
```

- `aws:TagKeys`— Speciifica le chiavi dei tag che devono essere utilizzate per creare o contrassegnare una condivisione di risorse.
- `ram:AllowsExternalPrincipals`— Verifica se la condivisione di risorse nella richiesta di servizio consente la condivisione con responsabili esterni. Un principale esterno è una persona Account AWS esterna all'organizzazione in AWS Organizations. Se il risultato è positivo`False`, puoi condividere questa condivisione di risorse con gli account solo della stessa organizzazione.
- `ram:PermissionArn`— Verifica se l'autorizzazione ARN specificata nella richiesta di servizio corrisponde a una ARN stringa specificata nella politica.
- `ram:PermissionResourceType`— Verifica se l'autorizzazione specificata nella richiesta di servizio è valida per il tipo di risorsa specificato nella politica. Specificate i tipi di risorse utilizzando il formato mostrato nell'elenco dei tipi di risorse condivisibili.
- `ram:Principal`— Verifica se il valore ARN del principale specificato nella richiesta di servizio corrisponde a una ARN stringa specificata nella politica.
- `ram:RequestedAllowsExternalPrincipals`— Verifica se la richiesta di servizio include il `allowExternalPrincipals` parametro e se il relativo argomento corrisponde al valore specificato nella politica.
- `ram:RequestedResourceType`— Verifica se il tipo di risorsa su cui si agisce corrisponde a una stringa di tipo di risorsa specificata nella politica. Specificate i tipi di risorse utilizzando il formato mostrato nell'elenco dei tipi di risorse condivisibili.
- `ram:ResourceArn`— Verifica se ARN la risorsa su cui si basa la richiesta di servizio corrisponde a ARN quella specificata nella politica.
- `ram:ResourceShareName`— Verifica se il nome della condivisione di risorse su cui agisce la richiesta di servizio corrisponde a una stringa specificata nella politica.
- `ram:ShareOwnerAccountId`— Verifica che il numero ID dell'account della condivisione di risorse su cui agisce la richiesta di servizio corrisponda a una stringa specificata nella politica.

AWS Policy gestite da per AWS RAM

AWS Resource Access Managerattualmente fornisce diversiAWS RAMpolitiche gestite, descritte in questo argomento.

Policy gestite da AWS

- AWSPolicy gestita: AWSResourceAccessManagerReadOnlyAccess
- AWSPolicy gestita: AWSResourceAccessManagerFullAccess
- AWSPolicy gestita: AWSResourceAccessManagerResourceShareParticipantAccess
- AWSPolicy gestita: AWSResourceAccessManagerServiceRolePolicy
- Aggiornamenti di AWS RAM alle policy gestite da AWS

Nell'elenco precedente, puoi allegare le prime tre policy ai tuoi ruoli, gruppi e utenti IAM per concedere le autorizzazioni. L'ultima politica dell'elenco è riservata alAWS RAMruolo legato ai servizi del servizio.

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

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

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

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

AWSPolicy gestita: AWSResourceAccessManagerReadOnlyAccess

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

Questa politica fornisce autorizzazioni di sola lettura per le condivisioni di risorse di proprietà dell'utenteAccount AWS.

Lo fa concedendo il permesso di eseguire uno qualsiasi dei`Get*`o`List*`operazioni. Non offre alcuna possibilità di modificare alcuna condivisione di risorse.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `ram`— Consente ai titolari di visualizzare i dettagli sulle quote di risorse possedute dall'account.

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

AWSPolicy gestita: AWSResourceAccessManagerFullAccess

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

Questa politica fornisce l'accesso amministrativo completo per visualizzare o modificare le condivisioni di risorse di proprietà dell'utente.Account AWS.

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

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `ram`— Consente ai committenti di visualizzare o modificare qualsiasi informazione sulle quote di risorse di proprietà delAccount AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ram:*"
            ],
```

```
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWSPolicy gestita: AWSResourceAccessManagerResourceShareParticipantAccess

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

Questa politica offre ai dirigenti la possibilità di accettare o rifiutare le condivisioni di risorse condivise con questo sito.Account AWSe per visualizzare i dettagli su queste condivisioni di risorse. Non offre alcuna possibilità di modificare tali condivisioni di risorse.

Lo fa concedendo il permesso di eseguirne alcuni`ram`operazioni.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `ram`— Consente agli amministratori di accettare o rifiutare gli inviti alla condivisione delle risorse e di visualizzare i dettagli sulle condivisioni di risorse condivise con l'account.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ram:AcceptResourceShareInvitation",
                "ram:GetResourcePolicies",
                "ram:GetResourceShareInvitations",
                "ram:GetResourceShares",
                "ram:ListPendingInvitationResources",
                "ram:ListPrincipals",
                "ram:ListResources",
                "ram:RejectResourceShareInvitation"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

```
}
```

AWSPolicy gestita: AWSResourceAccessManagerServiceRolePolicy

LaAWSpolitica gestita`AWSResourceAccessManagerServiceRolePolicy`può essere utilizzato solo con il ruolo collegato al servizio perAWS RAM. Non puoi allegare, scollegare, modificare o eliminare questa politica.

Questa politica prevedeAWS RAMcon accesso di sola lettura alla struttura della tua organizzazione. Quando abiliti l'integrazione traAWS RAMeAWS Organizations,AWS RAMcrea automaticamente un ruolo collegato al servizio denominatoAWSServiceRoleForResourceAccessManagerche il servizio presuppone quando deve cercare informazioni sull'organizzazione e sui relativi account, ad esempio, quando si visualizza la struttura dell'organizzazione nelAWS RAMconsolle.

Lo fa concedendo l'autorizzazione di sola lettura per eseguire il`organizations:Describe`e`organizations:List`operazioni che forniscono dettagli sulla struttura e sui conti dell'organizzazione.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `organizations`— Consente ai dirigenti di visualizzare informazioni sulla struttura dell'organizzazione, comprese le unità organizzative, eAccount AWScontengono.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListRoots"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowDeletionOfServiceLinkedRoleForResourceAccessManager",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-service-role/ram.amazonaws.com/*"
            ]
        }
    ]
}
```

Aggiornamenti di AWS RAM alle policy gestite da AWS

Visualizza i dettagli sugli aggiornamenti alle policy gestite da AWS per AWS RAM da quando questo servizio ha iniziato a tenere traccia delle modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivi il feed RSS nella pagina della cronologia dei documenti di AWS RAM.

Modifica	Descrizione	Data
AWS Resource Access Manager ha iniziato il rilevamento delle modifiche	AWS RAMha documentato le politiche gestite esistenti e ha iniziato a monitorare le modifiche.	16 settembre 2021

Utilizzo di ruoli collegati ai servizi per AWS RAM

AWS Resource Access Manager utilizza ruoli collegati al servizio AWS Identity and Access Management (IAM). Un ruolo collegato al servizio è un tipo unico di ruolo IAM collegato direttamente al AWS RAM servizio. I ruoli collegati ai servizi sono predefiniti AWS e includono tutte le autorizzazioni necessarie per chiamare altri servizi per AWS RAM tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione AWS RAM perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AWS RAMdefinisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumere i ruoli collegati al

servizio. AWS RAM Le autorizzazioni definite includono sia una politica di fiducia che una politica di autorizzazioni e tale politica di autorizzazioni non può essere associata a nessun'altra entità IAM.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta la sezione Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni del ruolo collegato ai servizi per AWS RAM

AWS RAMutilizza il ruolo collegato al servizio denominato `AWSServiceRoleForResourceAccessManager` quando abiliti la condivisione con. AWS Organizations Questo ruolo concede al AWS RAM servizio le autorizzazioni per visualizzare i dettagli dell'organizzazione, come l'elenco degli account membri e le unità organizzative in cui si trova ciascun account.

