



Guida per l'utente

AWS Resource Access Manager



AWS Resource Access Manager: Guida per l'utente

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Che cos'è AWS RAM?	1
Panoramiche video	1
Vantaggi di AWS RAM	2
Che dire dell'accesso tra più account con politiche basate sulle risorse?	2
Come funziona la condivisione delle risorse	3
Condivisione delle risorse	3
Utilizzo di risorse condivise	4
Accedendo AWS RAM	5
Prezzi per AWS RAM	6
Conformità e standard internazionali	6
PCI DSS	6
FedRAMP	6
SOC e ISO	7
Nozioni di base	8
Termini e concetti	8
Condivisione delle risorse	8
Account di condivisione	9
Principi di consumo	9
Politica basata sulle risorse	11
Autorizzazioni gestite	16
Versione con autorizzazione gestita	17
Condivisione delle tue risorse	18
Abilita la condivisione delle risorse all'interno AWS Organizations	18
Creare una condivisione di risorse	21
Utilizzo di risorse condivise	30
Rispondi all'invito alla condivisione delle risorse	31
Usa le risorse condivise con te	33
Utilizzo delle risorse condivise	34
Risorse regionali e globali	34
Quali sono le differenze tra risorse regionali e globali?	35
Condivisioni di risorse e relative regioni	36
Risorse di tua proprietà	37
Visualizzazione delle condivisioni di risorse create	38
Creazione di una condivisione di risorse	40

Aggiornamento di una condivisione di risorse	50
Visualizzazione delle risorse condivise	57
Visualizzazione dei principali con cui condividi	59
Eliminazione di una condivisione di risorse	61
Risorse condivise con te	63
Accettazione e rifiuto degli inviti	63
Visualizzazione delle condivisioni di risorse condivise con te	67
Visualizzazione delle risorse condivise con te	69
Visualizza i principali che condividono con te	71
Lasciare una condivisione di risorse	72
Zona di disponibilità IDs	75
Risorse condivisibili	79
AWS App Mesh	80
AWS AppSync API GraphQL	81
Gateway Amazon API	82
Amazon Application Recovery Controller (ARC)	83
Amazon Aurora	85
AWS Backup	86
Amazon Bedrock	87
Gestione di costi e fatturazione	88
AWS Billing Visualizza servizio	90
AWS Cloud Map	91
AWS WAN cloud	92
Amazon CloudFront	93
AWS CloudHSM	94
AWS CodeBuild	95
AWS CodeConnections	97
Amazon DataZone	98
Amazon EC2	99
EC2 Image Builder	105
Elastic Load Balancing	108
AWS End User Messaging SMS	110
Amazon FSx per OpenZFS	113
AWS Glue	115
AWS License Manager	118
Marketplace AWS	119

AWS Migration Hub Refactor Spaces	119
Approvazione multiparte	121
AWS Network Firewall	122
Oracle Database@AWS	124
AWS Outposts	127
Amazon S3 su Outposts	129
AWS Autorità di certificazione privata	130
Esploratore di risorse AWS	131
AWS Resource Groups	132
Amazon Route 53	133
Amazon Simple Storage Service	137
Amazon SageMaker AI	138
AWS Service Catalog AppRegistry	148
Strumento di gestione degli incidenti AWS Systems Manager	150
AWS Systems Manager	154
Amazon VPC	157
Amazon VPC Lattice	169
Gestione delle autorizzazioni in AWS RAM	173
Visualizzazione delle autorizzazioni gestite	174
Creazione e utilizzo di autorizzazioni gestite dal cliente	179
Crea un'autorizzazione gestita dal cliente	180
Crea una nuova versione di un'autorizzazione gestita dal cliente	181
Scegli una versione diversa come impostazione predefinita per un'autorizzazione gestita dal cliente	183
Eliminare una versione di autorizzazione gestita dal cliente	185
Eliminare un'autorizzazione gestita dal cliente	186
Aggiornamento delle versioni con autorizzazioni gestite	188
Considerazioni sulle autorizzazioni gestite dal cliente	190
Come funzionano le autorizzazioni gestite	191
Tipi di autorizzazioni gestite	192
Sicurezza	195
Protezione dei dati	196
Identity and Access Management	197
Come AWS RAM funziona con IAM	197
AWS politiche gestite	201
Uso di ruoli collegati ai servizi	206

Policy IAM di esempio	208
Esempio SCPs	211
Disattiva la condivisione con Organizations	216
Registrazione di log e monitoraggio	217
Monitoraggio utilizzando EventBridge	218
Registrazione delle chiamate AWS RAM API con AWS CloudTrail	220
Convalida della conformità	222
Resilienza	222
Sicurezza dell'infrastruttura	223
AWS PrivateLink	223
Considerazioni	224
Creazione di un endpoint di interfaccia	224
Creazione di una policy dell'endpoint	224
Risoluzione dei problemi	226
Errore: l'ID dell'account non esiste	226
Scenario	226
Causa	226
Soluzione	226
Errore: eccezione di accesso negato	227
Scenario	227
Causa	227
Soluzione	227
Errore: eccezione per una risorsa sconosciuta	229
Scenario	229
Causa	229
Soluzione	230
Errore: la condivisione all'esterno di un'organizzazione non è consentita	231
Scenario	231
Possibili cause e soluzioni	231
Errore: impossibile visualizzare le risorse condivise	232
Scenario	232
Possibili cause e soluzioni	232
Errore: eccezione del limite superato	234
Scenario	234
Causa	234
Soluzione	235

Nessun invito ricevuto	235
Scenario	235
Causa	235
Impossibile condividere un VPC	236
Scenario	236
Causa	236
Quote del servizio	237
Utilizzando il AWS SDKs	240
Cronologia dei documenti	241
.....	ccliv

Che cos'è AWS Resource Access Manager?

AWS Resource Access Manager (AWS RAM) consente di condividere in modo sicuro le risorse tra Account AWS, all'interno dell'organizzazione o delle unità organizzative (OUs) e con ruoli e utenti AWS Identity and Access Management (IAM) per i tipi di risorse supportati. Se ne hai più Account AWS, puoi creare una risorsa una sola volta e AWS RAM utilizzarla per renderla utilizzabile dagli altri account. Se il tuo account è gestito da AWS Organizations, puoi condividere le risorse con tutti gli altri account dell'organizzazione o solo con gli account contenuti in una o più unità organizzative specificate (OUs). Puoi anche condividere con ID specifici Account AWS per account, indipendentemente dal fatto che l'account faccia parte di un'organizzazione. [Alcuni tipi di risorse supportati](#) consentono inoltre di condividerli con ruoli e utenti IAM specifici.

Indice

- [Panoramiche video](#)
- [Vantaggi di AWS RAM](#)
- [Come funziona la condivisione delle risorse](#)
- [Accedendo AWS RAM](#)
- [Prezzi per AWS RAM](#)
- [Conformità e standard internazionali](#)

Panoramiche video

Il video seguente fornisce una breve introduzione AWS RAM e descrive come creare una condivisione di risorse. Per ulteriori informazioni, consulta [???](#).

Il video seguente mostra come applicare le autorizzazioni AWS gestite alle AWS risorse. Per ulteriori informazioni, consulta [???](#).

Questo video dimostra come creare e associare le autorizzazioni gestite dai clienti seguendo la best practice del privilegio minimo. Per ulteriori informazioni, consultare [???](#).

Vantaggi di AWS RAM

Perché usare AWS RAM? Offre i seguenti vantaggi:

- **Riduce i costi operativi:** crea una risorsa una sola volta e poi AWS RAM usala 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 politiche di autorizzazione basate 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 creassi risorse duplicate in tutti i tuoi account separati, avresti il compito di implementare politiche e autorizzazioni identiche e quindi dovresti mantenerle identiche in tutti gli account. Al contrario, tutti gli utenti di una condivisione di AWS RAM risorse sono gestiti da un unico set di politiche e autorizzazioni. AWS RAM offre un'esperienza coerente per la condivisione di diversi tipi di AWS risorse.
- **Fornisce visibilità e verificabilità:** visualizza i dettagli di utilizzo delle risorse condivise attraverso l'integrazione AWS RAM con Amazon CloudWatch e AWS CloudTrail. AWS RAM offre una visibilità completa su risorse e account condivisi.

Che dire dell'accesso tra più account con politiche basate sulle risorse?

Puoi condividere alcuni tipi di AWS risorse con altri Account AWS allegando una [policy basata sulle risorse](#) che identifica i principali (IAM) AWS Identity and Access Management (ruoli e utenti IAM) esterni al tuo. Account AWS Tuttavia, la condivisione di una risorsa allegando una policy non sfrutta i vantaggi aggiuntivi che ne derivano. AWS RAM Utilizzando AWS RAM si ottengono le seguenti funzionalità:

- È possibile condividere con un'[organizzazione o un'unità organizzativa \(OU\)](#) senza dover enumerare tutti i Account AWS IDs
- Gli utenti possono vedere le risorse condivise con loro direttamente nella Servizio AWS console di origine e nelle operazioni API come se tali risorse fossero direttamente nell'account dell'utente. Ad esempio, se condividi una sottorete Amazon VPC con un altro account, gli utenti di quell'account possono vedere la sottorete nella console Amazon VPC e i risultati delle operazioni API Amazon VPC eseguite in quell'account. AWS RAM Le risorse condivise allegando una policy basata sulle risorse non sono visibili in questo modo; devi invece scoprire e fare riferimento esplicitamente alla risorsa tramite il suo 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 preside 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 promuovere tali risorse a risorse completamente AWS RAM gestite effettuando una delle seguenti operazioni:

- Usa l'operazione API [PromoteResourceShareCreatedFromPolicy](#).
- Utilizzate l'equivalente dell'operazione API, che è il comando AWS Command Line Interface (AWS CLI). [promote-resource-share-created-from-policy](#)

Come funziona la condivisione delle risorse

Quando condividi una risorsa dell'account proprietario con un altro account Account AWS, l'account consumatore, concedi l'accesso alla risorsa condivisa ai responsabili dell'account di consumo. Tutte le politiche e le autorizzazioni che si applicano ai ruoli e agli utenti dell'account consumatore si applicano anche alla risorsa condivisa. Le risorse della condivisione sembrano risorse native nella cartella con Account 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 tua proprietà creando una [condivisione di risorse](#). Per creare una condivisione di risorse, è necessario specificare quanto segue:

- Regione AWS In cui si desidera creare la condivisione di risorse. Nella console, scegli dal menu a discesa Regione nell'angolo in alto a destra della console. Nel AWS CLI, si utilizza il parametro. `--region`
- Una condivisione di risorse può contenere solo risorse regionali che coincidono con Regione AWS la 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 principali a cui concedi l'accesso alla condivisione delle risorse. I responsabili possono essere singoli Account AWS, gli account di un'organizzazione o di un'unità organizzativa (OU) oppure ruoli o utenti individuali AWS 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, consulta [Risorse condivisibili AWS](#)

- Un'[autorizzazione gestita](#) da associare a ogni tipo di risorsa inclusa 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 principale:

- Se il principale si trova in un account diverso da quello che possiede la risorsa, le autorizzazioni associate alla condivisione delle 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 policy non possono superare quelle definite nelle autorizzazioni allegata 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 di proprietà del tuo account. Puoi accedere alla risorsa utilizzando la console, AWS CLI i comandi e le operazioni API del servizio pertinente. Le operazioni API che gli amministratori dell'account possono eseguire variano a seconda del tipo di risorsa e sono specificate dall' AWS RAM autorizzazione allegata alla condivisione delle risorse. Inoltre,

tutte le politiche IAM e le politiche di controllo dei servizi configurate nel tuo account continuano ad essere applicate, 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 del Account AWS proprietario della risorsa.

- Se la risorsa è regionale, puoi accedervi solo dalla risorsa Regione AWS in cui è presente nell'account proprietario.
- Se la risorsa è globale, puoi accedervi da qualsiasi Regione AWS dispositivo supportato dalla console di servizio e dagli strumenti della risorsa. È possibile visualizzare e gestire la condivisione 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.

Accedendo AWS RAM

Puoi lavorare con AWS RAM in uno dei seguenti modi:

AWS RAM console

AWS RAM fornisce un'interfaccia utente basata sul Web, la AWS RAM console. Se ti sei registrato a Account AWS, puoi accedere alla AWS RAM console accedendo [Console di gestione AWS](#) e selezionando AWS RAM dalla home page della console.

Puoi anche accedere direttamente alla [AWS RAM console](#) nel tuo browser. Se non hai ancora effettuato l'accesso, ti verrà chiesto di farlo prima che venga visualizzata la console.

AWS CLI e strumenti per Windows PowerShell

AWS CLI E AWS Strumenti per PowerShell forniscono accesso diretto alle operazioni API AWS RAM pubbliche. AWS supporta questi strumenti su Windows, macOS, e Linux. Per ulteriori informazioni su come iniziare, consulta la [Guida per AWS Command Line Interface l'utente](#) o la [Guida AWS Tools for Windows PowerShell per l'utente](#). Per ulteriori informazioni sui comandi per AWS RAM, vedere [AWS CLI Command Reference](#) o [AWS Tools for Windows PowerShell Cmdlet Reference](#).

AWS SDKs

AWS fornisce comandi API per un ampio set di linguaggi di programmazione. Per ulteriori informazioni su come iniziare, consulta la [AWS SDKs and Tools Reference Guide](#).

API della query

Se non utilizzi uno dei linguaggi di programmazione supportati, l'API AWS RAM HTTPS Query ti offre l'accesso programmatico a AWS RAM e AWS. Con l' AWS RAM API, puoi inviare richieste HTTPS direttamente al servizio. Quando utilizzi l' AWS RAM API, devi includere il codice per firmare digitalmente le richieste utilizzando le tue credenziali. Per ulteriori informazioni, consulta la [documentazione di riferimento dell'API di AWS RAM](#).

Prezzi per AWS RAM

Non sono previsti costi aggiuntivi per l'utilizzo AWS 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 sulla AWS fatturazione delle risorse condivisibili, consulta la documentazione del servizio di proprietà della risorsa.

Conformità e standard internazionali

PCI DSS

AWS RAM supporta l'elaborazione, l'archiviazione e la trasmissione dei dati delle carte di credito da parte di un commerciante o di un fornitore di servizi ed è stato convalidato come conforme al Payment Card Industry (PCI) Data Security Standard (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 RAM è autorizzato come FedRAMP Moderate nei Regioni AWS seguenti paesi: Stati Uniti orientali (Virginia settentrionale), Stati Uniti orientali (Ohio), Stati Uniti occidentali (California settentrionale) e Stati Uniti occidentali (Oregon).

AWS RAM è autorizzato come FedRAMP High nei Regioni AWS seguenti paesi AWS GovCloud : (Stati Uniti occidentali) e (Stati Uniti orientali). AWS GovCloud

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 con FedRAMP, vedere FedRAMP.](#)

SOC e ISO

AWS RAM può essere utilizzato per carichi di lavoro soggetti alla conformità SOC (Service Organization Control) 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 dettagliate sui processi e sui controlli di sicurezza che proteggono i dati dei clienti, disponibili nei report SOC e nei certificati ISO e CSA STAR in. AWS [AWS Artifact](#)

[Per ulteriori informazioni sulla conformità SOC, consulta SOC.](#)

[Per ulteriori informazioni sulla conformità ISO, vedere ISO 9001, ISO27001, ISO27017, ISO 27018 e ISO 27701.](#)

Guida introduttiva con AWS RAM

Con AWS Resource Access Manager, puoi condividere le risorse che possiedi con altre persone Account AWS. Se il tuo account è gestito da AWS Organizations, puoi anche condividere le risorse con gli altri account dell'organizzazione. Puoi anche utilizzare risorse condivise con te da altri Account AWS.

Se non abiliti la condivisione all'interno AWS Organizations, non puoi condividere le risorse con la tua organizzazione o con le unità organizzative (OU) dell'organizzazione. Tuttavia, puoi comunque condividere le risorse con i singoli Account AWS membri dell'organizzazione. Per i [tipi di risorse supportati](#), puoi anche condividere le risorse con singoli ruoli o utenti AWS Identity and Access Management (IAM) dell'organizzazione. In questo caso, questi responsabili vengono trattati come se fossero account esterni, anziché come parte dell'organizzazione. Ricevono un invito a partecipare alla condivisione di risorse e devono accettare l'invito per accedere alle risorse condivise.

Indice

- [Termini e concetti per AWS RAM](#)
- [Condivisione delle AWS risorse](#)
- [Utilizzo di AWS risorse condivise](#)

Termini e concetti per AWS RAM

I seguenti concetti aiutano a spiegare come 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 politica di autorizzazione AWS Identity and Access Management (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 dirigente IAM 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'PutResourcePolicyoperazione 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 ruoli e utenti IAM.

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 policy basate sull'identità IAM associate ai singoli ruoli o utenti dall'amministratore IAM nell'account di consumo. 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 principali di IAM come 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.
- Ruoli o utenti IAM individuali in un altro account: alcuni tipi di risorse supportano la condivisione diretta con singoli ruoli o utenti IAM. Specificate questo tipo principale tramite il relativo ARN.
 - Ruolo IAM: `arn:aws:iam::123456789012:role/rolename`
 - Utente IAM: `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 di un'organizzazione in base all'ARN dell'organizzazione o all'unità organizzativa.

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

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

- Tutti gli account in un'unità organizzativa: di seguito è riportato un esempio di ARN di un 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'utilizzo "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.

Politica basata sulle risorse

Le policy basate sulle risorse sono documenti di testo JSON che implementano il linguaggio di policy IAM. A differenza delle policy basate sull'identità associate al principale, come un ruolo o un utente IAM, le policy basate sulle risorse vengono associate alla risorsa. AWS RAM crea politiche basate sulle risorse per tuo conto sulla base delle 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, consulta [Politiche basate sull'identità e politiche basate sulle risorse nella Guida per l'utente IAM](#).

Le policy basate sulle risorse generate da AWS RAM vengono valutate insieme a tutti gli altri tipi di policy IAM. Ciò include tutte le policy basate sull'identità IAM associate ai responsabili che stanno tentando di accedere alla risorsa, e le policy 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 policy e su come determinare le autorizzazioni risultanti, consulta [Logica di valutazione delle policy](#) nella IAM User Guide.

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 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 delle risorse sottostante richiamando l'operazione. [GetResourcePolicy](#) 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 vedere tutte le risorse condivise con loro direttamente nella console del servizio proprietario delle risorse e nelle operazioni API 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 utente possono vedere il progetto nella CodeBuild console e nei risultati delle operazioni CodeBuild API eseguite. Le risorse condivise allegando direttamente una policy basata sulle risorse non sono

visibili in questo modo. È invece necessario scoprire e fare riferimento esplicitamente alla risorsa tramite il relativo 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 o nell'API pertinente.
- **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 di policy IAM basato su JSON. AWS RAM fornisce autorizzazioni ready-to-use AWS gestite tra cui scegliere di 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
- 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 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 immagine EC2 Image Builder con un AWS RAM account individuale, genera una policy simile al seguente esempio e la allega a tutte le risorse di immagine incluse nella condivisione delle risorse.

JSON

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

JSON

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

Note

Questa policy 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'utilizzo "Principal": "*" in una politica basata sulle risorse](#).