Questo ruolo collegato al servizio si affida al seguente servizio per l'assunzione del ruolo:

- `ram.amazonaws.com`

La politica di autorizzazione del ruolo denominata AWSResourceAccessManagerServiceRolePolicy è allegata a questo ruolo collegato al servizio e consente di AWS RAM completare le seguenti azioni sulle risorse specificate:

- Azioni: azioni di sola lettura che recuperano dettagli sulla struttura dell'organizzazione. Per l'elenco completo delle azioni, puoi visualizzare la policy nella console IAM:. AWSResourceAccessManagerServiceRolePolicy

Affinché un responsabile attivi la AWS RAM condivisione all'interno dell'organizzazione, tale responsabile (un'entità IAM come un utente, un gruppo o un ruolo) deve disporre dell'autorizzazione per creare un ruolo collegato al servizio. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per AWS RAM

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando attivi la AWS RAM condivisione all'interno della tua organizzazione o la AWS Management Console esegui EnableSharingWithAwsOrganizationnel tuo account utilizzando AWS CLI o un'AWSAPI, AWS RAM crea automaticamente il ruolo collegato al servizio.

Chiama `enable-sharing-with-aws-organizations` per creare il ruolo collegato al servizio nel tuo account.

Se elimini questo ruolo collegato al servizio, AWS RAM non hai più le autorizzazioni per visualizzare i dettagli della struttura della tua organizzazione.

Modifica di un ruolo collegato ai servizi per AWS RAM

AWS RAMnon consente di modificare il ruolo collegato al AWSResourceAccessManagerServiceRolePolicy servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta la sezione Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per AWS RAM

Per eliminare manualmente un ruolo collegato ai servizi è possibile utilizzare anche la console IAM, la AWS CLI o l'API di AWS.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM, la AWS CLI o l'API AWS per eliminare il ruolo collegato ai servizi `AWSResourceAccessManagerServiceRolePolicy`. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi AWS RAM

AWS RAM supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint AWS nella Riferimenti generali di Amazon Web Services.

Policy IAM di esempio per AWS RAM

Questo argomento include esempi di policy IAM AWS RAM che dimostrano la condivisione di risorse e tipi di risorse specifici e la limitazione della condivisione.

Esempi di policy IAM

- Esempio 1: consentire la condivisione di risorse specifiche
- Esempio 2: consentire la condivisione di tipi di risorse specifici

- Esempio 3: limita la condivisione con utenti esterni Account AWS

Esempio 1: consentire la condivisione di risorse specifiche

Puoi utilizzare una politica di autorizzazione IAM per limitare i responsabili ad associare solo risorse specifiche alle condivisioni di risorse.

Ad esempio, la seguente policy limita i responsabili a condividere solo la regola del resolver con l'Amazon Resource Name (ARN) specificato. L'operatore `StringEqualsIfExists` consente una richiesta se la richiesta non include un `ResourceArn` parametro o se include quel parametro, che il suo valore corrisponda esattamente all'ARN specificato.

Per ulteriori informazioni su quando e perché utilizzare `...IfExists` gli operatori, consulta... IfExistsoperatori di condizioni nella Guida per l'utente IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "StringEqualsIfExists": {
                "ram:ResourceArn": "arn:aws:route53resolver:us-
west-2:123456789012:resolver-rule/rslvr-rr-5328a0899aexample"
            }
        }
    }]
}
```

Esempio 2: consentire la condivisione di tipi di risorse specifici

Puoi utilizzare una policy IAM per limitare i responsabili ad associare solo tipi di risorse specifici alle condivisioni di risorse.

Ad esempio, la seguente politica limita i principati a condividere solo le regole del resolver.

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

```
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "StringEqualsIfExists": {
                "ram:RequestedResourceType": "route53resolver:ResolverRule"
            }
        }
    }]
}
```

Esempio 3: limita la condivisione con utenti esterni Account AWS

Puoi utilizzare una policy IAM per impedire ai responsabili di condividere risorse con Account AWS persone esterne all'AWSorganizzazione.

Ad esempio, la seguente politica IAM impedisce ai responsabili di aggiungere condivisioni Account AWS di risorse esterne.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": "ram:CreateResourceShare",
        "Resource": "*",
        "Condition": {
            "Bool": {
                "ram:RequestedAllowsExternalPrincipals": "false"
            }
        }
    }]
}
```

Esempi di politiche di controllo dei servizi per AWS Organizations e AWS RAM

AWS RAM supporta le politiche di controllo del servizio (SCPs). SCPssono politiche che allegate agli elementi di un'organizzazione per gestire le autorizzazioni all'interno di tale organizzazione. An SCP si applica a tutti gli elementi inclusi Account AWS nell'elemento a cui si allega il SCP. SCPsoffri il controllo centralizzato sulle autorizzazioni massime disponibili per tutti gli account della tua organizzazione. Possono aiutarvi a garantire che rispettiate le Account AWS linee guida per il

controllo degli accessi della vostra organizzazione. Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .

Prerequisiti

Per utilizzarloSCPs, devi prima fare quanto segue:

- Abilitazione di tutte le caratteristiche nell'organizzazione. Per ulteriori informazioni, vedere Abilitazione di tutte le funzionalità dell'organizzazione nella Guida AWS Organizations per l'utente
- Abilita SCPs per l'uso all'interno della tua organizzazione. Per ulteriori informazioni, vedere Abilitazione e disabilitazione dei tipi di policy nella Guida per l'AWS Organizations utente
- Crea quello SCPs che ti serve. Per ulteriori informazioni sulla creazioneSCPs, consulta Creazione e aggiornamento SCPs nella Guida AWS Organizations per l'utente.

Policy di controllo dei servizi di esempio

Indice

Di seguito sono riportati alcuni esempi che mostrano come controllare vari aspetti della condivisione delle risorse in un'organizzazione.

Esempio 1: Impedire la condivisione esterna

Quanto segue SCP impedisce agli utenti di creare condivisioni di risorse che consentano la condivisione con responsabili esterni all'organizzazione dell'utente che condivide.

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

```
                "ram:CreateResourceShare",
                "ram:UpdateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "ram:RequestedAllowsExternalPrincipals": "true"
                }
            }
        }
    ]
}
```

Esempio 2: impedire agli utenti di accettare inviti alla condivisione di risorse da account esterni all'organizzazione

Quanto segue SCP impedisce a qualsiasi responsabile di un account interessato di accettare un invito a utilizzare una condivisione di risorse. Le condivisioni di risorse condivise con altri account della stessa organizzazione dell'account di condivisione non generano inviti e pertanto non ne sono influenzate. SCP

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

Esempio 3: consentire ad account specifici di condividere tipi di risorse specifici

Quanto segue SCP consente solo gli account 111111111111 e la creazione 222222222222 di nuove condivisioni di risorse che condividono elenchi di EC2 prefissi Amazon o l'associazione di elenchi di prefissi a condivisioni di risorse esistenti.

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

```
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalAccount": [
                        "111111111111",
                        "222222222222"
                    ]
                },
                "StringEqualsIfExists": {
                    "ram:RequestedResourceType": "ec2:PrefixList"
                }
            }
        }
    ]
}
```

Esempio 4: impedire la condivisione con l'intera organizzazione o con le unità organizzative

Quanto segue SCP impedisce agli utenti di creare condivisioni di risorse che condividano risorse con un'intera organizzazione o con qualsiasi unità organizzativa. Gli utenti possono condividere con singoli Account AWS membri dell'organizzazione o con IAM ruoli o utenti.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ram:Principal": [
                        "arn:aws:organizations::*:organization/*",
                        "arn:aws:organizations::*:ou/*"
                    ]
```

```
                }
            }
        }
    ]
}
```

Esempio 5: consenti la condivisione solo con soggetti specifici

L'esempio seguente SCP consente agli utenti di condividere risorse solo con l'unità `o-12345abcdef, ou-98765fedcba` organizzativa dell'organizzazione e Account AWS `111111111111`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:AssociateResourceShare",
        "ram:CreateResourceShare"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ram:Principal": [
            "arn:aws:organizations::123456789012:organization/o-12345abcdef",
            "arn:aws:organizations::123456789012:ou/o-12345abcdef/ou-98765fedcba",
            "111111111111"
          ]
        },
        "Null": {
          "ram:Principal": "false"
        }
      }
    }
  ]
}
```

Disabilitazione della condivisione delle risorse con AWS Organizations

Se in precedenza hai abilitato la condivisione con AWS Organizations e non hai più bisogno di condividere le risorse con l'intera organizzazione o le unità organizzative (OU), puoi disabilitare la

condivisione. Quando si disabilita la condivisione conAWS Organizations, tutte le organizzazioni o le unità organizzative vengono rimosse dalle condivisioni di risorse create e perdono l'accesso alle risorse condivise. Gli account esterni (account aggiunti alla condivisione di risorse tramite invito) non subiranno alcun impatto e continueranno a essere associati alla condivisione di risorse.