JSON

```

{
  "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'utilizzo "Principal": "*" in una politica basata sulle risorse

Quando "Principal": "*" include una policy basata sulle risorse, questa concede l'accesso a tutti i principali IAM 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 utilizzano un'autorizzazione gestita e altre risorse dello stesso tipo utilizzano 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 dai clienti 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 autorizzazioni AWS gestite a una versione più recente](#).

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](#) (facoltativo)
- [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 le risorse possono accedere alle condivisioni di risorse solo Regioni AWS nelle quali 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 dividerlo con singoli account o con tutti gli account dell'organizzazione o di un'unità organizzativa senza dover enumerare ogni account.

Per condividere 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 `AWSResourceAccessManagerServiceRolePolicy`.

Note

Per impostazione predefinita, quando abiliti la condivisione con AWS Organizations, la condivisione delle risorse all'interno dell'organizzazione limita l'accesso ai consumatori all'interno della stessa organizzazione. Se un account consumatore lascia l'organizzazione, tale account perde l'accesso alle risorse della condivisione delle risorse. Questa restrizione si applica sia che si condividano risorse con un'unità organizzativa, con l'intera organizzazione o con un singolo account dell'organizzazione.

Per quanto riguarda la account-to-account condivisione all'interno dell'organizzazione, è possibile mantenere l'accesso alla condivisione anche quando gli account vengono abbandonati, impostando l'opzione `RetainSharingOnAccountLeaveOrganization` `True` quando si crea una nuova condivisione di risorse. Con questa impostazione abilitata, AWS RAM invia un invito all'account utente (simile alla condivisione con account esterni). L'account mantiene l'accesso alle risorse condivise anche se lascia l'organizzazione. L'`RetainSharingOnAccountLeaveOrganization` impostazione presenta i seguenti requisiti e limitazioni:

- Richiede `allowExternalPrincipals` di essere `True`
- Può essere impostato solo quando si creano nuove condivisioni di risorse
- Non si applica alla condivisione con OUs o con l'intera organizzazione
- Quando `RetainSharingOnAccountLeaveOrganization` è impostato su `True`, non è possibile utilizzare le condivisioni di risorse per condividere risorse che [possono essere condivise solo all'interno di un'organizzazione](#).

Se non è più necessario condividere risorse con l'intera organizzazione oppure OUs è possibile disabilitare 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

Usa 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 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 in [Risorse 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, vedere [Condivisione 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 ruoli o utenti IAM 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'utilizzo "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, puoi aggiungere ruoli e utenti IAM individuali Account AWS o, per i servizi supportati, esterni all'organizzazione come responsabili di una condivisione di risorse.

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, consulta. [Risorse 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
- 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: 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, consulta [Condivisione 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. Per Nome, inserire un nome descrittivo della risorsa da condividere.

- 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 [Zona di disponibilità IDs per le tue AWS 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 [Crea 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 sottoreti Amazon VPC. Puoi anche condividere alcuni [tipi di risorse supportati](#) con ruoli e utenti IAM.

Per limitare la condivisione delle risorse solo agli account e ai responsabili della tua 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'utilizzo "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 ruolo o un utente Account AWS esterno all'organizzazione o un ruolo o utente IAM. È invece necessario disattivare Visualizza la struttura organizzativa e utilizzare l'elenco a discesa e la casella di testo per inserire l'ID o l'ARN.

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

123456789012

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

o-abcd1234

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


ou-abcd-1234efgh

- Ruolo IAM: per aggiungere un ruolo IAM, inserisci l'ARN del ruolo. Utilizzare la seguente sintassi:

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

Esempio:

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

 Note


Per ottenere l'ARN univoco per un ruolo IAM, [visualizza l'elenco dei ruoli nella console IAM](#), usa il [AWS CLI comando `get-role`](#) o l'azione API. [GetRole](#)

- Utente IAM: per aggiungere un utente IAM, inserisci l'ARN dell'utente. Utilizzare la seguente sintassi:

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

Esempio:

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

 Note

Per ottenere l'ARN univoco per un utente IAM, [visualizza l'elenco degli utenti nella console IAM](#), utilizza il [`get-user` AWS CLI comando](#) o l'azione [GetUserAPI](#).

- **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`

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 [Condividi AWS le risorse di tua proprietà](#).

AWS CLI

Per creare una condivisione di risorse

Utilizza il comando [create-resource-share](#). 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'ARN per l'autorizzazione gestita dal cliente, quindi crea la condivisione di risorse. Per ulteriori informazioni, consulta [Crea 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 di AWS risorse condivise

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

Processi

- [Rispondi all'invito alla condivisione delle risorse](#)
- [Usa le risorse condivise con te](#)

Rispondi all'invito alla condivisione delle risorse

Se ricevi un invito a partecipare a una condivisione di risorse, devi accettarlo per accedere alle risorse condivise.

Gli inviti non vengono utilizzati nei seguenti scenari:

- Se fai parte di un'organizzazione AWS Organizations e la condivisione all'interno dell'organizzazione è abilitata, i responsabili dell'organizzazione ottengono automaticamente l'accesso alle risorse condivise senza inviti.
- Se condividi la Account AWS risorsa con il proprietario, i responsabili di quell'account avranno automaticamente accesso alle risorse condivise senza inviti.

Console

Per rispondere agli inviti

1. Apri la pagina [Condivisi con me: condivisioni di risorse](#) nella AWS RAM console.

Note

Una condivisione di risorse è visibile solo nella cartella Regione AWS in cui è stata creata. Se la condivisione di risorse prevista non viene visualizzata nella console, potrebbe essere necessario passare a un'altra Regione AWS utilizzando il menu a discesa nell'angolo in alto a destra.

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

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.

3. 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 iniziare, ottieni un elenco degli inviti alla condivisione di risorse disponibili. Il comando di esempio seguente è stato eseguito nella `us-west-2` regione e mostra che una condivisione di risorse è disponibile nello `PENDING` 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-bbbbbbb222222",
      "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-bbbbbbb222222",
    "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 condivisione di risorse sono ora disponibili per i responsabili 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 API/CLI operazioni di ciascuna risorsa. Se la risorsa è regionale, è necessario utilizzare il comando corretto Regione AWS nella console di servizio o 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 AWS RAM, è necessario aprire la AWS RAM console in Regione AWS cui è stata creata la condivisione di risorse.

Lavorare con AWS risorse condivise

Puoi usare AWS Resource Access Manager (AWS RAM) per condividere AWS risorse di tua proprietà e accedere a AWS risorse condivise con te.

Indice

- [Condivisione delle risorse regionali rispetto alle risorse globali](#)
 - [Quali sono le differenze tra risorse regionali e globali?](#)
 - [Condivisioni di risorse e relative regioni](#)
- [Condividi AWS le risorse di tua proprietà](#)
 - [Visualizzazione delle condivisioni di risorse create in AWS RAM](#)
 - [Creazione di una condivisione di risorse in AWS RAM](#)
 - [Aggiornare una condivisione di risorse in AWS RAM](#)
 - [Visualizzazione delle risorse condivise in AWS RAM](#)
 - [Visualizzazione dei principali con cui condividi le risorse in AWS RAM](#)
 - [Eliminazione di una condivisione di risorse in AWS RAM](#)
- [Accedi alle AWS risorse condivise con te](#)
 - [Accettazione e rifiuto degli inviti alla condivisione di risorse](#)
 - [Visualizzazione delle condivisioni di risorse condivise con te](#)
 - [Visualizzazione delle risorse condivise con te](#)
 - [Visualizza i principali che condividono con te](#)
 - [Lasciare una condivisione di risorse](#)
 - [Prerequisiti per abbandonare una condivisione di risorse](#)
 - [Come abbandonare una condivisione di risorse](#)
- [Zona di disponibilità IDs per le tue AWS risorse](#)

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 il. Regione AWS Se è vuoto, 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. Vengono create in una Regione AWS specificata e quindi esistono in quella regione. Per visualizzare o interagire con tali risorse, occorre indirizzare le tue operazioni verso quella regione. Ad esempio, per creare un'istanza Amazon Elastic Compute Cloud (Amazon EC2) con, [scegli Console di gestione AWS](#) l'istanza in cui desideri creare Regione AWS l'istanza. Se usi AWS Command Line Interface (AWS CLI) per creare l'istanza, includi il `--region` parametro. AWS SDKs Ciascuno di essi ha il proprio meccanismo equivalente per specificare la regione utilizzata dall'operazione.

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

Se ne specifichi uno diverso Regione AWS nella console o in un AWS CLI comando, non potrai più vedere o interagire con le risorse che potevi vedere nella regione precedente.

Esaminando il [nome della risorsa Amazon \(ARN\)](#) di una risorsa regionale, la regione in cui si trova la risorsa è specificata nel quarto campo dell'ARN. Ad esempio, un'istanza Amazon EC2 è una risorsa regionale. Tali risorse ARNs hanno un aspetto simile al seguente esempio di 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 ne specifichi una Regione AWS nella console di un servizio globale. Per accedere a una risorsa globale, non si specifica un `--region` parametro quando si utilizzano le operazioni del servizio AWS CLI e dell' AWS SDK.

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 regioni diverse 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 centrale AWS Cloud WAN come risorsa globale, è coerente per tutti gli utenti. Viene visualizzata come un'unica rete globale contigua in tutte le regioni.

Il [nome della risorsa Amazon \(ARN\)](#) di una risorsa globale non include la regione. Il quarto campo di tale ARN è vuoto, ad esempio l'ARN di esempio seguente per una rete centrale Cloud WAN.

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

Condivisioni di risorse e relative regioni

AWS RAM è un servizio regionale e una condivisione di risorse è regionale. Pertanto, una condivisione di risorse può contenere risorse della 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, è possibile creare condivisioni di risorse con risorse globali solo nella regione di origine designata, regione Stati Uniti orientali (Virginia settentrionale), `us-east-1`. Sebbene sia possibile creare la condivisione di risorse solo in quella singola area di residenza, qualsiasi risorsa globale condivisa viene visualizzata come risorsa globale standard se visualizzata nella console del servizio o nelle operazioni CLI e SDK. 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, è necessario configurare la AWS RAM console per utilizzarla `us-west-2` e creare la condivisione di risorse nella regione. Non è possibile creare una condivisione di risorse che includa risorse regionali di diverse fonti Regioni AWS. Ciò significa che per condividere le risorse di entrambi `us-west-2` e `eu-north-1`, è necessario creare due diverse condivisioni di risorse. Non è possibile 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. È possibile 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 cartella condivisa Account AWS da qualsiasi regione dalla quale potevi accedervi nell'originale Account AWS.

Considerazioni

- Per creare una condivisione di risorse nella AWS RAM console, devi utilizzare la regione che contiene le risorse che desideri 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 l'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.
- È possibile creare una condivisione di risorse con risorse regionali e globali solo nella regione di origine designata, Stati Uniti orientali (Virginia settentrionale),. us-east-1

Condividi AWS le risorse di tua proprietà

È possibile utilizzare AWS Resource Access Manager (AWS RAM) per condividere le risorse specificate con i principali specificati. 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 in AWS RAM](#)
- [Creazione di una condivisione di risorse in AWS RAM](#)
- [Aggiornare una condivisione di risorse in AWS RAM](#)
- [Visualizzazione delle risorse condivise in AWS RAM](#)
- [Visualizzazione dei principali con cui condividi le risorse in AWS RAM](#)
- [Eliminazione di una condivisione di risorse in AWS RAM](#)

Visualizzazione delle condivisioni di risorse create in AWS RAM

Puoi visualizzare un elenco delle condivisioni di risorse che hai creato. Puoi vedere quali risorse condividi e con chi sono condivise.

Console

Per visualizzare le tue condivisioni di risorse

1. Apri la 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, consulta [Condivisione delle risorse regionali rispetto alle risorse globali](#).
3. Se una delle autorizzazioni gestite utilizzate dalle condivisioni di risorse nei risultati presenta 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 di autorizzazione gestita 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, nella colonna Stato viene visualizzato Aggiornamento disponibile. La scelta di tale 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 di attributi suggeriti. Dopo averne scelto uno, puoi sceglierlo dall'elenco dei valori disponibili per quel campo. Puoi aggiungere altri attributi o parole chiave fino a trovare la risorsa desiderata.
5. Scegli il nome della condivisione di risorse da esaminare. La console visualizza le seguenti informazioni sulla condivisione delle risorse:
 - Riepilogo: elenca il nome, l'ID, il proprietario, il nome della risorsa Amazon Resource Name (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 esistere al massimo un'autorizzazione gestita per tipo di risorsa inclusa nella condivisione di risorse. Ogni autorizzazione gestita mostra la versione di tale autorizzazione gestita associata alla condivisione di risorse. Se non è la versione predefinita, la console visualizza il link **Aggiorna** alla versione predefinita. Se scegli quel link, avrai 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 e visualizzare la risorsa nella console del servizio nativo.
 - Principi condivisi: elenca i responsabili con cui vengono condivise le risorse.
 - Tag: elenca le coppie chiave-valore dei tag allegate alla condivisione di risorse stessa; non si tratta dei tag allegati alle singole risorse incluse nella condivisione di risorse.

AWS CLI

Per visualizzare le condivisioni di risorse

È possibile utilizzare il [get-resource-shares](#) comando con il parametro `--resource-owner` impostato `SELF` per visualizzare i dettagli delle condivisioni di risorse create in Account AWS.

L'esempio seguente mostra le condivisioni di risorse condivise in current Regione AWS (`us-east-1`) per la chiamata Account AWS. Per ottenere le condivisioni di risorse create in una regione diversa, utilizzate 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 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 in [Risorse 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, vedere [Condivisione 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 ruoli o utenti IAM 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'utilizzo "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, puoi aggiungere

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

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, consulta. [Risorse 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
- 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: 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, consulta [Condivisione 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 [Zona di disponibilità IDs per le tue AWS 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 [Crea 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 sottoreti Amazon VPC. Puoi anche condividere alcuni [tipi di risorse supportati](#) con ruoli e utenti IAM.

Per limitare la condivisione delle risorse solo agli account e ai responsabili della tua 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. In questo modo 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'utilizzo "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.

ℹ 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 ruolo o un utente Account AWS esterno all'organizzazione o un ruolo o utente IAM. È invece necessario

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

- Per specificare un principale tramite ID o ARN, inclusi i principali esterni all'organizzazione, selezionare il tipo principale per ogni principale. Quindi, inserisci l'ID (per un' Account AWS organizzazione o un'unità organizzativa) o l'ARN (per un ruolo o un utente IAM), quindi scegli Aggiungi. I tipi principali e i formati ID e ARN 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

- Ruolo IAM: per aggiungere un ruolo IAM, inserisci l'ARN del ruolo. Utilizzare la seguente sintassi:

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

Per esempio:

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

Note


Per ottenere l'ARN univoco per un ruolo IAM, [visualizza l'elenco dei ruoli nella console IAM](#), [usa il](#) AWS CLI comando [get-role](#) o l'azione API. [GetRole](#)

- Utente IAM: per aggiungere un utente IAM, inserisci l'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'ARN univoco per un utente IAM, [visualizza l'elenco degli utenti nella console IAM](#), utilizza il [get-user](#) AWS CLI comando o l'azione [GetUserAPI](#).

- **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 [Condividi AWS le risorse di tua proprietà](#).

AWS CLI

Per creare una condivisione di risorse

Utilizza il comando [create-resource-share](#). 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'ARN per l'autorizzazione gestita dal cliente, quindi crea la condivisione di risorse. Per ulteriori informazioni, consulta [Crea 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, consulta [Prerequisiti 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, consulta [Condivisione 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. Console di gestione AWS
 - 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 [Crea 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 ruoli o utenti IAM 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'utilizzo "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 ruolo o un utente Account AWS esterno all'organizzazione o un ruolo o utente IAM. È invece necessario aggiungere questi principi 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 l'ARN per 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 appartenenti alla 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, utilizzare 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-permissionse](#) [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'opzione `--replace` 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 l'ARN specificato 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](#). [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 in AWS 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 condividendo attualmente, il numero di condivisioni di risorse in cui sono incluse e il numero di destinatari che vi hanno accesso.

Console

Per visualizzare le risorse che stai condividendo attualmente

1. Apri la pagina [Condivise da me: risorse condivise](#) 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, consulta [Condivisione delle risorse regionali rispetto alle risorse globali](#).
3. Per ogni risorsa condivisa, sono disponibili le seguenti informazioni:
 - ID risorsa: l'ID della risorsa. Scegliete l'ID di una risorsa per aprire una nuova scheda del browser e visualizzare la risorsa nella sua console di servizio nativa.
 - 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 responsabili che possono accedere alla risorsa. Scegli il valore per visualizzare i principali.

AWS CLI

Per visualizzare le risorse che stai attualmente condividendo

Puoi utilizzare il comando [list-resources](#) con il parametro `--resource-owner` impostato su `SELF` per visualizzare i dettagli delle risorse che condividi attualmente.

L'esempio seguente mostra le risorse incluse nelle condivisioni di risorse in Regione AWS (us-east-1) per la chiamata. Account AWS Per ottenere le risorse condivise in un'altra regione, utilizzate 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 principali con cui condividi le risorse in AWS RAM

Puoi visualizzare i principali con cui condividi le tue risorse, in tutte le condivisioni di risorse. La visualizzazione di questo elenco di responsabili ti aiuta a determinare chi ha accesso alle tue risorse condivise.

Console

Per visualizzare i principali con cui condividi le risorse

1. Vai alla pagina [Shared by me: Principal](#) 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, consulta [Condivisione delle risorse regionali rispetto alle risorse globali](#).
3. Applica un filtro per trovare principi specifici. È possibile applicare più filtri per limitare la ricerca. Scegli la casella di testo per visualizzare un elenco a discesa dei campi di attributi

suggeriti. Dopo averne scelto uno, puoi sceglierlo dall'elenco dei valori disponibili per quel campo. Puoi aggiungere altri attributi o parole chiave fino a trovare la risorsa desiderata.

4. Per ogni principale nell'elenco, la console visualizza le seguenti informazioni:
 - ID principale: l'ID del principale. Scegli l'ID per aprire una nuova scheda del browser e visualizzare il principale nella sua console nativa.
 - Condivisioni di risorse: il numero di condivisioni di risorse condivise con il principale specificato. Scegli il numero per visualizzare l'elenco delle condivisioni di risorse.
 - Risorse: il numero di risorse che hai condiviso con il responsabile. Scegli il numero per visualizzare l'elenco delle risorse condivise.

AWS CLI

Per visualizzare i principali con cui condividi le risorse

Puoi usare il comando [list-principals](#) per ottenere un elenco dei principali a cui fai riferimento nelle condivisioni di risorse che hai creato nella versione corrente Regione AWS per l'account chiamante.

L'esempio seguente elenca i principali che hanno accesso alle condivisioni create nella regione predefinita per l'account chiamante. In questo esempio, i principali sono l'organizzazione dell'account chiamante e un account separato Account AWS, come parte di due diverse condivisioni di risorse. È necessario utilizzare l'endpoint del servizio Regione AWS 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 in AWS RAM

Puoi eliminare una condivisione di 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 elimina le risorse condivise.

Per eliminare una risorsa AWS

Se è necessario eliminare una AWS risorsa inclusa in una condivisione di risorse, si AWS 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 nella AWS RAM console per un breve periodo dopo l'eliminazione, ma il suo stato cambia in Deleted.

Console

Come eliminare una condivisione di risorse

1. Apri la pagina [Shared by me: Resource](#) shared 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, consulta [Condivisione delle risorse regionali rispetto alle risorse globali](#).
3. Seleziona la condivisione di risorse che desideri eliminare.

⚠ Warning

Assicurati di selezionare la condivisione di risorse corretta. Non puoi ripristinare una condivisione di 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, rimane visibile nella console con lo stato eliminato.

AWS CLI

Come eliminare una condivisione di risorse

Puoi usare il [delete-resource-share](#) comando per eliminare una condivisione di risorse che non ti serve più.

L'esempio seguente utilizza innanzitutto il [get-resource-shares](#) comando per ottenere l'Amazon Resource Name (ARN) della condivisione di risorse che desideri eliminare. Quindi viene utilizzato [delete-resource-share](#) per 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](#)
- [Visualizzazione delle condivisioni di risorse condivise con te](#)
- [Visualizzazione delle risorse condivise con te](#)
- [Visualizza i principali che condividono con te](#)
- [Lasciare una condivisione di risorse](#)

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: IPv4 indirizzi 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, consulta [Condivisione 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-invitations](#) comando 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 aACCEPTED.

Se invece desideri rifiutare l'invito, esegui il [reject-resource-share-invitation](#) comando, 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-fbf6-4336-8377-06c559dfce49
{
  "resourceShareInvitation": {
    "resourceShareInvitationArn": "arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/3b3bc051-fbf6-4336-8377-06c559dfce49",
    "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 responsabili condividono risorse con te e quali risorse condividono.

Console

Per visualizzare le condivisioni 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, consulta [Condivisione 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 di attributi suggeriti. Dopo averne scelto uno, puoi sceglierlo dall'elenco dei valori disponibili per quel campo. Puoi aggiungere altri attributi o parole chiave fino a trovare la risorsa desiderata.
4. La AWS RAM console visualizza le seguenti informazioni:
 - Nome: il nome della condivisione di risorse.
 - ID: l'ID della condivisione di risorse. Scegli l'ID per visualizzare la pagina dei dettagli della condivisione delle risorse.
 - Proprietario: l'ID di chi Account 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'uso.
 - Deleted— La condivisione di risorse viene eliminata e non è più disponibile per l'uso.
 - Pending— Un invito ad accettare la condivisione di risorse è in attesa di una risposta.

AWS CLI

Per visualizzare le condivisioni di risorse

Utilizzate il [get-resource-shares](#) comando con il `--resource-owner` parametro impostato su `OTHER-ACCOUNTS`.

L'esempio seguente mostra l'elenco delle condivisioni di risorse condivise nell'account chiamante specificato Regione AWS con l'account chiamante da altri Account 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 [Condivisi con me: risorse condivise](#) 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, consulta [Condivisione 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.
 - 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 principale 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 comando di esempio seguente visualizza i dettagli sulla risorsa accessibile tramite una condivisione di risorse nell'area specificata Regione AWS da un'altra. Account 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 principali che condividono con te

Puoi visualizzare un elenco di tutti i responsabili che condividono risorse con te. Puoi vedere quali risorse e condivisioni di risorse condividono con te.

Console

Per visualizzare i principali elementi che condividono le risorse con te

1. Apri la AWS RAM console a <https://console.aws.amazon.com/ram/casa>.
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, consulta [Condivisione delle risorse regionali rispetto alle risorse globali](#).
3. Nel riquadro di navigazione, scegliere Shared with me (Condivise con me), Principals (Principali).
4. (Facoltativo) Puoi applicare un filtro per trovare principali specifici. È possibile applicare più filtri per limitare la ricerca.
5. La console visualizza le seguenti informazioni:
 - ID principale: l'ID del principale che condivide con te.
 - Condivisioni di risorse: il numero di condivisioni di risorse a cui il committente ti ha aggiunto. Scegli 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 le risorse con te

Puoi usare il comando [list-principals](#) per recuperare l'elenco dei responsabili che condividono risorse con i tuoi. Account AWS

Il comando di esempio seguente visualizza i dettagli relativi a chi Account AWS ha condiviso una condivisione di risorse con l'account utilizzato per chiamare l'operazione nel campo specificato.
Regione 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

Servizio	Tipo di risorsa
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 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, consulta [Condivisione 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-share](#) comando 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"
    }
  ]
}
```

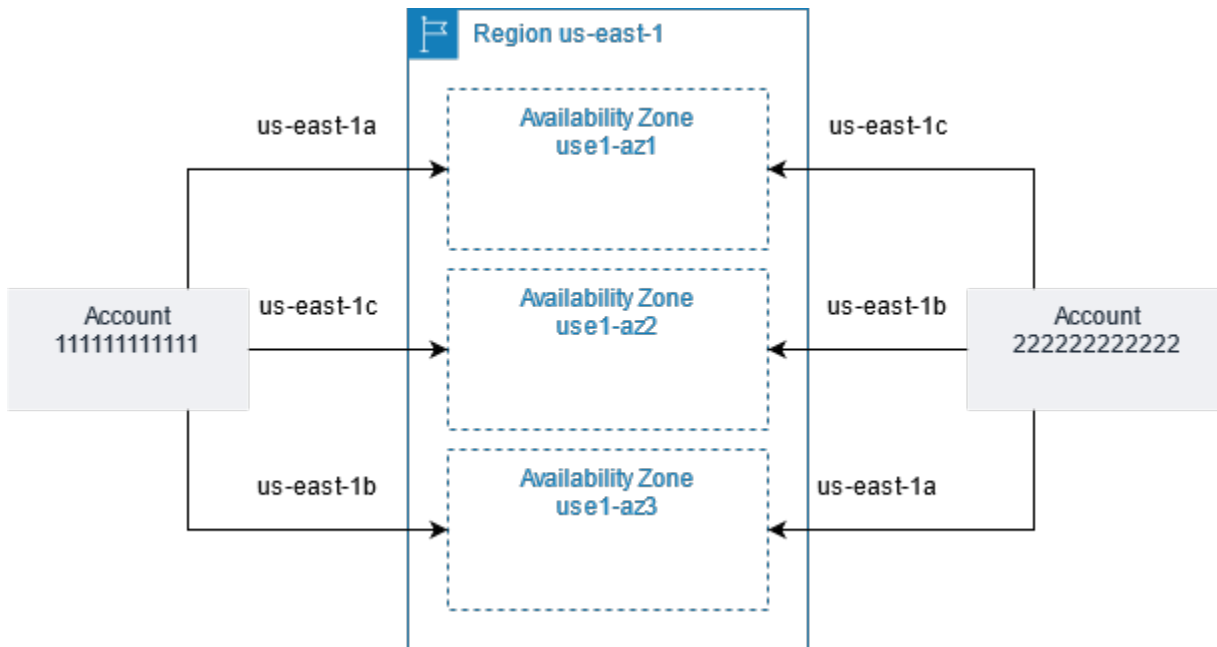
- Quindi, puoi eseguire il comando per lasciare quella condivisione di risorse. Tieni presente che devi anche specificare l'ID del tuo account123456789012, come principale da dissociare dalla condivisione di risorse specificata, che è condivisa per account111111111111.

```
$ 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  
        }  
      ]  
    }  
}
```

Zona di disponibilità IDs per le tue AWS risorse

AWS mappa le zone di disponibilità fisiche in modo casuale ai nomi delle zone di disponibilità di ciascuna. Account AWS Questo approccio consente di distribuire le risorse tra le zone di disponibilità in una Regione AWS regione, anziché concentrarle probabilmente nella zona di disponibilità «a» per ogni regione. Di conseguenza, la zona us-east-1a di disponibilità AWS dell'account potrebbe non rappresentare la stessa ubicazione fisica us-east-1a di un altro AWS account. Per ulteriori informazioni, consulta [Regioni e zone di disponibilità](#) nella Amazon EC2 User Guide.

L'illustrazione seguente mostra come le AZ IDs siano le stesse per tutti gli 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 Regione 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 su un nome specifico non è importante. Tuttavia, quando si condivide una risorsa del genere con altri Account AWS, la mappatura è importante. AWS RAM Questa mappatura casuale complica la capacità dell'account che accede alla risorsa condivisa di sapere a quale zona di disponibilità fare riferimento. A tal fine, tali risorse consentono inoltre di identificare la posizione effettiva delle risorse relative agli account utilizzando l'ID AZ. Un ID AZ è un identificatore univoco e coerente per una zona di disponibilità comune. Account AWS Ad esempio, use1-az1 è un ID AZ per una zona di disponibilità nella us-east-1 regione e rappresenta la stessa posizione fisica in ogni AWS account.

È possibile utilizzare AZ IDs per determinare la posizione delle risorse in un account rispetto alle risorse di 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 viene visualizzato nella console Amazon VPC e può essere interrogato utilizzando. AWS CLI

Console

Per visualizzare la AZ IDs per le zone di disponibilità nel tuo account

1. Vai alla pagina della [AWS RAM console](#) all'interno della AWS RAM console.
2. Puoi visualizzare la AZ IDs attuale nella Regione AWS sezione Il tuo ID AZ.

AWS CLI

Per visualizzare la AZ IDs per le zone di disponibilità nel tuo account

Il comando di esempio seguente mostra la zona di disponibilità IDs per le zone di disponibilità nella regione us-west-2 e come vengono mappate per la chiamata. Account 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 ruoli e utenti individuali AWS Identity and Access Management (IAM).

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:

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

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.





AWS App Mesh

Puoi condividere le seguenti AWS App Mesh risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
<p>Mesh</p> <p>appmesh:Mesh</p>	<p>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.</p>	<p> S</p>	<p> S</p> <p>Può condividere con chiunque Account AWS.</p>	<p> N</p>	<p> No</p>





AWS AppSync API GraphQL

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

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
AppSync GraphQL APIs 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'API AWS AppSync unificata in grado di 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

Gateway Amazon API

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

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

Amazon Application Recovery Controller (ARC)





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

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Cluster ARC Route 53 <code>route53-recovery-control:Cluster</code>	Crea e gestisci i cluster ARC 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 <u>Condivisione di cluster tra account</u> nella Amazon Application Recovery Controller (ARC) Developer Guide.	 S	 S Può condividere con chiunque Account AWS.	 S	 No
Piani di cambio della regione ARC	Crea e gestisci i piani centralmente e condividili con altri	 S	 S	 S	 No

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
arc-region-switch:Plan	Account AWS o con la tua organizzazione. Ciò consente a più account di utilizzare le risorse di un account diverso dall'account che ospita il piano. Per ulteriori informazioni, consulta Region switch nella Amazon Application Recovery Controller (ARC) Developer Guide .		Può condividere con chiunque Account AWS.		





Amazon Aurora

Puoi condividere le seguenti risorse Amazon Aurora utilizzando. AWS RAM

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Cluster Aurora DB <code>rds:Cluster</code>	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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Vault di backup 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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
<p>Modello personalizzato Bedrock</p> <p><code>bedrock:CustomModel</code></p>	<p>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.</p>	<p> S</p>	<p> N</p> <p>Può condividere solo con Account AWS la propria organizzazione.</p>	<p> S</p>	<p> No</p>

Gestione di costi e fatturazione

Puoi condividere le seguenti risorse di Billing and Cost Management utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
<p>Dashboard BCM</p> <p>bcm-dashboards:dashboard</p>	<p>Crea e gestisci dashboard di Billing and Cost Management e condividili con Account AWS altri all'interno o all'esterno dell'organizzazione. Quando condividi una dashboard, vengono condivise solo le configurazioni della dashboard, non i dati sottostanti. I destinatari hanno accesso al layout della dashboard e alle configurazioni dei widget e vedranno i dati in base alle proprie autorizzazioni di accesso. Questa funzionalità di condivisione consente alle organizzazioni di stabilire pratiche comuni di rendicontazione dei costi e aiuta i</p>	<p> N</p>	<p> S</p> <p>Può condividere con chiunque. Account AWS</p>	<p> S</p>	<p> No</p>

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	<p>diversi team a visualizzare i dati sui costi in modo coerente. Per ulteriori informazioni, consulta la sezione Condivisione delle dashboard nella Guida per l'utente di Billing and Cost Management.</p>				





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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Visualizzazioni di fatturazione <code>billing:billingview</code>	Crea e gestisci le visualizzazioni di fatturazione personalizzate in modo centralizzato e condividerle con altri utenti 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 Condivisione di visualizzazioni di fatturazione personalizzate nella Guida per l'AWS Cost Management utente.	 N	 N Può condividere solo con Account AWS la propria organizzazione.	 S	 No





AWS Cloud Map

È possibile condividere le seguenti AWS Cloud Map risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
AWS Cloud Map Namespace <code>servicediscovery:Namespace</code>	Crea e gestisci i namespace centralmente e condividili con altri membri dell'organizzazione. Account AWS Ciò consente di Account AWS scoprire più servizi e istanze nello spazio dei nomi condiviso senza la necessità di credenziali temporanee. Per ulteriori informazioni, consulta Shared AWS Cloud Map namespaces nella Developer Guide.AWS Cloud Map	 S	 N Può condividere solo con la propria Account AWS organizzazione.	 S	 No





AWS WAN cloud

È possibile condividere le seguenti risorse AWS Cloud WAN utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Reti principali <code>networkmanager:CoreNetwork</code>	Crea e gestisci centralmente una rete centrale Cloud WAN e condividila con altri Account AWS. Ciò consente Account AWS l'accesso e il provisioning di più host su un'unica rete principale Cloud WAN. Per ulteriori informazioni, consulta Condividi una rete principale nella Guida per l'utente di AWS Cloud WAN.	 S	 S Può condividere con chiunque Account AWS.	 N	 No





Amazon CloudFront

Puoi condividere le seguenti CloudFront risorse Amazon utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Amazon CloudFront VpcOrigin cloudfront:VpcOrigin	Crea e gestisci le origini CloudFront VPC centralmente e condividile con altri Account AWS o con la tua organizzazione. Ciò consente Account AWS l'utilizzo di origini VPC condivise per CloudFront le distribuzioni. Per ulteriori informazioni, consulta la sezione Lavorare con risorse condivise CloudFront nella Amazon CloudFront Developer 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 condividere con utenti e ruoli IAM	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 ccloudhsm: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, vedere 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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
CodeBuild Progetti <code>codebuild:Project</code>	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 analizzare 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
CodeBuild Gruppi di report <code>codebuild:ReportGroup</code>	Crea un gruppo di report e utilizzalo 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	 S	 S Può condividere con chiunque Account AWS.	 S	 No

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	<p>Account 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 sua 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.</p>				





AWS CodeConnections

È possibile condividere le seguenti CodeConnections risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
<p>Connessioni di codice</p> <p>codeconnections:Connection</p>	<p>Gestisci il riutilizzo delle connessioni di codice in più account. In altre parole, la condivisione delle connessioni tramite codice riduce l'onere dell'amministratore e la necessità dell'accesso da amministratore in ogni account che richiede una connessione tramite codice. Per ulteriori informazioni, consulta Share connections with Account AWS nella Guida per l'utente della console Developer Tools.</p>	<p> N</p>	<p> S</p> <p>Può condividere con chiunque Account AWS.</p>	<p> S</p>	<p> No</p>




Amazon DataZone


Puoi condividere le seguenti DataZone risorse utilizzando AWS RAM.

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

Amazon EC2





Puoi condividere le seguenti risorse Amazon EC2 utilizzando. AWS RAM





Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
<p>Prenotazioni della capacità</p> <p><code>ec2:CapacityReservation</code></p>	<p>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 EC2 di Account AWS lanciare le proprie istanze Amazon EC2 in una capacità riservata gestita centralmente. Per ulteriori informazioni, consulta Lavorare con le prenotazioni di capacità condivise nella Guida per l'utente di Amazon EC2.</p> <p>Condividi Capacity Blocks for ML (non UltraServer CBs sono ancora supportati) con altri Account AWS o</p>	<p> N</p>	<p>Sì per le prenotazioni di capacità (può essere condivisa con chiunque Account AWS).</p> <p>No per Capacity Blocks (può condividere solo Account AWS con la propria organizzazione).</p>	<p> N</p>	<p> No</p>

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	<p>con la tua organizzazione. Questa funzionalità consente a carichi di lavoro in esecuzione e su istanze Amazon EC2 diverse di Account AWS lanciare istanze Amazon EC2 in blocchi di capacità di tua proprietà, aiutandoti a utilizzare meglio la capacità riservata e a risparmiare sui costi. Per ulteriori informazioni, consulta Working with shared Capacity Blocks nella Amazon EC2 User Guide.</p> <div data-bbox="399 1480 743 1852" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; background-color: #fff9f9;"> <p> Important Se non soddisfi tutti i prerequisiti per condividere una prenotazione di capacità,</p> </div>				

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




Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	<p>monitorar 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.</p>				





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





Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	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 istanze Amazon EC2 da qualsiasi account con cui condividi in un gruppo di collocamento condiviso. Per ulteriori informazioni, consulta Condividi un gruppo di collocamento nella Guida per l'utente di Amazon EC2.	 S	 S Può condividere con chiunque Account AWS.	 N	 No

EC2 Image Builder

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

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Componenti Image Builder <code>imagebuilder:Component</code>	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 Condividere le risorse di EC2 Image Builder nella Guida per l'utente di EC2 Image Builder.	 S	 S Può condividere con chiunque. Account AWS	 S	 No
ricette di container Image Builder <code>imagebuilder:ContainerRecipe</code>	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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	<p>per duplicare le build di immagini dei contenitori. Per ulteriori informazioni, consulta Condividere le risorse di EC2 Image Builder nella Guida per l'utente di EC2 Image Builder.</p>				
<p>Immagini di Image Builder</p> <p><code>imagebuilder:Image</code></p>	<p>Crea e gestisci le tue immagini dorate in modo centralizzato e condividile con altri Account AWS o con la tua organizzazione. Gestisci chi può utilizzare le immagini create con EC2 Image Builder nella tua organizzazione. Per ulteriori informazioni, consulta Condividere le risorse di EC2 Image Builder nella Guida per l'utente di EC2 Image Builder.</p>	<p> S</p>	<p> S</p> <p>Può condividere con chiunque. Account AWS</p>	<p> S</p>	<p> No</p>

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
ricette di immagini Image Builder <code>imagebuilder:ImageRecipe</code>	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 Condividere le risorse di EC2 Image Builder nella Guida per l'utente di EC2 Image Builder.	 S	 S Può condividere con chiunque. Account AWS	 S	 No





Elastic Load Balancing





È possibile condividere le seguenti risorse Elastic Load Balancing utilizzando. AWS RAM





Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Negozi ELB Trust elasticloadbalancing:TrustStore	Crea e gestisci gli archivi di fiducia Elastic Load Balancing centralmente e condividili con altri Account AWS o con la tua organizzazione. Gli amministratori della sicurezza possono gestire uno o più piccoli archivi di fiducia e abilitare le configurazioni TLS reciproche tra Application Load Balancer. Per ulteriori informazioni, consulta Share your Elastic Load Balancing trust store for Application Load Balancers nella User Guide for Application Load Balancers.	 S	 S	 N	 No