Per disabilitare la condivisione con AWS Organizations

1. Disabilita l'accesso affidabile all'AWS Organizationsutilizzo del AWS Organizations disable-aws-service-accessAWS CLIcomando.

```
$  aws organizations disable-aws-service-access --service-principal
 ram.amazonaws.com
```

> **Important**
>
> Quando si disabilita l'accesso affidabile aAWS Organizations, i responsabili all'interno dell'organizzazione vengono rimossi da tutte le condivisioni di risorse e perdono l'accesso a tali risorse condivise.

2. Utilizza la console IAMAWS CLI, o le operazioni dell'API IAM per eliminare il ruolo collegato al AWSServiceRoleForResourceAccessManagerservizio. Per ulteriori informazioni, consultare Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Registrazione e monitoraggio AWS RAM

Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle AWS RAM AWS soluzioni esistenti. È necessario raccogliere i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica. AWS fornisce diversi strumenti per monitorare le AWS RAM risorse e rispondere a potenziali incidenti:

Amazon EventBridge

Fornisce un near-real-time flusso di eventi di sistema che descrivono i cambiamenti nelle AWS risorse. EventBridge abilita l'elaborazione automatizzata basata sugli eventi, poiché è possibile scrivere regole che controllano determinati eventi e attivano azioni automatiche in altri AWS servizi quando si verificano tali eventi. Per ulteriori informazioni, consulta Monitoraggio AWS RAM tramite EventBridge.

AWS CloudTrail

Cattura le API chiamate e gli eventi correlati effettuati da o per conto tuo Account AWS e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta Registrazione delle chiamate API AWS RAM con AWS CloudTrail.

Monitoraggio AWS RAM tramite EventBridge

Utilizzando Amazon EventBridge, puoi configurare notifiche automatiche per eventi specifici in AWS RAM. Gli eventi di AWS RAM vengono consegnati quasi EventBridge in tempo reale. È possibile EventBridge configurare il monitoraggio degli eventi e richiamare le destinazioni in risposta a eventi che indicano modifiche alle condivisioni di risorse. Le modifiche a una condivisione di risorse attivano eventi sia per il proprietario della condivisione di risorse che per i principali a cui è stato concesso l'accesso alla condivisione di risorse.

Quando si crea un modello di eventi, l'origine è `aws.ram`.

> **Note**
>
> Fai attenzione a scrivere codice che dipenda da questi eventi. Questi eventi non sono garantiti, ma vengono emessi con la massima diligenza possibile. Se si verifica un errore durante il AWS RAM tentativo di emettere un evento, il servizio riprova diverse volte. Tuttavia, può scadere e causare la perdita di quell'evento specifico.

Per ulteriori informazioni, consulta la Amazon EventBridge User Guide.

Esempio: avvisi in caso di errori di condivisione delle risorse

Prendi in considerazione lo scenario in cui desideri condividere le prenotazioni EC2 di capacità di Amazon con altri account della tua organizzazione. Ciò è un buon modo per ridurre i costi.

Tuttavia, se non si soddisfano tutti i prerequisiti per la condivisione di una prenotazione di capacità, è possibile che l'esecuzione delle attività asincrone relative alla condivisione delle risorse non venga eseguita automaticamente. Se l'operazione di condivisione fallisce e gli utenti di altri account tentano di avviare istanze con una di queste prenotazioni di capacità, Amazon si EC2 comporta come se

la prenotazione di capacità fosse piena e avvia invece l'istanza come istanza on demand. Ciò può comportare costi superiori al previsto.

Per monitorare gli errori di condivisione delle risorse, imposta una EventBridge regola Amazon che ti avvisa ogni volta che una condivisione di AWS RAM risorse fallisce. La seguente procedura del tutorial utilizza un argomento Amazon Simple Notification Service (SNS) per notificare a tutti gli abbonati all'argomento ogni volta che EventBridge rileva un errore di condivisione delle risorse. Per ulteriori informazioni su AmazonSNS, consulta la Amazon Simple Notification Service Developer Guide.

Per creare una regola che ti avvisi quando la condivisione delle risorse fallisce

1. Apri la EventBridge console Amazon.
2. Nel riquadro di navigazione, scegli Regole, quindi nell'elenco Regole scegli Crea regola.
3. Inserisci un nome e una descrizione facoltativa per la regola, quindi scegli Avanti.
4. Scorri verso il basso fino alla casella Modello di evento e scegli Modelli personalizzati (JSONeditor).
5. Copia e incolla il seguente schema di eventi:

```
{
  "source": ["aws.ram"],
  "detail-type": ["Resource Sharing State Change"],
  "detail": {
    "event": ["Resource Share Association"],
    "status": ["failed"]
  }
}
```

6. Scegli Next (Successivo).
7. Per Target 1, in Tipo di destinazione, scegli Servizio AWS.
8. In Seleziona un obiettivo, scegli l'SNSargomento.
9. Per Argomento, scegli l'SNSargomento in cui desideri pubblicare la notifica. Questo argomento deve già esistere.
10. Scegli Avanti, quindi scegli nuovamente Avanti per verificare la configurazione.
11. Quando sei soddisfatto delle opzioni a tua disposizione, scegli Crea regola.
12. Tornando alla pagina Regole, assicurati che la nuova regola sia contrassegnata come Abilitata. Se necessario, scegli il pulsante di opzione accanto al nome della regola, quindi scegli Abilita.

Finché la regola è abilitata, qualsiasi condivisione di AWS RAM risorse che fallisce genera un SNS avviso per i destinatari dell'argomento su cui hai pubblicato.

Puoi anche confermare che le prenotazioni di capacità condivisa sono accessibili agli account con cui le hai condivise provando a visualizzarle nella EC2 console Amazon da tali account.

Registrazione delle chiamate API AWS RAM con AWS CloudTrail

AWS RAMè integrato conAWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o unAWS servizio inAWS RAM. CloudTrail acquisisce tutte le chiamate APIAWS RAM come eventi. Le chiamate acquisite includono le chiamate dalla console di AWS RAM e le chiamate di codice alle operazioni delle API AWS RAM. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi in un bucket Amazon S3 includendo eventi perAWS RAM. Se non configuri un trail, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizza le informazioni raccolte da CloudTrail per determinare la richiesta effettuata a AWS RAM, l'indirizzo IP da cui è stata effettuata la richiesta, il richiedente, la data della richiesta e altri dettagli.

Per ulteriori informazioni CloudTrail, consultare la Guida per l'AWS CloudTrailutente.

AWS RAMinformazioni in CloudTrail

CloudTrail è abilitato sul tuo alAccount AWS momento della sua creazione. Quando si verifica un'attività inAWS RAM, questa viene registrata in un CloudTrail evento insieme ad altri eventi diAWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nell'Account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia CloudTrail eventi di.

Per una registrazione continua degli eventi nell'Account AWS che includa gli eventi per AWS RAM, crea un trail. Un trail consente di CloudTrail distribuire i file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altriAWS servizi per analizzare con maggiore dettaglio e usare i dati raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Creazione di un trail per il tuo Account AWS
- Servizio AWSintegrazioni con CloudTrail i log

- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail log da più Regioni e Ricezione di file di CloudTrail log da più account

TutteAWS RAM le azioni vengono registrate CloudTrail e documentate nell'AWS RAMAPI Reference. Ad esempio, le chiamate alle operazioni `CreateResourceShare`, `AssociateResourceShare` e `EnableSharingWithAwsOrganization` generano voci nei file di log CloudTrail.

Ogni evento o voce di log contiene informazioni che consentono di determinare chi ha effettuato la richiesta.