AWS End User Messaging SMS

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

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
<p>AWS SMS</p> <p>Elenchi di disattivazione vocale</p> <p><code>sms-voice:OptOutList</code></p>	<p>Crea un elenco di opt-out e condividilo con altri membri Account AWS della tua organizzazione. Puoi condividere l'elenco di opt-out 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 per AWS End User Messaging SMS l'utente.</p>	<p> No</p>	<p> Sì</p> <p>Può condividere con chiunque Account AWS.</p>	<p> Sì</p>	<p> No</p>

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
<p>AWS SMS Numeri di telefono vocali</p> <p><code>sms-voice:PhoneNumber</code></p>	<p>Crea e gestisci numeri di telefono per condividerli con altri Account AWS o 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.</p>	<p> N</p>	<p> S</p> <p>Può condividere con chiunque Account AWS.</p>	<p> S</p>	<p> Sì</p>

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






Amazon FSx per OpenZFS

Puoi condividere le seguenti risorse Amazon FSx for OpenZFS utilizzando. AWS RAM

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
FSx Volumi fsx:Volume	Crea e gestisci FSx i volumi OpenZFS centralmente 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 o. FSx APIs CreateVolume CopySnaps hotAndUpdateVolume Per ulteriori informazioni, consulta la replica dei dati su richiesta nella Guida per l'utente di Amazon FSx for OpenZFS.	 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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
<p>AWS Glue Catalogo</p> <p><code>glue:Catalog</code></p>	<p>Gestisci un catalogo di dati centralizzato e condividi i metadati su database e tabelle con Account AWS o con la tua organizzazione. Ciò consente agli utenti di eseguire query sui dati su più account. Per ulteriori informazioni, consulta Condivisone delle tabelle e dei database del catalogo dati tra AWS account nella Guida per gli AWS Lake Formation sviluppatori.</p>	<p> N</p>	<p> S</p> <p>Può condividere con chiunque Account AWS.</p>	<p> N</p>	<p> No</p>
<p>AWS Glue Database</p> <p><code>glue:Database</code></p>	<p>Crea e gestisci i database dei cataloghi di dati in modo centralizzato e condividili con Account AWS la tua</p>	<p> N</p>	<p> S</p>	<p> N</p>	<p> No</p>

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	<p>organizzazione. I database sono raccolte di tabelle di cataloghi di dati. Ciò consente agli utenti di eseguire query e processi di estrazione, trasformazione e caricamento (ETL) in grado di unire e interrogare i dati su più account. Per ulteriori informazioni, consulta Condivisone delle tabelle e dei database del catalogo dati tra AWS account nella Guida per gli AWS Lake Formation sviluppatori.</p>		<p>Può condividere con chiunque Account AWS.</p>		

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
AWS Glue Tavoli <code>glue:Table</code>	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 S3, origini dati JDBC, Amazon Redshift, sorgenti di streaming e altri archivi dati. Ciò consente agli utenti di eseguire query e job ETL 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 condividere con utenti e ruoli IAM	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 condividere con utenti e ruoli IAM	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 <code>aws-marketplace:Entity</code>	Crea, gestisci e condividi entità all'interno Account AWS o all'interno della tua organizzazione in Marketplace AWS. Per ulteriori informazioni, consulta Condivisi one 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 condividere con utenti e ruoli IAM	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









Approvazione multiparte

Puoi condividere le seguenti risorse di approvazione multipartitiche utilizzando AWS RAM.


Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Team di approvazione multipartitico mpa:ApprovalTeam	Crea e gestisci team di approvazione e condividili con altri Account AWS o con la tua organizzazione. Ciò consente Account AWS ad altri di utilizzare un team di approvazione associato a un'operazione protetta. Un'operazione protetta è un elenco predefinito di operazioni che richiedono l'approvazione del team prima di poter essere eseguite. Per ulteriori informazioni, consulta Termini e concetti nella Guida per l'utente all'approvazione multipartitica.	 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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Firewall di rete network-firewall:Firewall	Crea e gestisci i firewall centralmente e condividili con altri utenti Account AWS in modo che possano creare endpoint firewall. Ciò consente a più account di utilizzare le protezioni di un singolo firewall. Per ulteriori informazioni, consulta Condivisione AWS Network Firewall delle risorse nella Guida per gli AWS Network Firewall sviluppatori.	 S	 S Può condividere con chiunque Account AWS.	 N	 No
Politiche del Network 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	 S	 S Può condividere	 N	 No


Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
firewallPolicy	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 AWS Network Firewall delle risorse nella Guida per gli AWS Network Firewall sviluppatori.		re con chiunque Account AWS.		

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
<p>Gruppi di regole del Network Firewall</p> <p><code>network-firewall:StatefulRuleGroup</code></p> <p><code>network-firewall:StatelessRuleGroup</code></p>	<p>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 AWS Network Firewall delle risorse nella Guida per gli AWS Network Firewall sviluppatori.</p>	<p> S</p>	<p> S</p> <p>Può condividere con chiunque Account AWS.</p>	<p> N</p>	<p> No</p>

Oracle Database@AWS

È possibile condividere le seguenti Oracle Database@AWS risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
<p>Oracle Database@AWS Infrastruttura Exadata</p> <p>odb:Cloud ExadataInfrastrutture</p>	<p>Con Oracle Database@AWS, puoi condividere la tua infrastruttura Exadata e la tua rete ODB tra più Account AWS utenti della stessa organizzazione. AWS Ciò consente di effettuare il provisioning dell'infrastruttura una sola volta e di riutilizzarla su più account affidabili, riducendo i costi e separando le responsabilità. Per ulteriori informazioni, consulta la sezione Condivisione delle risorse Oracle Database@AWS nella Guida per l' Oracle Database@AWS utente.</p>	<p> N</p>	<p> N</p> <p>Può condividere solo Account AWS con la propria organizzazione.</p>	<p> N</p>	<p> No</p>





Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Oracle Database@AWS Rete ODB odb:OdbNetwork	Con Oracle Database@AWS, puoi condividere la tua infrastruttura Exadata e la tua rete ODB tra più Account AWS utenti della stessa organizzazione. AWS Ciò consente di effettuare il provisioning dell'infrastruttura una sola volta e di riutilizzarla su più account affidabili, riducendo i costi e separando le responsabilità. Per ulteriori informazioni, consulta la sezione Condivisione delle risorse Oracle Database@AWS nella Guida per l' Oracle Database@AWS utente .	 N	 N Può condividere solo Account AWS con la propria organizzazione.	 N	 No

AWS Outposts

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





Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	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 volumi EBS 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
Tabelle di routing del gateway locale	Crea e gestisci le associazioni VPC verso un gateway locale centralmente e condividile con	 N	 N	 N	 No

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
ec2:LocalGatewayRouteTable	altri membri della tua Account AWS organizzazione. Ciò consente a più account di creare associazioni VPC 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 .		Può condividere solo Account AWS con la propria organizzazione.		

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Siti Outposts outposts: Site	Crea e gestisci siti Outpost e condividi li con altri membri della tua Account AWS 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 condividere con utenti e ruoli IAM	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





AWS Autorità di certificazione privata

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

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
<p>Autorità di certificazione privata () CAs</p> <p>acm-pca:CertificateAuthority</p>	<p>Crea e gestisci autorità di certificazione private (CAs) per l'infrastruttura a chiave pubblica interna (PKI) della tua organizzazione 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.</p> <p>Per ulteriori informazioni, consulta Controllare l'accesso a una CA privata nella Guida per l'AWS Autorità di certificazione privata utente.</p>	 S	 S <p>Può condividere con chiunque Account AWS.</p>	 N	 Sì





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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
<p>Visualizzazioni dell'esploratore di risorse</p> <p><code>resource-explorer-2:View</code></p>	<p>Crea e configura le visualizzazioni di Resource Explorer centralmente e condividerle con altri Account AWS 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.</p>	<p> N</p>	<p> N</p> <p>Può condividere solo Account AWS con la propria organizzazione.</p>	<p> N</p>	<p> No</p>





AWS Resource Groups





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

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Resource Groups 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 dedicati Amazon EC2 creati utilizzando AWS License Manager Per ulteriori informazioni, consulta Host resource groups AWS License Manager nella Guida per l'AWS License Manager 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 condividere con utenti e ruoli IAM	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 <code>route53resolver:FirewallRuleGroup</code>	Crea e gestisci centralmente i gruppi di regole Route 53 Resolver DNS Firewall e condividili con altri o con la tua organizzazione. Account AWS Ciò consente a più account di condividere una serie di criteri per l'ispezione e la gestione delle query DNS in uscita che passano attraverso Route 53 Resolver. Per ulteriori informazioni, consulta la sezione Condivisione dei gruppi di regole del firewall DNS 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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Itinerario 53 Profiles <code>route53profiles:Profile</code>	Crea e gestisci Route 53 Profiles centralmente e condividila con altri Account AWS o con la tua organizzazione. Ciò consente a più account di applicare le configurazioni DNS specificate in Route 53 Profiles a più account VPCs Per ulteriori informazioni, consulta Amazon Route 53 Profiles nella Amazon Route 53 Developer Guide.	 S	 S Può condividere con chiunque Account AWS.	 S	 No

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Regole 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 le query DNS 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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Configurazioni di registrazione delle query Resolver <code>route53resolver:ResolverQueryLogConfig</code>	Crea e gestisci i registri delle interrogazioni centralmente e condividili con altri o con la tua organizzazione. Account AWS Ciò consente di Account AWS registrare e più query DNS che hanno origine in un registro VPCs di query gestito centralmente. Per ulteriori informazioni, consulta la sezione <u>Condivisione delle configurazioni di registrazione delle query di Resolver con altre</u> nella Amazon Route 53 Account AWS 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 condividere con utenti e ruoli IAM	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 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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
SageMaker Cataloghi di risorse AI sagemaker:SagemakerCatalog	<p>Per la reperibilità: consente ai proprietari degli account di concedere autorizzazioni di reperibilità ad altri account, per tutte le risorse dei gruppi di funzionalità nel catalogo AI. SageMaker 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.</p>	 N	 S Può condividere con chiunque. Account AWS	 S	 No




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





Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
SageMaker Gruppi di funzionalità AI sagemaker: FeatureGroup	<p>Per l'accesso: consente ai proprietari di account di concedere le autorizzazioni di accesso ad altri account, per determinare 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.</p> <div data-bbox="399 1591 743 1818" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>La rilevabilità e l'accesso sono autorizzazioni</p> </div>	 S	 S Può condividere con chiunque. Account AWS	 S	 No

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	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 Hub AI <code>sagemaker:Hub</code>	Con Amazon SageMaker AI JumpStart, puoi crearli e gestirli <code>sagemaker:Hub</code> 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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
SageMaker Gruppi AI Lineage sagemaker:LineageGroup	Amazon SageMaker AI ti consente di creare gruppi di derivazione dei metadati della tua pipeline per comprendere 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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e 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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	Amazon SageMaker AI Developer Guide.				
SageMaker Gruppi di pacchetti AI Model 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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
SageMaker App per partner AI sagemaker:PartnerApp	Con SageMaker AI Partner AI Apps, puoi creare e gestire le app SageMaker AI Partner AI in modo centralizzato e condividerne l'accesso con altri Account AWS. Per ulteriori informazioni, consulta Configurazione della condivisione tra account per le app SageMaker AI partner di Amazon AI 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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e 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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e 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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
AppRegistry Applicazioni <code>servicecatalog:Applications</code>	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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	<p>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.</p>		<p>Account AWS con la propria organizzazione.</p>		





Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
AppRegistry Gruppi di attributi servicecatalog:AttributeGroups	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

Strumento di gestione degli incidenti AWS Systems Manager

È possibile condividere le seguenti Strumento di gestione degli incidenti AWS Systems Manager risorse utilizzando AWS RAM.

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Contatti di Incident Manager 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.	 S	 S Può condividere con chiunque Account AWS.	 S	 No
<div style="border: 1px solid #add8e6; border-radius: 15px; padding: 10px;"> <p> Note</p> <p>Attualmente, la possibilità di aggiungere un contatto condiviso da un altro account a un piano di risposta agli incidenti non è supportata.</p> </div>					

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	Per ulteriori informazioni, vedere Utilizzo dei contatti condivisi e dei piani di risposta nella Guida per l'utente di AWS Systems Manager Incident Manager.				

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Piani di risposta di Incident Manager <code>ssm-incidents:ResponsePlan</code>	Crea e gestisci i piani di risposta centralmente e condividili con altri Account AWS o con la tua organizzazione. Ciò consente di 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.	 S	 S Può condividere con chiunque Account AWS.	 S	 No

AWS Systems Manager

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





Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Politiche di rifiuto automatico di SMS JITNA ssm:Document	Crea una politica di approvazione per l'accesso ai just-in-time nodi con Systems Manager. Una policy di negazione dell'accesso impedisce esplicitamente l'approvazione automatica delle richieste di accesso ai nodi specificati. Condividi la politica di negazione dell'accesso con altri Account AWS o con la tua organizzazione. Ciò garantisce che la politica di negazione dell'accesso ai just-in-time nodi si applichi a tutti gli account dell'organizzazione. Per ulteriori informazioni, vedere	 S	 S Può condividere con chiunque Account AWS.	 S	 No

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	<p>l'accesso ai Just-in-time nodi tramite Systems Manager nella Guida AWS Systems Manager per l'utente.</p>				





Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Parameter Store Parametri avanzati <code>ssm:Parameter</code>	Crea un parametro e utilizzalo per archiviare i dati di configurazione a cui puoi fare riferimento negli script, nei comandi, nei documenti SSM 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 (Amazon VPC) utilizzando AWS RAM


Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
<p>Di proprietà del cliente IPv4pool</p> <p>ec2:CoipPool</p>	<p>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 sulla rete locale.</p> <p>Gli indirizzi IP di proprietà del cliente forniscono connettività locale o esterna alle risorse nelle sottoreti Outposts attraverso o la rete locale. Puoi assegnare questi indirizzi alle risorse del tuo Outpost, come le istanze EC2, utilizzando indirizzi IP elastici o utilizzando l'imposta</p>	<p> N</p>	<p> N</p> <p>Può condividere solo con la propria organizzazione. Account AWS</p>	<p> N</p>	<p> No</p>


Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	<p>zione 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 .</p>				





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

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare e le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
<p>Scoperte di risorse IPAM</p> <p><code>ec2:IpamResourceDiscovery</code></p>	<p>Condividi le scoperte di risorse con altri. Account AWS Un resource discovery è un componente IPAM di Amazon VPC che consente a IPAM di gestire e monitorare le risorse che appartengono all'account proprietario. Per ulteriori informazioni, consulta Lavorare con il rilevamento delle risorse nella Guida per l'utente IPAM di Amazon VPC.</p>	<p> N</p>	<p> S</p> <p>Può condividere con chiunque. Account AWS</p>	<p> N</p>	<p> No</p>





Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	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 proprie risorse, come i gruppi di sicurezza VPC e le tabelle di routing delle sottoreti. Per ulteriori informazioni, consulta Lavorare con 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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Sottoreti <code>ec2:Subnet</code>	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 in VPC gestiti centralmente. Queste risorse includono istanze Amazon EC2, 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 condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	<p> Note</p> <p>Per includere una sottorete quando crei una condivisione di risorse, devi disporre dei <code>ec2:DescribeVpcs</code> e <code>ec2:DescribeSubnets</code> permessi, oltre a <code>ram:CreateResourceShare</code>.</p> <p>Le sottoreti predefinite non sono condivisibili. È possibile condividere solo le sottoreti create dall'utente.</p>				

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	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 <code>ec2:SecurityGroup</code>	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 con Account AWS la propria organizzazione.	 S	 No





Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
<p>Traffic Mirror, obiettivi</p> <p><code>ec2:TrafficMirrorTarget</code></p>	<p>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.</p>	<p> N</p>	<p> S</p> <p>Può condividere con chiunque. Account AWS</p>	<p> N</p>	<p> No</p>


Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	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 Condivisi one di un gateway di transito nei gateway di transito Amazon VPC .	 No	 Sì Può condividere con chiunque Account AWS.	 No	 No

 **Note**

Per includere un gateway di transito quando crei una condivisi

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
	<p>one di risorse, devi disporre dell'ec2:DescribeTransitGateway autorizzazione in aggiunta a. ram:CreateResourceShare</p>				

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
<p>Domini multicast Transit Gateway</p> <p>ec2:TransitGatewayMulticastDomain</p>	<p>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.</p>	<p> N</p>	<p> S</p> <p>Può condividere con chiunque. Account AWS</p>	<p> N</p>	<p> No</p>

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
<p>Accesso verificato da AWS gruppi</p> <p><code>ec2:VerifiedAccessGroup</code></p>	<p>Crea e gestisci Accesso verificato da AWS i 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.</p>	<p> S</p>	<p> S</p> <p>Può condividere con chiunque Account AWS.</p>	<p> N</p>	<p> No</p>





Amazon VPC Lattice





Puoi condividere le seguenti risorse Amazon VPC Lattice utilizzando AWS RAM

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
Configurazione delle risorse Amazon VPC Lattice vpc-lattice:ResourceConfiguration	Crea una configurazione delle risorse in Amazon VPC Lattice per condividere le risorse VPC tra account e VPCs. Nella configurazione delle risorse, identifica chi può accedere a quella risorsa e specificare il gateway di risorse attraverso il quale condividere la risorsa. I consumatori possono accedere alla risorsa VPC tramite un endpoint VPC di risorse in cui creano. AWS PrivateLink. Per ulteriori informazioni, consulta Accesso alle risorse VPC AWS PrivateLink nella Guida per l'AWS PrivateLink utente e Configurazione delle risorse per le risorse	 N	 S Può condividere con chiunque. Account AWS	 S	 No

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

[VPC nella VPC Lattice](#) User Guide.

<p>Servizi Amazon VPC Lattice</p> <p>vpc-lattice:Service</p>	<p>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.</p>	<p> N</p>	<p> S</p> <p>Può condividere con chiunque. Account AWS</p>	<p> S</p>	<p> No</p>
--	--	--	--	--	---

Tipo e codice di risorsa	Caso d'uso	Può condividere con utenti e ruoli IAM	Può condividere con account esterni alla propria organizzazione	Può utilizzare le autorizzazioni gestite dal cliente	Può condividere con i responsabili del servizio
<p>Rete di servizi Amazon VPC Lattice</p> <p><code>vpc-lattice:ServiceNetwork</code></p>	<p>Crea e gestisci reti di servizi Amazon VPC Lattice centralmente e condividile con singoli utenti Account AWS o con la tua organizzazione. Ciò consente 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.</p>	<p> N</p>	<p> S</p> <p>Può condividere con chiunque. Account AWS</p>	<p> S</p>	<p> No</p>

Gestione delle autorizzazioni in AWS RAM

Nel AWS RAM, esistono [due tipi di autorizzazioni gestite, autorizzazioni](#) AWS gestite e autorizzazioni gestite dai clienti.

Le autorizzazioni gestite definiscono in che modo un consumatore può agire sulle risorse di 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 politica contenuto nell'autorizzazione gestita contiene tutto il necessario per una politica basata sulle risorse, ad eccezione del principale e della risorsa. L'Amazon Resource Name (ARN) della risorsa e l'ARN dei principali associati alla condivisione di risorse completano gli elementi di una policy basata sulle risorse. AWS RAM crea quindi la policy basata sulle risorse che allega a tutte le risorse di quella condivisione di risorse.

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

Note

Ti consigliamo di eseguire l'aggiornamento alla nuova versione dell'autorizzazione AWS gestita il prima possibile. Questi aggiornamenti in genere aggiungono il supporto per le risorse nuove o aggiornate Servizi AWS che possono essere utilizzate per condividere tipi di risorse aggiuntivi AWS RAM. Una nuova versione predefinita può inoltre risolvere e correggere le vulnerabilità di sicurezza.

Important

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

È possibile recuperare l'elenco delle autorizzazioni gestite disponibili in qualsiasi momento. Per ulteriori informazioni, consulta [Visualizzazione delle autorizzazioni gestite](#).

Argomenti

- [Visualizzazione delle autorizzazioni gestite](#)
- [Creazione e utilizzo delle autorizzazioni gestite dai clienti in AWS RAM](#)
- [Aggiornamento delle autorizzazioni AWS gestite a una versione più recente](#)
- [Considerazioni sull'utilizzo delle autorizzazioni gestite dal cliente in AWS RAM](#)
- [Come funzionano le autorizzazioni gestite](#)
- [Tipi di autorizzazioni gestite](#)

Visualizzazione delle autorizzazioni gestite

È possibile visualizzare i dettagli sulle autorizzazioni gestite disponibili per l'assegnazione ai tipi di risorse nelle condivisioni di risorse. È possibile identificare le autorizzazioni gestite assegnate alle condivisioni di risorse. Per visualizzare questi dettagli, utilizza la libreria di autorizzazioni gestite nella AWS RAM console.

Console

Per visualizzare i dettagli sulle autorizzazioni gestite disponibili in AWS RAM

1. Vai alla pagina della [libreria delle autorizzazioni gestite](#) 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, consulta [Condivisione delle risorse regionali rispetto alle risorse globali](#). Sebbene tutte le regioni condividano le stesse autorizzazioni AWS gestite disponibili, ciò influisce sul numero di condivisioni di risorse associate visualizzate per ogni autorizzazione gestita in [Step 5](#). Le autorizzazioni gestite dai clienti 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. Puoi utilizzare la casella di ricerca per filtrare l'elenco delle autorizzazioni gestite inserendo parte di un nome o di un 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. Puoi modificare le seguenti preferenze:

- Dimensioni della pagina: il numero di risorse visualizzate in ogni pagina.
- Avvolgere le linee: indica se avvolgere le linee 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 mostra 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: indica se l'autorizzazione gestita è un'autorizzazione AWS 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 con autorizzazione gestita: la versione dell'autorizzazione gestita allegata a questa condivisione di risorse.
 - Proprietario: il Account AWS numero del proprietario della condivisione di risorse.
 - Consenti responsabili esterni: indica se la condivisione di risorse consente la condivisione con responsabili esterni all'organizzazione all'interno. AWS Organizations
 - Stato: lo stato attuale dell'associazione tra la condivisione delle risorse e l'autorizzazione gestita.
- Stato: descrive se l'autorizzazione gestita è:
 - Allegabile: è possibile allegare l'autorizzazione gestita alle 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 eliminata a breve.
 - Eliminata: l'autorizzazione gestita è stata eliminata. Rimane visibile per due ore prima di scomparire dalla libreria di autorizzazioni gestite.

È possibile scegliere il nome dell'autorizzazione gestita per visualizzare ulteriori informazioni su tale autorizzazione gestita. La pagina dei dettagli di un'autorizzazione gestita visualizza le seguenti informazioni:

- Tipo di risorsa: il tipo di AWS risorsa a cui si applica questa autorizzazione gestita.
- Numero di versioni: puoi avere fino a cinque versioni di un'autorizzazione gestita dal cliente.
- Versione predefinita: specifica quale versione è quella predefinita e quindi viene assegnata automaticamente a tutte le nuove condivisioni di risorse che utilizzano questa autorizzazione gestita. In tutte le condivisioni di risorse esistenti che utilizzano versioni diverse viene visualizzato un messaggio che richiede all'utente di aggiornare la condivisione di risorse alla versione predefinita.
- ARN: [Amazon Resource Name \(ARN\)](#) dell'autorizzazione gestita. Le ARNs autorizzazioni AWS 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 con autorizzazione gestita: puoi scegliere le informazioni della versione da 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 di servizio, se applicabile, che questa versione dell'autorizzazione gestita consente ai responsabili 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 in AWS RAM

È possibile utilizzare il [list-permissions](#) comando per ottenere un elenco delle autorizzazioni gestite disponibili per le condivisioni di risorse nell'account corrente Regione 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 nome nel `--query` parametro del `list-permissions` AWS CLI comando. L'esempio seguente filtra l'output per includere solo gli elementi nei risultati dell'`permissionsarray` che corrispondono al nome specificato. Specifichiamo inoltre che vogliamo vedere solo il campo ARN nei risultati e in formato testo semplice anziché il 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 policy 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\t\"Effect\": \"Allow\",\n\t\t\"Action\": [\n\t\t\t\"ec2:GetIpamPoolAllocations\",\n\t\t\t\"ec2:GetIpamPoolCidrs\",\n\t\t\t\"ec2:AllocateIpamPoolCidr\",\n\t\t\t\"ec2:AssociateVpcCidrBlock\",\n\t\t\t\"ec2:CreateVpc\",\n\t\t\t\"ec2:ProvisionPublicIpv4PoolCidr\",\n\t\t\t\"ec2:ReleaseIpamPoolAllocation\"\n\t\t]\n\t\t}",
    "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 in AWS RAM

AWS Resource Access Manager (AWS RAM) fornisce almeno un'autorizzazione AWS gestita per ogni tipo di risorsa che puoi condividere. Tuttavia, tali autorizzazioni gestite potrebbero non fornire il [minimo privilegio di accesso](#) per il caso d'uso relativo alla condivisione. Quando una delle autorizzazioni AWS gestite fornite non funziona, puoi creare un'autorizzazione gestita dal cliente personalizzata.

Le autorizzazioni gestite dai clienti sono autorizzazioni gestite che crei e gestisci specificando con precisione quali azioni possono essere eseguite in quali condizioni con risorse condivise. 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 dai clienti 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.

Inoltre, è possibile aggiornare o eliminare le autorizzazioni gestite dai clienti in base alle esigenze.

Argomenti

- [Crea un'autorizzazione gestita dal cliente](#)
- [Crea una nuova versione di un'autorizzazione gestita dal cliente](#)
- [Scegli una versione diversa come impostazione predefinita per un'autorizzazione gestita dal cliente](#)
- [Eliminare una versione di autorizzazione gestita dal cliente](#)
- [Eliminare un'autorizzazione gestita dal cliente](#)

Crea un'autorizzazione gestita dal cliente

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

Console

Per creare un'autorizzazione gestita dal cliente

1. Esegui una delle seguenti operazioni:
 - Vai alla [libreria delle autorizzazioni gestite](#) e scegli Crea un'autorizzazione gestita dal cliente.
 - Vai 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 Policy template, si definiscono le operazioni che possono essere eseguite su questo tipo di risorsa.
 - È possibile scegliere Importa autorizzazioni gestite per utilizzare le azioni da 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 tag aggiuntivi scegliendo Aggiungi nuovo tag. Ripeti questo passaggio se necessario.

- 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 comando di esempio seguente 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. Vai 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 con autorizzazione gestita, scegli Crea versione.
4. Per Policy template, puoi aggiungere o rimuovere azioni e condizioni con l'editor visuale o l'editor JSON.

È inoltre possibile scegliere Importa autorizzazioni gestite per utilizzare un modello di policy esistente.

5. Quando hai finito, scegli Crea versione nella parte inferiore della pagina.

AWS CLI

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

1. Trova l'Amazon Resource Name (ARN) dell'autorizzazione gestita per la quale desideri creare una nuova versione. A tale scopo, richiama [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 richiamare l'[create-permission-version](#) operazione 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 impostazione predefinita per un'autorizzazione gestita dal cliente

Puoi impostare un'altra versione di autorizzazione gestita dal cliente come nuova versione predefinita.

Console

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

1. Vai 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 con autorizzazione gestita, utilizza l'elenco a discesa per scegliere la versione che desideri impostare come nuova versione predefinita.
4. Scegli Imposta come versione predefinita.
5. Quando viene visualizzata la finestra di dialogo, conferma che desideri che questa versione sia quella 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 comando di esempio seguente 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 richiamare l'[set-default-permission-version](#) operazione.

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

Questo comando non restituisce alcun output in caso di successo. È possibile eseguire [list-permission-versions](#) nuovamente 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 in uso, puoi eliminarla. Non puoi 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. Vai 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. Nella sezione Versioni della pagina, scegli la scheda Condivisioni di risorse associate per vedere se alcune condivisioni utilizzano questa versione.