- Account AWSCredenziali root
- Credenziali di sicurezza temporanee fornite da un ruolo AWS Identity and Access Management (IAM) o un utente federato.
- Credenziali di sicurezza a lungo termine fornite da un utente IAM.
- Un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Comprensione delle voci dei file di log di AWS RAM

Un trail è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di log possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, data e ora dell'operazione, parametri della richiesta e così via. CloudTrail i file di log non sono una traccia di pila ordinata delle chiamate API pubbliche e di conseguenza non appaiono in base a un ordine specifico.

Nell'esempio seguente viene illustrata una voce di CloudTrail log per l'`CreateResourceShare`operazione.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "NOPIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/admin",
        "accountId": "111122223333",
```

```
        "accessKeyId": "BCDIOSFODNN7EXAMPLE",
        "userName": "admin"
    },
    "eventTime": "2018-11-03T04:23:19Z",
    "eventSource": "ram.amazonaws.com",
    "eventName": "CreateResourceShare",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.1.0",
    "userAgent": "aws-cli/1.16.2 Python/2.7.10 Darwin/16.7.0 botocore/1.11.2",
    "requestParameters": {
        "name": "foo"
    },
    "responseElements": {
        "resourceShare": {
            "allowExternalPrincipals": true,
            "name": "foo",
            "owningAccountId": "111122223333",
            "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
EXAMPLE0-1234-abcd-1212-987656789098",
            "status": "ACTIVE"
        }
    },
    "requestID": "EXAMPLE0-abcd-1234-mnop-987654567876",
    "eventID": "EXAMPLE0-1234-abcd-hijk-543234565434",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```


Resilienza in AWS RAM

L'infrastruttura globale di AWS è progettata attorno a Regioni AWS e zone di disponibilità. Regioni AWS fornisce più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e velocità effettiva elevata. Con le zone di disponibilità, è possibile progettare e gestire le applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, fault tolerant e scalabili rispetto alle infrastrutture a data center singolo o multiplo.

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

Sicurezza dell'infrastruttura in AWS RAM

In quanto servizio gestito, AWS Resource Access Manager 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.

Si utilizzano API chiamate AWS pubblicate per accedere tramite AWS RAM la rete. I client devono supportare quanto segue:

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

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

Accesso AWS Resource Access Manager utilizzando un endpoint di interfaccia (AWS PrivateLink)

È possibile utilizzare… AWS PrivateLink per creare una connessione privata tra il tuo VPC e AWS Resource Access Manager. Puoi accedere AWS RAM come se fosse nel tuoVPC, senza l'uso di un gateway Internet, un NAT dispositivo, VPN una connessione o AWS Direct Connect connessione. Le istanze del tuo VPC non hanno bisogno di indirizzi IP pubblici per accedere AWS RAM.

Questa connessione privata viene stabilita creando un endpoint di interfaccia, alimentato da AWS PrivateLink. Creiamo un'interfaccia di rete endpoint in ogni sottorete abilitata per l'endpoint dell'interfaccia. Si tratta di interfacce di rete gestite dal richiedente che fungono da punto di ingresso per il traffico destinato a AWS RAM.

Per ulteriori informazioni, vedere Access Servizi AWS attraverso AWS PrivateLink nella AWS PrivateLink guida.

Considerazioni per AWS RAM

Prima di configurare un endpoint di interfaccia per AWS RAM, consulta le considerazioni nella AWS PrivateLink Guida.

AWS RAM supporta l'effettuazione di chiamate a tutte API le sue azioni tramite l'endpoint dell'interfaccia.

VPCle politiche degli endpoint sono supportate per AWS RAM. Per impostazione predefinita, accesso completo a AWS RAM è consentito tramite l'endpoint dell'interfaccia.

Crea un endpoint di interfaccia per AWS RAM

È possibile creare un endpoint di interfaccia per AWS RAM utilizzando la VPC console Amazon o il AWS Command Line Interface (AWS CLI). Per ulteriori informazioni, consulta Creare un endpoint di interfaccia nel AWS PrivateLink Guida.

Crea un endpoint di interfaccia per AWS RAM utilizzando il seguente nome di servizio:

```
com.amazonaws.region.ram
```

Se si abilita la modalità privata DNS per l'endpoint dell'interfaccia, è possibile effettuare API richieste a AWS RAM utilizzando il DNS nome regionale predefinito. Ad esempio `ram.us-east-1.amazonaws.com`.

Creazione di una policy dell' endpoint per l'endpoint dell'interfaccia

Una policy per gli endpoint è una IAM risorsa che è possibile collegare a un endpoint di interfaccia. La policy predefinita per gli endpoint consente l'accesso completo a AWS RAM tramite l'endpoint dell'interfaccia. Per controllare l'accesso consentito a AWS RAM dal tuoVPC, allega una policy personalizzata per gli endpoint all'endpoint dell'interfaccia.

Una policy di endpoint specifica le informazioni riportate di seguito:

- I principi che possono eseguire azioni (Account AWS, IAM utenti e IAM ruoli).
- Le azioni che possono essere eseguite.
- Le risorse in cui è possibile eseguire le operazioni.

Per ulteriori informazioni, consulta Controllare l'accesso ai servizi utilizzando le policy degli endpoint nel AWS PrivateLink Guida.

Esempio: policy VPC sugli endpoint per AWS RAM actions

Di seguito è riportato l'esempio di una policy dell'endpoint personalizzata. Quando alleghi questa policy all'endpoint dell'interfaccia, concede l'accesso a quanto elencato AWS RAM azioni per tutti i committenti su tutte le risorse.

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

Risoluzione dei problemi con AWS RAM

Utilizza le informazioni contenute in questa sezione della guida per aiutarti a diagnosticare e risolvere i problemi più comuni quando lavori con AWS Resource Access Manager ().AWS RAM

Argomenti

Errore: «L'ID del tuo account non esiste in un' AWS organizzazione»

Scenario

Viene visualizzato l'errore "L'ID dell'account non esiste in un' AWS organizzazione" quando si tenta di condividere una risorsa con account o unità organizzative (OUs) dell'organizzazione.

Causa

Questo errore può verificarsi se il ruolo collegato al servizio AWSServiceRoleForResourceAccessManagernon viene creato correttamente quando si attiva l'integrazione tra e AWS Resource Access Manager . AWS Organizations

Soluzione

Per ricreare il ruolo collegato al servizio richiesto, esegui i seguenti passaggi per disattivare l'integrazione e riattivarla.

> **Important**
>
> Quando si disabilita l'accesso affidabile a AWS Organizations, i responsabili dell'organizzazione vengono rimossi da tutte le condivisioni di risorse e perdono l'accesso a tali risorse condivise.

1. Accedi al tuo account di gestione dell'organizzazione utilizzando un IAM ruolo o un utente con autorizzazioni amministrative.
2. Vai alla pagina Servizi nella AWS Organizations console.
3. Scegli RAM.
4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Vai alla pagina Impostazioni nella AWS RAM console.
6. Seleziona la casella Abilita condivisione con AWS Organizations, quindi scegli Salva impostazioni.

Ora dovresti essere in grado di utilizzare per AWS RAM condividere le tue risorse con gli account e OUs all'interno dell'organizzazione.

Errore: "AccessDeniedException»

Scenario

Viene visualizzata un'eccezione di accesso negato quando si tenta di condividere una risorsa o di visualizzare una condivisione di risorse.

Causa

È possibile ricevere questo errore se si tenta di creare una condivisione di risorse quando non si dispone delle autorizzazioni richieste. Ciò può essere causato da autorizzazioni insufficienti nelle politiche allegate al tuo AWS Identity and Access Management (IAM) principal. Può anche accadere a causa delle restrizioni imposte da una policy di controllo AWS Organizations del servizio (SCP) che influiscono su Account AWS.

Soluzione

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .
- Utenti gestiti IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate in Creare un ruolo per un provider di identità di terze parti (federazione) nella Guida per l'IAMutente.
- IAMutenti:
  - Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate in Creare un ruolo per un IAM utente nella Guida per l'IAMutente.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate in Aggiungere autorizzazioni a un utente (console) nella Guida per l'IAMutente.