Se sono associate 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 confermare che desideri eliminare 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-versions](#) operazione 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
```

Questo comando non restituisce alcun output in caso di successo. È possibile eseguire [list-permission-versions](#) nuovamente 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 lo stato eliminato.

Console

Per eliminare un'autorizzazione gestita dal cliente

1. Vai 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 ci siano 0 condivisioni associate dall'elenco delle autorizzazioni gestite prima di selezionare l'autorizzazione gestita dal cliente.

Se ci sono 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, scegli 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, forniscilo come parametro per delete-permission.](#)

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

Aggiornamento delle autorizzazioni AWS gestite a una versione più recente

Occasionalmente, AWS aggiorna le autorizzazioni AWS gestite disponibili da allegare a una condivisione di risorse per un tipo di risorsa specifico. Quando AWS esegue questa operazione, crea una nuova versione dell'autorizzazione AWS 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 tali 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 delle risorse utilizza una versione diversa da quella predefinita.

Inoltre, le autorizzazioni individuali possono visualizzare il pulsante **Aggiorna alla versione predefinita** accanto al numero della versione corrente quando tale versione non è quella predefinita.

La scelta di quel pulsante avvia la procedura guidata di [aggiornamento della condivisione delle risorse](#). Nel passaggio 2 della procedura guidata è possibile aggiornare la versione di tutte le autorizzazioni non predefinite per utilizzare le relative versioni predefinite.

Le modifiche vengono salvate solo dopo aver completato la procedura guidata scegliendo **Invia** nell'ultima pagina della procedura guidata.

Note

È possibile allegare solo la versione predefinita e non è possibile ripristinare un'altra versione.

Per le autorizzazioni gestite dai clienti, dopo aver aggiornato le autorizzazioni alla versione predefinita, non puoi applicare un'altra versione a una condivisione di risorse a meno che non 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 impostarla 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'autorizzazione AWS gestita

1. Esegui il comando [get-resource-shares](#) con il `--permission-arn` parametro per specificare l'[Amazon Resource Name \(ARN\)](#) dell'autorizzazione gestita che desideri aggiornare.

Ciò comporta 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'autorizzazione AWS 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 `--resource-share-arn` per specificare

la condivisione di risorse da aggiornare, `--permission-arn` per specificare quale autorizzazione AWS 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; viene utilizzata automaticamente la versione predefinita.

```
$ 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 del passaggio precedente per ogni `ResourceShareArn` comando ricevuto nei risultati del comando nel 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, vedere [Risorse 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 seguente video che dimostra come le autorizzazioni gestite ti consentano di applicare la best practice dell'accesso con privilegi minimi alle tue risorse.AWS

Questo video dimostra come creare e associare le autorizzazioni gestite dai clienti seguendo la best practice del privilegio minimo. Per ulteriori informazioni, consultare [???](#).

Quando si crea una condivisione di risorse, si associa un'autorizzazione AWS gestita a ciascun 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 `Allow` o dispone `Deny` dell'autorizzazione principale per eseguire un'operazione su una risorsa condivisa. Per un'autorizzazione gestita, l'effetto è sempre `Allow`. Per ulteriori informazioni, consulta [Effect](#) nella IAM User Guide.

Azione

L'elenco delle operazioni che il principale è autorizzato a eseguire. Può trattarsi di un'azione in Console di gestione AWS o di un'operazione in AWS Command Line Interface(AWS CLI) o AWS API. Le azioni sono definite dall'AWS autorizzazione. Per ulteriori informazioni, consulta [Action](#) nella IAM User Guide.

Condizione

Quando e come un principale può interagire con una risorsa in una condivisione di risorse. Le condizioni aggiungono un ulteriore livello di sicurezza alle risorse condivise. Utilizzale per limitare l'accesso per azioni sensibili alle risorse condivise. Ad esempio, è possibile includere condizioni che richiedono che le azioni provengano da uno specifico intervallo di indirizzi IP aziendali o che le azioni debbano essere eseguite da utenti autenticati con l'autenticazione a più fattori. Per ulteriori informazioni sulle condizioni, consulta le [chiavi di contesto delle condizioni AWS globali nella Guida](#) per l'utente IAM. Per ulteriori informazioni sulle condizioni specifiche del servizio, consulta [Azioni, risorse e chiavi di condizione per AWS i servizi](#) nel Service Authorization Reference.

Note

Sono disponibili condizioni per le autorizzazioni gestite dai clienti e i tipi di risorse supportati per AWS le autorizzazioni gestite.

Per informazioni sulle condizioni che sono escluse dall'uso con le autorizzazioni gestite dal cliente, vedere. [Considerazioni 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 ciascun tipo di risorsa incluso nella condivisione di risorse. AWS le autorizzazioni gestite sono definite dal servizio AWS proprietario della risorsa e gestite da AWS RAM. Sei tu a creare e gestire le tue autorizzazioni gestite dai clienti.

- **AWS autorizzazione gestita:** è disponibile un'autorizzazione gestita predefinita per ogni tipo di risorsa AWS 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 responsabili di eseguire le seguenti azioni:

- `ec2:RunInstances`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeSubnets`

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

Note

L'autorizzazione gestita predefinita è diversa 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, come l'accesso in lettura-scrittura o in sola lettura. Qualsiasi autorizzazione gestita, gestita dal cliente AWS o 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 un'autorizzazione gestita ad accesso completo (`ReadWrite`) 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 [procedura di concessione del privilegio minimo](#).

Note

Tutti i AWS servizi che funzionano con AWS RAM supportano almeno un'autorizzazione gestita predefinita. È possibile visualizzare le autorizzazioni disponibili per ciascuna di esse nella Servizio AWS pagina della [libreria delle autorizzazioni gestite](#). Questa pagina fornisce dettagli su ogni autorizzazione gestita disponibile, incluse eventuali condivisioni di risorse attualmente associate all'autorizzazione e se la condivisione con responsabili

esterni è consentita, 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, AWS RAM viene applicata automaticamente l'autorizzazione predefinita definita per il tipo di risorsa scelto. Se supportata, avrai anche la possibilità di scegliere Crea autorizzazione gestita dal cliente nella pagina Associa autorizzazioni gestite.

- **Autorizzazione gestita dal cliente:** le autorizzazioni gestite dai clienti sono autorizzazioni gestite che crei e gestisci specificando con precisione quali azioni possono essere eseguite in quali condizioni con risorse condivise. 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 dai clienti 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.

Sicurezza in AWS Resource Access Manager

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 (AWS RAM), consulta [Servizi coperti dal programma di conformitàAWS](#).
- **Sicurezza nel cloud:** la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria 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 Resource Access Manager](#)
- [Gestione delle identità e degli accessi per AWS Resource Access Manager](#)
- [Registrazione e monitoraggio AWS RAM](#)
- [Convalida della conformità per AWS Resource Access Manager](#)
- [Resilienza in AWS Resource Access Manager](#)
- [Sicurezza dell'infrastruttura in AWS Resource Access Manager](#)
- [Accesso AWS Resource Access Manager tramite un endpoint di interfaccia \(AWS PrivateLink\)](#)

Protezione dei dati in AWS Resource Access Manager

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 maggiori informazioni sulla privacy dei dati, consulta le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [AWS Modello di responsabilità condivisa e GDPR](#) nel AWS Blog sulla sicurezza.

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

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

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori AWS RAM o Servizi AWS utilizzi la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per la fatturazione o i log di diagnostica. Quando si fornisce un URL a un server esterno, suggeriamo

vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Gestione delle identità e degli accessi per AWS Resource Access Manager

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 di IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (dispone delle autorizzazioni) a utilizzare le risorse. AWS Utilizzando IAM, crei i principali, come ruoli, utenti e gruppi, all'interno del tuo Account AWS. Sei tu a controllare le autorizzazioni di cui dispongono i responsabili per eseguire attività utilizzando le risorse. AWS Puoi utilizzare IAM senza alcun costo aggiuntivo. Per ulteriori informazioni sulla gestione e la creazione di policy IAM personalizzate, consulta [Managing IAM policy](#) nella IAM User Guide.

Argomenti

- [Come AWS RAM funziona con IAM](#)
- [AWS politiche gestite per AWS Resource Access Manager](#)
- [Utilizzo di ruoli collegati ai servizi per AWS RAM](#)
- [Esempi di politiche IAM per AWS RAM](#)
- [Esempi di politiche di controllo dei servizi per AWS Organizations e AWS RAM](#)
- [Disabilitazione della condivisione delle risorse con AWS Organizations](#)

Come AWS RAM funziona con IAM

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

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

- Utenti e gruppi in AWS IAM Identity Center:

Creare 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 in IAM tramite un provider di identità:

Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina [Create a role for a third-party identity provider \(federation\)](#) della Guida per l'utente IAM.

- Utenti IAM:

- Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate nella pagina [Create a role for an IAM user](#) della Guida per l'utente IAM.
- (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina [Aggiunta di autorizzazioni a un utente \(console\)](#) nella Guida per l'utente IAM.

AWS RAM fornisce diverse politiche AWS gestite che è possibile utilizzare per soddisfare le esigenze di molti utenti. Per ulteriori informazioni su queste impostazioni, consulta [AWS politiche gestite per AWS Resource Access Manager](#).

Se hai bisogno di un controllo più preciso sulle autorizzazioni concesse ai tuoi utenti, puoi creare le tue policy nella console IAM. Per informazioni sulla creazione di policy e sulla loro associazione ai ruoli e agli utenti IAM, consulta [Policies and permissions in IAM nella User Guide](#).AWS Identity and Access Management

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

Indice

- [Struttura delle policy](#)
 - [Effetto](#)
 - [Azione](#)
 - [Risorsa](#)
 - [Condizione](#)

Struttura delle policy

Una policy di autorizzazione IAM è un documento JSON che include le seguenti dichiarazioni: Effect, Action, Resource e Condition. Una policy IAM 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 policy consente o nega l'autorizzazione principale per eseguire un'azione. I valori possibili includono: `Allow` e `Deny`.

Azione

L'istruzione `Action` specifica le azioni AWS RAM API per le quali la policy consente o nega l'autorizzazione. Per un elenco completo delle azioni consentite, consulta [Actions defined by AWS Resource Access Manager](#) nella IAM User Guide.

Risorsa

La dichiarazione `Resource` specifica le AWS RAM risorse interessate dalla policy. Per specificare una risorsa nell'istruzione, devi utilizzare il relativo Amazon Resource Name (ARN) univoco. Per un elenco completo delle risorse consentite, consulta [Resources defined by AWS Resource Access Manager](#) nella IAM User Guide.

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`— Specifica 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 `positiveFalse`, puoi condividere questa condivisione di risorse con gli account solo della stessa organizzazione.
- `ram:PermissionArn`— Verifica se l'ARN di autorizzazione specificato nella richiesta di servizio corrisponde a una stringa ARN specificata nella policy.
- `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 l'ARN del principale specificato nella richiesta di servizio corrisponde a una stringa ARN specificata nella policy.
- `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 l'ARN della risorsa su cui agisce la richiesta di servizio corrisponde a un ARN specificato nella policy.
- `ram:ResourceShareName`— Verifica se il nome della condivisione di risorse su cui agisce la richiesta di servizio corrisponde a una stringa specificata nella policy.
- `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 politiche gestite per AWS Resource Access Manager

AWS Resource Access Manager attualmente fornisce diverse politiche AWS RAM gestite, descritte in questo argomento.

AWS politiche gestite

- [AWS politica gestita: AWSResource AccessManagerReadOnlyAccess](#)
- [AWS politica gestita: AWSResource AccessManagerFullAccess](#)
- [AWS politica gestita: AWSResource AccessManagerResourceShareParticipantAccess](#)
- [AWS politica gestita: AWSResource AccessManagerServiceRolePolicy](#)
- [AWS RAM aggiornamenti alle politiche AWS gestite](#)

Nell'elenco precedente, puoi allegare le prime tre policy ai ruoli, ai gruppi e agli utenti IAM per concedere le autorizzazioni. L'ultima policy dell'elenco è riservata al ruolo collegato al AWS RAM servizio.

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

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando nel Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

AWS politica gestita: AWSResource AccessManagerReadOnlyAccess

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

Questo criterio fornisce autorizzazioni di sola lettura per le condivisioni di risorse di proprietà dell'utente. Account AWS

Lo fa concedendo il permesso di eseguire una qualsiasi delle operazioni o. `Get*` `List*` Non fornisce alcuna possibilità di modificare alcuna condivisione di risorse.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

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

JSON

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

AWS politica gestita: `AWSResource AccessManagerFullAccess`

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` operazione.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ram`— Consente ai responsabili di visualizzare o modificare qualsiasi informazione sulle condivisioni di risorse di proprietà di. Account AWS

JSON

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

AWS politica gestita: AWSResource AccessManagerResourceShareParticipantAccess

È possibile allegare la policy

AWSResourceAccessManagerResourceShareParticipantAccess alle identità IAM.

Questa politica offre ai mandanti la possibilità di accettare o rifiutare le condivisioni di risorse condivise con questo Account AWS provider e di visualizzare i dettagli su tali condivisioni di risorse. Non offre alcuna possibilità di modificare tali condivisioni di risorse.

Lo fa concedendo il permesso di eseguire alcune ram operazioni.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

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

JSON

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

AWS politica gestita: AWSResource AccessManagerServiceRolePolicy

La policy AWS gestita `AWSResourceAccessManagerServiceRolePolicy` può essere utilizzata solo con il ruolo collegato al servizio per. AWS RAM Non puoi allegare, scollegare, modificare o eliminare questa politica.

Questa politica fornisce AWS RAM l'accesso in sola lettura alla struttura dell'organizzazione. Quando abiliti l'integrazione tra AWS RAM e AWS Organizations, crea AWS RAM automaticamente un ruolo collegato al servizio denominato [AWSServiceRoleForResourceAccessManager](#) che il servizio assume quando deve cercare informazioni sull'organizzazione e sui relativi account, ad esempio quando si visualizza la struttura dell'organizzazione nella console. AWS RAM

A tale scopo, concede l'autorizzazione di sola lettura per eseguire `organizations:List` le operazioni `organizations:Describe` e le operazioni che forniscono dettagli sulla struttura e sugli account dell'organizzazione.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `organizations`— Consente ai dirigenti di visualizzare le informazioni sulla struttura dell'organizzazione, comprese le unità organizzative, e il contenuto in esse contenuto. Account AWS

JSON

```
{
  "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/*"
      ]
    }
  ]
}
```

AWS RAM aggiornamenti alle politiche AWS gestite

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

Modifica	Descrizione	Data
AWS Resource Access Manager ha iniziato a tenere traccia delle modifiche	AWS RAM ha documentato le politiche gestite esistenti e ha iniziato a tenere traccia delle modifiche.	16 settembre 2021

Utilizzo di ruoli collegati ai servizi per AWS RAM

AWS Resource Access Manager utilizza ruoli collegati ai [servizi AWS Identity and Access Management](#) (IAM). Un ruolo collegato al servizio è un tipo unico di ruolo IAM collegato direttamente al servizio. AWS RAM 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 RAM definisce 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 di ruolo collegate al servizio per AWS RAM

AWS RAM utilizza 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 dei 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 Console di gestione AWS esegui [EnableSharingWithAwsOrganization](#) nel tuo account utilizzando AWS CLI o un' AWS API, 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 al servizio per AWS RAM

AWS RAM non consente di modificare il ruolo collegato al `AWSResourceAccessManagerServiceRolePolicy` servizio. Dopo avere creato un ruolo collegato al servizio, non sarà possibile 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 al servizio per AWS RAM

Puoi utilizzare la console IAM, AWS CLI o l' AWS API per eliminare manualmente il ruolo collegato al servizio.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al `AWSResourceAccessManagerServiceRolePolicy` servizio. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato al servizio](#) 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 al servizio 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.