Per risolvere l'errore, devi assicurarti che le autorizzazioni siano concesse mediante `Allow` dichiarazioni contenute nella politica di autorizzazione utilizzata dal responsabile che effettua la richiesta. Inoltre, le autorizzazioni non devono essere bloccate dall'organizzazione. SCPs

Per creare una condivisione di risorse, sono necessarie le due autorizzazioni seguenti:

- `ram:CreateResourceShare`

- `ram:AssociateResourceShare`

Per visualizzare una condivisione di risorse, è necessaria la seguente autorizzazione:

- `ram:GetResourceShares`

Per allegare le autorizzazioni a una condivisione di risorse, è necessaria la seguente autorizzazione:

- *`resourceOwningService`*`:`*`PutPolicyAction`*

  Si tratta di un segnaposto. È necessario sostituirlo con l'autorizzazione PutPolicy "" (o equivalente) del servizio proprietario della risorsa che si desidera condividere. Ad esempio, se condividi una regola del resolver Route 53, l'autorizzazione richiesta sarebbe:. `route53resolver:PutResolverRulePolicy` Se desideri consentire la creazione di una

condivisione di risorse che contenga più tipi di risorse, devi includere l'autorizzazione pertinente per ogni tipo di risorsa che desideri autorizzare.

L'esempio seguente mostra come potrebbe essere una politica di IAM autorizzazione di questo tipo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare",
                "ram:GetResourceShares",
                "resourceOwningService:PutPolicyAction"
            ],
            "Resource": "*"
        }
    ]
}
```

Errore: "UnknownResourceException»

Scenario

Viene visualizzato uno dei seguenti errori:

- «CannotCreateResourceShare UnknownResourceException: OrganizationalUnit o-*xxxx* non può essere trovato»
- "CannotUpdateResourceShare UnknownResourceException: OrganizationalUnit o-*xxxx* non può essere trovato».

Causa

Questi errori possono verificarsi se si abilita l'integrazione tra AWS RAM e AWS Organizations utilizzando la console Organizations o Organizations E nableAWSService Access API anziché utilizzando la AWS RAM console. Quando abiliti l'integrazione utilizzando la console Organizations o API il servizio non crea il `AWSServiceRoleForResourceAccessManager` ruolo nel tuo account.

Tale ruolo è necessario per accedere alle informazioni sulla tua organizzazione. Poiché il ruolo non è stato creato, non AWS RAM puoi accedere ai dettagli sugli account o sulle unità organizzative (OUs) dell'organizzazione.

Soluzione

Per risolvere il problema, disattiva l'integrazione tra AWS RAM e AWS Organizations. Quindi riaccendilo chiamando l' AWS RAM EnableSharingWithAwsOrganizationAPIoperazione o utilizzando il AWS Management Console per eseguire le seguenti operazioni.

> **Important**
>
> Quando si disabilita l'accesso affidabile a AWS Organizations, i responsabili dell'organizzazione vengono rimossi da tutte le condivisioni di risorse e perdono l'accesso a tali risorse condivise.

1. Accedi al tuo account di gestione dell'organizzazione utilizzando un IAM ruolo o un utente con autorizzazioni amministrative.
2. Vai alla pagina Servizi nella AWS Organizations console.
3. Scegli RAM.
4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Vai alla pagina Impostazioni nella AWS RAM console.
6. Seleziona la casella Abilita condivisione con AWS Organizations, quindi scegli Salva impostazioni.

Ora dovresti essere in grado di utilizzare per AWS RAM condividere le tue risorse con gli account e OUs all'interno dell'organizzazione.

Errori durante il tentativo di condivisione con account esterni alla mia organizzazione

Scenario

Quando si tenta di condividere risorse con account esterni all'organizzazione, si verifica uno dei seguenti errori:

- «Non è possibile condividere la risorsa all'esterno dell'organizzazione. »
- «La risorsa che stai tentando di condividere può essere condivisa solo all'interno della tua AWS organizzazione. »
- "InvalidParameterException: Il Principal Account-ID non è presente nell'organizzazione AWS . Non sei autorizzato ad aggiungere elementi esterni Account AWS a una condivisione di risorse. »
- "OperationNotPermittedException: La risorsa che stai tentando di condividere può essere condivisa solo all'interno della tua AWS organizzazione. »

Possibili cause e soluzioni

Alcuni tipi di risorse possono essere condivisi solo con account della stessa organizzazione

Alcuni tipi di risorse non possono essere condivisi con nessun account che non sia membro di tale organizzazione. Un tipo di risorsa di esempio con questa restrizione sono le connessioni private virtuali (VPCs) che fanno parte di Amazon Elastic Compute Cloud (AmazonEC2).

Per verificare se puoi condividere un particolare tipo di risorsa con account e responsabili esterni alla tua organizzazione, consulta Risorse condivisibili. AWS

Il ruolo collegato al servizio non è stato creato correttamente

Questo problema può verificarsi se il ruolo collegato al servizio non `AWSServiceRoleForResourceAccessManager` è stato creato correttamente quando è stata attivata l'integrazione tra e. AWS RAM AWS Organizations

Se ricevi uno di questi errori quando tenti di condividere una risorsa con un account che fa parte della tua organizzazione, esegui i seguenti passaggi per eliminare e ricreare il ruolo collegato al servizio.

> **Important**
>
> Quando disabiliti l'accesso affidabile a AWS Organizations, i responsabili all'interno dell'organizzazione vengono rimossi da tutte le condivisioni di risorse e perdono l'accesso a tali risorse condivise.

1. Accedi al tuo account di gestione dell'organizzazione utilizzando un IAM ruolo o un utente con autorizzazioni amministrative.

2. Vai alla pagina Servizi nella AWS Organizations console.
3. Scegli RAM.
4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Vai alla pagina Impostazioni nella AWS RAM console.
6. Seleziona la casella Abilita condivisione con AWS Organizations, quindi scegli Salva impostazioni.

Non riesco a visualizzare le risorse condivise nell'account di destinazione

Scenario

Gli utenti non possono vedere le risorse che ritengono siano condivise con loro da altri Account AWS.

Possibili cause e soluzioni

La condivisione con AWS Organizations è stata attivata utilizzando Organizations anziché AWS RAM

Se AWS Organizations è stata attivata utilizzando Organizations anziché AWS RAM, la condivisione all'interno dell'organizzazione non riesce. Per verificare se questa è la causa del problema, vai alla pagina Impostazioni nella AWS RAM console e verifica che la AWS Organizations casella di controllo Abilita condivisione con sia selezionata.

- Se la casella di controllo è selezionata, non è questa la causa.
- Se la casella di controllo non è selezionata, questa potrebbe essere la causa. Non selezionare ancora la casella di controllo. Effettuare le seguenti operazioni per correggere la situazione.

> **Important**
>
> Quando si disabilita l'accesso affidabile a AWS Organizations, i responsabili dell'organizzazione vengono rimossi da tutte le condivisioni di risorse e perdono l'accesso a tali risorse condivise.

1. Accedi al tuo account di gestione dell'organizzazione utilizzando un IAM ruolo o un utente con autorizzazioni amministrative.
2. Vai alla pagina Servizi nella AWS Organizations console.
3. Scegli RAM.
4. Scegli Disable trusted access (Disabilita accesso attendibile).
5. Vai alla pagina Impostazioni nella AWS RAM console.
6. Seleziona la casella Abilita condivisione con AWS Organizations, quindi scegli Salva impostazioni.

Potrebbe essere necessario aggiornare la condivisione e specificare gli account o le unità organizzative all'interno dell'organizzazione con cui condividere.

La condivisione di risorse non specifica questo account come principale

Nella cartella Account AWS che ha creato la condivisione di risorse, visualizza la condivisione di risorse nella AWS RAM console. Verifica che l'account che non può accedere alle risorse sia elencato come Principal. In caso contrario, aggiorna la condivisione per aggiungere l'account come principale.

Il ruolo o l'utente dell'account non dispone delle autorizzazioni minime richieste

Quando condividi una risorsa dell'account A con un altro account B, i ruoli e gli utenti dell'account B non ottengono automaticamente l'accesso alle risorse della condivisione. L'amministratore dell'account B deve prima concedere l'autorizzazione ai IAM ruoli e agli utenti dell'account B che devono accedere alla risorsa. Ad esempio, la seguente politica mostra come concedere l'accesso in sola lettura a ruoli e utenti nell'account B per una risorsa dall'account A. La politica specifica la risorsa in base al suo Amazon Resource Name (). ARN

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ram:Get*",
                "ram:List*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:<service>:<Region-code>:<Account-A-ID>:<resource-id>"
```

```
        }
    ]
}
```

L'impostazione della risorsa è diversa da Regione AWS quella corrente della console

AWS RAM è un servizio regionale. Le risorse esistono in una regione specifica Regione AWS e per visualizzarle AWS Management Console devono essere configurate in modo da visualizzare le risorse in quella regione.

Le Regione AWS informazioni a cui la console sta attualmente accedendo vengono visualizzate nell'angolo superiore destro della console. Per cambiarlo, scegli il nome della regione corrente e dal menu a discesa, scegli la regione di cui vuoi vedere le risorse.

Errore: limite superato

Scenario

Quando provi a condividere risorse, ricevi "Hai raggiunto il numero massimo di risorse che puoi condividere ResourceShareLimitExceededException" o "".

Causa

Questi errori si verificano quando raggiungi il numero massimo di risorse che puoi condividere utilizzando il AWS RAM servizio o chi ha creato la risorsa Servizio AWS che stai cercando di condividere. Questa quota (precedentemente denominata limite) può influire sia sull'account di condivisione che sull'account con cui condividi la risorsa.

Soluzione

1. Per visualizzare le quote, nella pagina in Account AWS cui vedi l'errore, accedi a una delle seguenti pagine, a seconda del tipo di quota che stai raggiungendo:
   - La AWS RAM pagina nella console Service Quotas
   - La pagina per le Servizio AWS cui risorse sono interessate dalla quota
2. Scorri verso il basso e scegli la quota pertinente.
3. Se è disponibile per questa quota, scegli Richiedi un aumento della quota.
4. Inserisci un nuovo valore per la quota, quindi scegli Richiedi.

5. La richiesta viene visualizzata nella pagina della cronologia delle richieste di quota, dove puoi controllare lo stato della richiesta fino al suo completamento.

L'altro account della mia organizzazione non riceve mai un invito

Scenario

Quando condividi risorse con un altro account della stessa organizzazione gestita da AWS Organizations, questi non ricevono inviti.

Causa

Questo è un comportamento previsto se sul tuo account è attivata la condivisione all'interno AWS dell'organizzazione.

Quando questa opzione è attivata e la condividi con un altro account dell'organizzazione, non vengono inviati inviti né è richiesta l'accettazione. Tutti gli account dell'organizzazione a cui fai riferimento come responsabili nella condivisione delle risorse possono iniziare immediatamente ad accedere alle risorse della condivisione.

Se il tuo account non ha attivato la condivisione all'interno AWS dell'organizzazione, quando condividi con altri account, anche se fanno parte della stessa AWS organizzazione, questi vengono considerati account autonomi. Gli inviti vengono inviati e devono essere accettati prima che gli utenti possano accedere alle risorse delle condivisioni.

Non puoi condividere una VPC sottorete

Scenario

Quando si tenta di AWS RAM condividere una VPC sottorete con un altro account, l'operazione di condivisione ha esito positivo. Tuttavia, l'account utente viene visualizzato `LIMIT EXCEEDED` per quella risorsa nella AWS RAM console.

Causa

Alcuni tipi di risorse individuali prevedono restrizioni specifiche del servizio distinte dalle restrizioni applicate da. AWS RAM Alcune di queste restrizioni possono impedire efficacemente la condivisione anche se non hai raggiunto una delle restrizioni previste. AWS RAM I limiti sono un esempio di

queste restrizioni. Amazon Virtual Private Cloud (AmazonVPC) limita il numero di sottoreti che puoi condividere con un altro account individuale. Se provi a condividere una sottorete con un account utente che contiene già il numero massimo di sottoreti, gli account di consumo vengono visualizzati `LIMIT EXCEEDED` nella console per quella risorsa. Per ulteriori informazioni su questo limite, consulta Amazon VPC Quotas — VPC sharing in the Amazon Virtual Private Cloud User Guide.

Per risolvere questo problema, verifica innanzitutto la presenza di altre condivisioni di risorse che potrebbero condividere la risorsa specificata con l'account interessato e rimuovi quelle condivisioni che potrebbero non essere più necessarie. Puoi anche richiedere un aumento di un limite che supporti la regolazione. Utilizza la console Service Quotas per richiedere un aumento del limite.

> **Note**
>
> AWS RAM non rileva automaticamente le modifiche all'aumento del limite. È necessario riassociare la risorsa o il principale alla condivisione di risorse per RAM rilevare la modifica.

Service Quotas per AWS RAM

Hai i Account AWS seguenti limiti relativi a AWS Resource Access Manager (AWS RAM). Puoi richiedere un aumento di alcuni di questi limiti. Per richiedere un aumento del limite, contatta Support.

Note

Le seguenti definizioni si applicano alla descrizione nelle quote seguenti:

- Risorsa: un elemento Servizio AWS creato individualmente che desideri condividere, come un bucket Amazon S3 o un'istanza Amazon EC2. Ogni risorsa a cui si fa riferimento in una condivisione di risorse viene conteggiata come una risorsa rispetto a questa quota. Se condividi la stessa risorsa in tre diverse condivisioni di risorse, il conteggio per questa quota aumenta di tre.
- Condivisione delle risorse: un contenitore AWS RAM creato che è possibile utilizzare per condividere risorse. Ogni condivisione di risorse, indipendentemente dal numero di risorse che contiene, viene conteggiata come una sola unità rispetto alla quota.
- Principal condiviso: un identificatore che hai associato a una condivisione di risorse. Può trattarsi di un ruolo o utente AWS Identity and Access Management (IAM), di un Account AWS identificatore, di un'unità organizzativa o di un'intera organizzazione. Ogni principio condiviso a cui fai riferimento in una condivisione di risorse ne aggiunge uno all'utilizzo della quota. Se condividi con un'intera organizzazione facendo riferimento al relativo ID, questo viene conteggiato come uno solo rispetto a questa quota.
- Autorizzazioni gestite dai clienti: autorizzazioni gestite che crei per affrontare casi d'uso specifici utilizzando l'accesso con privilegi minimi per gestire l'utilizzo delle risorse condivise.

Risorsa	Limite predefinito
Numero massimo di condivisioni di risorse per Regione AWS	25.000
Numero massimo di associazioni di risorse per condivisione di risorse	5.000

Risorsa	Limite predefinito
Numero massimo di associazioni principali per condivisione di risorse	5.000
Numero massimo di autorizzazioni gestite dal cliente	1.500
Numero massimo di autorizzazioni gestite dal cliente per tipo di risorsa	10
Numero massimo di versioni per autorizzazione gestita dal cliente	5
Numero massimo di associazioni di risorse in tutte le condivisioni di risorse in un Regione AWS **Note** Ogni risorsa inclusa in una condivisione di risorse viene conteggiata ai fini di questo limite. Se una risorsa è inclusa in 10 diverse condivisioni di risorse, ne vengono conteggiate 10 rispetto al limite.	25.000

Risorsa	Limite predefinito
Numero massimo di associazioni principali in tutte le condivisioni di risorse in un Regione AWS **Note** Ogni committente incluso in una condivisione di risorse viene conteggiato ai fini di questo limite. Se un capitale è incluso in 10 diverse quote di risorse, ne vengono conteggiati 10 rispetto al limite.	25.000
Numero massimo di inviti in sospeso per account di condivisione • Questa quota si applica solo all'invio di account che condividono con account che non fanno parte dello stessoAWS Organizations. • Non esiste una quota per limitare il numero di inviti in sospeso che può avere un account ricevente. • Gli inviti non vengono utilizzati durante la condivisione tra account che fanno parte dello stesso AWS Organizations e hai attivato la condivisione delle risorse all'interno delAWS Organizations.	250

Utilizzo di AWS RAM con un SDK AWS

I Software Development Kit (SDK) di AWS sono disponibili per molti dei 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 for C++	Esempi di codice AWS SDK for C++
AWS SDK for Go	Esempi di codice AWS SDK for Go
AWS SDK for Java	Esempi di codice AWS SDK for Java
AWS SDK for JavaScript	Esempi di codice AWS SDK for JavaScript
AWS SDK for .NET	Esempi di codice AWS SDK for .NET
AWS SDK for PHP	Esempi di codice AWS SDK for PHP
AWS SDK for Python (Boto3)	Esempi di codice AWS SDK for Python (Boto3)
AWS SDK for Ruby	Esempi di codice AWS SDK for Ruby

Disponibilità di esempi

Non riesci a trovare quello che ti serve? Richiedi un esempio di codice con il link di feedback.

Cronologia dei documenti per la Guida per AWS RAM l'utente

La tabella seguente descrive importanti aggiunte alla documentazione. AWS Resource Access Manager Inoltre, aggiorniamo la documentazione per rispondere al feedback che ci inviate.

Per ricevere notifiche su questi aggiornamenti, puoi iscriverti al AWS RAM RSS feed.

Modifica	Descrizione	Data
È stato aggiunto il supporto per la condivisione di AWS Billing risorse.	Ora puoi condividere le AWS Billing visualizzazioni con altri membri Account AWS della tua organizzazione.	20 dicembre 2024
È stato aggiunto il supporto per la condivisione delle risorse Amazon API Gateway.	Ora puoi condividere i nomi di dominio API Gateway con altri Account AWS o all'interno della tua organizzazione.	21 novembre 2024
È stato aggiunto il supporto per la condivisione di VPC risorse Amazon.	Ora puoi condividere i gruppi VPC di Amazon Security con altri Account AWS o all'interno della tua organizzazione.	30 ottobre 2024
È stato aggiunto il supporto per la condivisione di AWS End User Messaging SMS risorse.	Puoi condividere AWS End User Messaging SMS risorse con altri Account AWS o con le tue organizzazioni AWS RAM.	24 settembre 2024
AWS PrivateLink	Con AWS PrivateLink for AWS RAM, puoi connetterti direttamente RAM utilizzan do un endpoint di interfaccia nel tuo cloud privato virtuale ()VPC.	9 settembre 2024

È stato aggiunto il supporto per la condivisione AWS Backup.	È possibile condividere casseforti logicamente isolati all'interno dell'organizzazione Account AWS o all'interno di essa.	7 agosto 2024
Aggiunto il supporto per la condivisione di modelli Amazon Bedrock Custom	Ora puoi utilizzarli AWS RAM per condividere i modelli personalizzati di Amazon Bedrock con altri Account AWS e con la tua organizza zione.	1° agosto 2024
È stato aggiunto il supporto per la condivisione dei AWS CloudHSM backup.	Puoi condividere i AWS CloudHSM backup con altri Account AWS o con le tue organizzazioni. AWS RAM	28 giugno 2024
Aggiunto il supporto per condividere Amazon SageMaker AI Model Registry risorse.	Ora puoi condividere parametri avanzati in modo sicuro ed efficiente all'interno Account AWS o all'interno della tua organizzazione.	27 giugno 2024
È stato aggiunto il supporto per condividere Amazon SageMaker AI JumpStart.	Ora puoi condividere Amazon SageMaker AI JumpStart Hubs con Account AWS o all'interno della tua organizza zione.	27 giugno 2024
È stato aggiunto il supporto per la condivisione Amazon Route 53 ResolverProfiles.	Ora puoi usare AWS RAM per condividere Amazon Route 53 Resolver Profiles con altri Account AWS membri della tua organizzazione.	22 aprile 2024

È stato aggiunto il supporto per condividere le risorse di AWS Systems Manager Parameter Store.	Ora puoi condividere parametri avanzati in modo sicuro ed efficiente all'interno della tua organizzazione Account AWS o all'interno di essa.	21 febbraio 2024
È stato aggiunto il supporto per condividere Amazon FSx for Open ZFS Snapshots.	Ora puoi condividere Amazon FSx for Open ZFS Snapshots con altri membri Account AWS della tua organizzazione.	19 dicembre 2023
È stato aggiunto il supporto per la condivisione Amazon Simple Storage Service delle risorse.	Ora puoi condividere Amazon Simple Storage Service l'istanza di Access Grants con altri utenti Account AWS o con AWS RAM la tua organizza zione.	27 novembre 2023
È stato aggiunto il supporto per condividere le Esploratore di risorse AWS visualizzazioni.	Ora puoi condividere le Esploratore di risorse AWS visualizzazioni con altri membri Account AWS della tua organizzazione.	14 novembre 2023
È stato aggiunto il supporto per condividere le risorse di Amazon Application Recovery Controller (ARC).	Ora puoi condividere i cluster Amazon Application Recovery Controller (ARC) con altri Account AWS o con AWS RAM la tua organizzazione.	18 ottobre 2023
È stato aggiunto il supporto per condividere DataZone le risorse di Amazon.	Ora puoi condividere DataZone le risorse di Amazon con altri Account AWS o con la tua organizzazione.	4 ottobre 2023

È stato aggiunto il supporto per la condivisione dei principali servizi.	È ora possibile associare i principali di servizio alle condivisioni di risorse. Ciò consente a servizi specifici di gestire le azioni necessarie per le risorse dei clienti per tuo conto.	29 agosto 2023
È stato aggiunto il supporto per condividere le risorse della SageMaker Model Card.	Ora puoi condividere le risorse SageMaker Model Card con altri Account AWS o con la tua organizzazione.	18 agosto 2023
È stato aggiunto il supporto per i gruppi di funzionalità di Amazon SageMaker AI Feature Store e SageMaker AI Catalog come risorse condivisibili.	Ora puoi condividere i gruppi di funzionalità di Amazon SageMaker AI Feature Store e le risorse di SageMaker AI Catalog con altri Account AWS o con la tua organizzazione.	20 luglio 2023
Aumento del limite della quota di servizio per gli inviti in sospeso.	Il numero massimo di inviti in sospeso per account di condivisione è stato aumentato da 20 a 250.	8 giugno 2023
È stato aggiunto il supporto per AWS AppSync GraphQL APIs come risorse condivisibili.	Ora puoi condividere AWS AppSync GraphQL APIs con altri Account AWS con. AWS RAM	24 maggio 2023
È stato aggiunto il supporto per Accesso verificato da AWS i gruppi come risorse condivisibili.	Ora puoi creare e gestire Accesso verificato da AWS gruppi centralmente e poi condividerli con altri Account AWS o con la tua organizzazione.	27 aprile 2023

È stato aggiunto il supporto per l'autorizzazione gestita dal cliente nella AWS RAM console.	Ora puoi creare e gestire in modo sicuro controlli granulari di accesso alle risorse per i tipi di risorse supportati.	19 aprile 2023
È stato aggiunto il supporto per il servizio Amazon VPC Lattice e le risorse condivisibili della rete di servizi.	Ora puoi condividere il servizio Amazon VPC Lattice e le risorse della rete di assistenza con altri Account AWS.	31 marzo 2023
È stato aggiunto il supporto per le entità Marketplace AWS del catalogo come risorse condivisibili.	Ora puoi condividere le tue entità con altri utenti Account AWS nel Marketplace.	27 marzo 2023
È stato aggiunto il supporto per la gestione delle versioni di autorizzazione nella AWS RAM console.	È ora possibile utilizzare la AWS RAM console per visualizzare i dettagli della versione e aggiornare le autorizzazioni in base alla versione designata come predefinita.	16 gennaio 2023
IAMaggiornamento delle migliori pratiche.	Guida aggiornata per allinears i alle IAM migliori pratiche. Per ulteriori informazioni, consulta le migliori pratiche di sicurezza in IAM.	3 gennaio 2023
È stato aggiunto il supporto per i gruppi di EC2 collocamento Amazon come risorse condivisibili.	Ora puoi condividere i gruppi di EC2 collocamento Amazon con altri utenti in Account AWS cui lanciare le loro istanze.	8 novembre 2022

Sono stati aggiunti collegamenti a due video introduttivi su. AWS RAM	Sono stati aggiunti video di panoramica che descrivono AWS RAM e forniscono una guida dettagliata alla condivisione di una risorsa con altri. Account AWS	29 agosto 2022
È stato aggiunto il supporto per le pipeline di Amazon SageMaker AI.	Ora puoi condividere le pipeline di SageMaker intelligenza artificiale con altri. Account AWS	2 agosto 2022
È stato aggiunto il supporto per AWS Service Catalog AppRegistry applicazioni e gruppi di attributi come tipi di risorse condivisibili.	È ora possibile condividere AppRegistry applicazioni e gruppi di attributi con altri Account AWS.	17 giugno 2022
AWS Resource Access Manager ricevute SOC e ISO certificazioni.	AWS RAM è stato convalidato come conforme agli standard Service Organization Control (SOC) e International Organization for Standardization (ISO) ISO 9001, ISO 27001, 27017, 27018 e 27701. ISO ISO ISO	31 maggio 2022
AWS Resource Access Manager riceve la certificazione Fed. RAMP	AWS RAM è stato convalidato come conforme al Federal Risk and Authorization Management Program (Fed). RAMP	8 aprile 2022
AWS Resource Access Manager riceve la certificazione. PCI DSS	AWS RAM è stato convalidato come conforme al Payment Card Industry (PCI) Data Security Standard (). DSS	27 febbraio 2022

È stato aggiunto il supporto per la scoperta di VPC IPAM risorse Amazon come risorse condivisibili. Inoltre, ora puoi condividere i IPAM pool con account esterni all'organ izzazione.	Ora puoi condividere le scoperte di IPAM risorse con altri Account AWS.	25 gennaio 2022
È stato aggiunto il supporto per la condivisione di risorse globali	Ora puoi condividere risorse globali con altri Account AWS.	2 dicembre 2021
È stato aggiunto il supporto per le reti WAN principali AWS Cloud come risorse globali condivisibili.	Ora puoi condividere le reti WAN principali di Cloud con altri Account AWS.	2 dicembre 2021
Supporto per la condivisione dei pool di Amazon VPC IP Address Manager (IPAM)	Puoi usarlo AWS RAM per condividere i VPC IPAM pool Amazon. Per ulteriori informazi oni, consulta AWS Risorse condivisibili nella Guida per l'AWS RAM utente.	1° dicembre 2021
Support per la condivisione di risorse Amazon SageMaker AI	Puoi usarlo AWS RAM per condividere gruppi di discendenza dell' SageMaker IA. Per ulteriori informazi oni, consulta AWS Risorse condivisibili nella Guida per l'AWS RAM utente.	30 novembre 2021

Support per la condivisione delle risorse di AWS Migration Hub Refactor Spaces	È possibile utilizzarlo AWS RAM per condividere ambienti Migration Hub. Per ulteriori informazioni, consulta AWS Risorse condivisibili nella Guida per l'AWS RAM utente.	29 novembre 2021
Sono state aggiunte informazioni sulle politiche AWS RAMAWS di IAM autorizzazione gestite.	Sono stati pubblicati dettagli sulle politiche di autorizzazione AWS gestite disponibili a cui puoi accedere dalla IAM console e allegare ai IAM principali del tuo. Account AWS	16 settembre 2021
Aggiunto il supporto per la condivisione di S3 sulle risorse Outposts	Ora puoi usarlo AWS RAM per condividere S3 su Outposts con altri. Account AWS	5 agosto 2021
È stato aggiunto il supporto per autorizzazioni gestite aggiuntive e la condivisione di risorse con i responsabili IAM	Per i tipi di risorse supportati, puoi scegliere tra autorizzazioni AWS RAM gestite aggiuntive e condividere risorse con singoli IAM ruoli e utenti.	10 giugno 2021
Aggiunto il supporto per la condivisione delle risorse AWS di Systems Manager Incident Manager	È ora possibile utilizzarlo AWS RAM per condividere AWS i contatti e i piani di risposta di Systems Manager Incident Manager con altri Account AWS.	10 maggio 2021

È stato aggiunto il supporto per la condivisione di risorse Amazon Route 53	Ora puoi usare AWS RAM per condividere i gruppi di regole di Amazon Route 53 Resolver DNS Firewall con altri. Account AWS	31 marzo 2021
È stato aggiunto il supporto per la condivisione di risorse AWS Transit Gateway	Ora puoi utilizzarli AWS RAM per condividere i domini multicast del gateway di transito con altri. Account AWS	10 dicembre 2020
È stato aggiunto il supporto per la condivisione delle risorse AWS Network Firewall	Ora puoi utilizzarlo AWS RAM per condividere le politiche AWS Network Firewall del firewall e i gruppi di regole con altri Account AWS.	17 novembre 2020
Aggiunto il supporto per la condivisione per Outposts e le tabelle di routing del gateway locale	Ora puoi usare AWS RAM per condividere Outposts e tabelle di routing del gateway locale con altri. Account AWS	15 ottobre 2020
È stato aggiunto il supporto per la condivisione dei log delle query di Route 53	È ora possibile utilizzarli AWS RAM per condividere i log delle query di Route 53 con altri. Account AWS	7 settembre 2020
È stato aggiunto il supporto per la condivisione AWS Private Certificate Authority delle risorse.	Ora puoi usare AWS RAM per condividere le autorità di certificazione CA privata AWS private (CAs) con altri Account AWS.	17 agosto 2020
È stato aggiunto il supporto per AWS la condivisione di cataloghi di dati, database e tabelle di Glue.	Ora puoi usare AWS RAM per condividere cataloghi di dati, database e tabelle di AWS Glue con altri Account AWS.	7 luglio 2020

È stato aggiunto il supporto per la condivisione degli elenchi di VPC prefissi Amazon.	Ora puoi utilizzarlo AWS RAM per condividere elenchi di prefissi.	29 giugno 2020
È stato aggiunto il supporto per la condivisione degli indirizzi di AWS Outposts proprietà dei clientiIPv4.	Ora puoi utilizzarlo AWS RAM per condividere gli indirizzi di AWS Outposts proprietà del cliente con altriIPv4. Account AWS	22 aprile 2020
È stato aggiunto il supporto per la condivisione di mesh AWS App Mesh	Ora puoi usare AWS RAM per condividere le mesh con altri. Account AWS	17 gennaio 2020
È stato aggiunto il supporto per la condivisione di AWS CodeBuild progetti e gruppi di report	Ora puoi AWS RAM utilizzar lo per condividere AWS CodeBuild progetti e gruppi di report con altri Account AWS.	13 dicembre 2019
È stato aggiunto il supporto per la condivisione di risorse aggiuntive	Ora puoi AWS RAM usare Amazon EC2 Dedicated Hosts, gruppi di AWS Resource Groups risorse e componenti, immagini e ricette di immagini di Amazon EC2 Image Builder con altri. Account AWS	2 dicembre 2019
È stato aggiunto il supporto per la condivisione delle prenotazioni di capacità su richiesta	Ora puoi utilizzarle AWS RAM per condividere le prenotazi oni di capacità su richiesta con altri. Account AWS	29 luglio 2019
Aggiunto il supporto per la condivisione dei cluster Aurora DB	Ora puoi usare AWS RAM per condividere i cluster Aurora DB con altri. Account AWS	2 luglio 2019

È stato aggiunto il supporto per la condivisione degli obiettivi di Traffic Mirroring	Ora puoi utilizzarli AWS RAM per condividere gli obiettivi di Traffic Mirroring con altri. Account AWS	25 giugno 2019
È stato aggiunto il supporto per la condivisione delle configurazioni delle licenze	È ora possibile utilizzare AWS RAM per condividere le configurazioni di AWS licenza del License Manager con altri Account AWS.	5 dicembre 2018
È stato aggiunto il supporto per la condivisione di sottoreti	Ora puoi usare AWS RAM per condividere le VPC sottoreti Amazon con altri. Account AWS	27 novembre 2018
È stato aggiunto il supporto per la condivisione dei gateway di transito	Ora puoi usare AWS RAM per condividere i gateway di VPC transito Amazon con altri Account AWS.	26 novembre 2018
È stato aggiunto il supporto per la condivisione delle regole Resolver	Ora puoi usare AWS RAM per condividere le regole di Route 53 Resolver con altri. Account AWS	20 novembre 2018

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.