Esempi di politiche IAM per AWS RAM

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

Esempi di politiche 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 siti esterni Account AWS](#)

Esempio 1: consentire la condivisione di risorse specifiche

Puoi utilizzare una policy di autorizzazione IAM per limitare i principali all'associazione solo di risorse specifiche a condivisioni di risorse.

Ad esempio, la seguente policy limita i principali alla condivisione della sola 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, se il suo valore corrisponde esattamente all'ARN specificato.

[Per ulteriori informazioni su quando e perché utilizzare gli `IfExists` operatori, consulta... `IfExists` condition operator](#) nella IAM User Guide.

JSON

```
{
  "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 principali all'associazione solo di tipi di risorse specifici alle condivisioni di risorse.

Le azioni `AssociateResourceShare` e `CreateResourceShare` possono accettare i principi e `resourceArns` come parametri di input indipendenti. Pertanto, AWS RAM autorizza ogni principale e risorsa in modo indipendente, quindi potrebbero esserci più contesti di [richiesta](#). Ciò significa che quando un principale viene associato a una condivisione di AWS RAM risorse, la chiave di `ram:RequestedResourceType` condizione non è presente nel contesto della richiesta. Allo stesso modo, quando una risorsa viene associata a una condivisione di AWS RAM risorse, la chiave di `ram:Principal` condizione non è presente nel contesto della richiesta. Pertanto, per consentire `AssociateResourceShare` e `CreateResourceShare` quando si associano i principali alla condivisione di AWS RAM risorse, è possibile utilizzare l'operatore [Nullcondition](#).

Ad esempio, la seguente policy limita i principali a condividere solo le regole del resolver Amazon Route 53 e consente loro di associare qualsiasi principale a quella condivisione.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowOnlySpecificResourceType",
    "Effect": "Allow",
    "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
    "Resource": "*",
    "Condition": {

```

```

        "StringEquals": {
            "ram:RequestedResourceType": "route53resolver:ResolverRule"
        }
    },
    {
        "Sid": "AllowAssociatingPrincipals",
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "Null": {
                "ram:Principal": "false"
            }
        }
    }
]
}

```

Esempio 3: limita la condivisione con siti esterni Account AWS

Puoi utilizzare una policy IAM per impedire ai responsabili di condividere risorse con Account AWS soggetti esterni all' AWS organizzazione.

Ad esempio, la seguente policy IAM impedisce ai responsabili di aggiungere elementi esterni Account AWS alle condivisioni di risorse.

JSON

```

{
    "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). SCPs sono politiche che allegare agli elementi di un'organizzazione per gestire le autorizzazioni all'interno di tale organizzazione. Un SCP si applica a tutti gli elementi Account AWS [inclusi nell'elemento a cui si collega l'SCP](#). SCPs offrono il controllo centralizzato sulle autorizzazioni massime disponibili per tutti gli account della vostra 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 utilizzarlo SCPs, 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 creazione SCPs, consulta [Creazione e aggiornamento SCPs](#) nella Guida AWS Organizations per l'utente.

Policy di controllo dei servizi di esempio

Indice

- [Esempio 1: Impedire la condivisione esterna](#)
- [Esempio 2: Impedisci agli utenti di accettare inviti alla condivisione di risorse da account esterni all'organizzazione](#)
- [Esempio 3: consentire ad account specifici di condividere tipi di risorse specifici](#)
- [Esempio 4: Impedire la condivisione con l'intera organizzazione o con le unità organizzative](#)
- [Esempio 5: consenti la condivisione solo con principali specifici](#)
- [Esempio 6: Impedisci la condivisione delle risorse se abilitato `RetainSharingOnAccountLeaveOrganization`](#)

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

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

AWS RAM autorizza APIs separatamente per ogni principale e risorsa elencati nella chiamata.

JSON

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

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

Il seguente SCP impedisce a qualsiasi principale 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 sono interessate da questo SCP.

JSON

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

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

Il seguente SCP consente solo di 222222222222 creare account 111111111111 e nuove condivisioni di risorse che condividono elenchi di prefissi Amazon EC2 o di associare elenchi di prefissi a condivisioni di risorse esistenti.

AWS RAM autorizza APIs separatamente per ogni principale e risorsa elencati nella chiamata.

L'operatore `StringEqualsIfExists` consente una richiesta se la richiesta non include un parametro del tipo di risorsa o, se include quel parametro, se il suo valore corrisponde esattamente al tipo di risorsa specificato. Se stai includendo un preside devi averlo...`IfExists`.

Per ulteriori informazioni su quando e perché utilizzare ...`IfExists` gli operatori, consulta... [IfExists condition operator](#) nella IAM User Guide.

JSON

```
{
  "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

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

AWS RAM autorizza APIs separatamente per ogni principale e risorsa elencati nella chiamata.

JSON

```

{
  "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 principali 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

Se si utilizza un "Effect": "Deny" elemento con un operatore di condizione negata, ad esempio `StringNotEqualsIfExists`, la richiesta viene comunque negata anche se la chiave di condizione non è presente. Utilizza un operatore di condizione `Null` per verificare se una chiave di condizione è presente o meno al momento dell'autorizzazione.

AWS RAM autorizza APIs separatamente per ogni principale e risorsa elencati nella chiamata.

JSON

```

{
  "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"
      }
    }
  ]
}

```

```

    }
  }
]
}

```

Esempio 6: Impedisce la condivisione delle risorse se abilitato RetainSharingOnAccountLeaveOrganization

Il seguente SCP impedisce agli utenti di creare o modificare condivisioni di risorse quando la chiave di `ram:RetainSharingOnAccountLeaveOrganization` condizione è impostata su `true`

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:CreateResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare"
      ],
      "Resource": "*",
      "Condition": {
        "Bool": {
          "ram:RetainSharingOnAccountLeaveOrganization": "true"
        }
      }
    }
  ]
}

```

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 (OUs), puoi disabilitare la condivisione. Quando disabiliti la condivisione con AWS Organizations, tutte le organizzazioni OUs vengono rimosse dalle condivisioni di risorse che hai creato 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 Organizations utilizzo del AWS Organizations [disable-aws-service-access](#) AWS CLI comando.

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

Important

Quando si disabilita 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.

2. Utilizza la console IAM AWS 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 automatizzate in altri AWS servizi quando si verificano tali eventi. Per ulteriori informazioni, consulta [Monitoraggio AWS RAM tramite EventBridge](#).

AWS CloudTrail

Acquisisce le chiamate API 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 AWS RAM API 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 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

Considera lo scenario in cui desideri condividere le prenotazioni di capacità di Amazon EC2 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 EC2 si 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 Amazon SNS, consultare la [Guida per gli sviluppatori di Amazon Simple Notification Service](#).

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 (editor JSON).
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 target, scegli l'argomento SNS.
9. Per Argomento, scegli l'argomento SNS 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 questa regola è abilitata, qualsiasi condivisione di AWS RAM risorse che non riesce genera un avviso SNS ai 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 console Amazon EC2 da](#) tali account.

Registrazione delle chiamate AWS RAM API con AWS CloudTrail

AWS RAM è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, un ruolo o un AWS servizio in AWS RAM. CloudTrail acquisisce tutte le chiamate API AWS RAM come eventi. Le chiamate acquisite includono chiamate dalla AWS RAM console e chiamate di codice alle operazioni AWS RAM API. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3 da te specificato, inclusi gli eventi per cui. AWS RAM Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizza le informazioni raccolte da CloudTrail per determinare la richiesta a cui è stata effettuata AWS RAM, l'indirizzo IP richiedente, il richiedente, quando è stata effettuata e altri dettagli.

Per ulteriori informazioni in merito CloudTrail, consulta la Guida per l'[AWS CloudTrail utente](#).

AWS RAM informazioni in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in AWS RAM, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti in Account AWS. Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi nell' Account AWS che includa gli eventi per AWS RAM, crea un trail. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un percorso nella console, il percorso si applica a tutte le AWS regioni. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consultare gli argomenti seguenti:

- [Creare un percorso per il tuo Account AWS](#)
- [Servizio AWS integrazioni con log CloudTrail](#)
- [Configurazione delle notifiche Amazon SNS per CloudTrail](#)
- [Ricezione di file di CloudTrail registro da più regioni](#) e [ricezione di file di CloudTrail registro da più account](#)

Tutte AWS RAM le azioni vengono registrate CloudTrail e documentate nell'[AWS RAM API 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 AWS credenziali root
- Credenziali di sicurezza temporanee da un ruolo AWS Identity and Access Management (IAM) o da 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](#).

Comprendere AWS RAM le voci dei file di registro

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

L'esempio seguente mostra una voce di CloudTrail registro per l'`CreateResourceShare`azione.

```
{
  "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"
}
```

Convalida della conformità per AWS Resource Access Manager

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione [Scope by Compliance Program Servizi AWS](#) e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di [AWS conformità Programmi](#) di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Scaricamento dei report in AWS Artifact](#) .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. Per ulteriori informazioni sulla responsabilità di conformità durante l'utilizzo Servizi AWS, consulta la [Documentazione AWS sulla sicurezza](#).

Resilienza in AWS Resource Access Manager

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza,

ad alto throughput e altamente ridondanti. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

[Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS](#)

Sicurezza dell'infrastruttura in AWS Resource Access Manager

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.

Utilizzate chiamate API AWS pubblicate per accedere AWS RAM attraverso la rete. I client devono supportare quanto segue:

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

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

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

Stabilisci questa connessione privata creando un endpoint di interfaccia attivato da AWS PrivateLink. In ciascuna sottorete viene creata un'interfaccia di rete endpoint da abilitare per l'endpoint di interfaccia. Queste sono interfacce di rete gestite dal richiedente che fungono da punto di ingresso per il traffico destinato a AWS RAM.

Per ulteriori informazioni, consulta la sezione [Accesso a Servizi AWS tramite AWS PrivateLink](#) nella Guida di AWS PrivateLink .

Considerazioni per AWS RAM

Prima di configurare un endpoint di interfaccia per AWS RAM, consulta [le considerazioni nella Guida](#).AWS PrivateLink

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

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

Crea un endpoint di interfaccia per AWS RAM

Puoi creare un endpoint di interfaccia per AWS RAM utilizzare la console Amazon VPC o AWS Command Line Interface ().AWS CLI Per ulteriori informazioni, consulta la sezione [Creazione di un endpoint di interfaccia](#) nella Guida per l'utente di AWS PrivateLink .

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

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

Se abiliti il DNS privato per l'endpoint dell'interfaccia, puoi effettuare richieste API AWS RAM utilizzando il nome DNS regionale predefinito. Ad esempio, ram.us-east-1.amazonaws.com.

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

Una policy dell'endpoint è una risorsa IAM che è possibile allegare all'endpoint dell'interfaccia. La policy predefinita per gli endpoint consente l'accesso completo AWS RAM tramite l'endpoint dell'interfaccia. Per controllare l'accesso consentito AWS RAM dal tuo VPC, collega una policy endpoint personalizzata all'endpoint di interfaccia.

Una policy di endpoint specifica le informazioni riportate di seguito:

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

Per ulteriori informazioni, consulta la sezione [Controllo dell'accesso ai servizi con policy di endpoint](#) nella Guida di AWS PrivateLink .

Esempio: policy degli endpoint VPC per le azioni AWS RAM

Di seguito è riportato l'esempio di una policy dell'endpoint personalizzata. Quando alleggi questa policy all'endpoint dell'interfaccia, concede l'accesso alle AWS RAM azioni elencate per tutti i principali su tutte le risorse.

JSON

```
{
  "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 (RAM).

Argomenti

- [Errore: «L'ID del tuo account non esiste in un' AWS organizzazione»](#)
- [Errore: "AccessDeniedException»](#)
- [Errore: "UnknownResourceException»](#)
- [Errori durante il tentativo di condivisione con account esterni alla mia organizzazione](#)
- [Non riesco a visualizzare le risorse condivise nell'account di destinazione](#)
- [Errore: limite superato](#)
- [L'altro account della mia organizzazione non riceve mai un invito](#)
- [Non puoi condividere una sottorete VPC](#)

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 [AWSServiceRoleForResourceAccessManager](#) non viene creato correttamente quando si attiva l'integrazione tra AWS Resource Access Manager e 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 all'interno dell'organizzazione vengono rimossi da tutte le condivisioni di risorse e perdono l'accesso a tali risorse condivise.

1. Accedi all'account di gestione della tua organizzazione utilizzando un ruolo IAM 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 principale AWS Identity and Access Management (IAM). Può verificarsi anche a causa delle restrizioni imposte da una policy di controllo dei AWS Organizations servizi (SCP) che influiscono sulla tua. Account AWS

Soluzione

Per fornire l'accesso, aggiungi autorizzazioni agli 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 in IAM tramite un provider di identità:

Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina [Create a role for a third-party identity provider \(federation\)](#) della Guida per l'utente IAM.

- Utenti IAM:

- Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate nella pagina [Create a role for an IAM user](#) della Guida per l'utente IAM.

- (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina [Aggiunta di autorizzazioni a un utente \(console\)](#) nella Guida per l'utente IAM.

Per risolvere l'errore, è necessario assicurarsi 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 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 autorizzazione IAM di questo tipo.

JSON

```
{
  "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 ou- **xxxx** non è stato trovato»
- «CannotUpdateResourceShare: UnknownResourceException: OrganizationalUnit ou- **xxxx** non è stato trovato».

Causa

Questi errori possono verificarsi se si abilita l'integrazione tra AWS RAM e AWS Organizations utilizzando la [console Organizations](#) o l'[API Organizations Enable AWSService Access](#) anziché

[utilizzando la AWS RAM console](#). Quando abiliti l'integrazione utilizzando la console o l'API Organizations, 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'operazione AWS RAM [EnableSharingWithAwsOrganization](#)API o utilizzando il Console di gestione AWS per eseguire i passaggi seguenti.

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 all'account di gestione della tua organizzazione utilizzando un ruolo IAM 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 tua 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 (VPC) che fanno parte di Amazon Elastic Compute Cloud (Amazon EC2).

[Per verificare se è possibile condividere un particolare tipo di risorsa con account e responsabili esterni all'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 all'account di gestione della tua organizzazione utilizzando un ruolo IAM 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 all'account di gestione della tua organizzazione utilizzando un ruolo IAM 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 ruoli e agli utenti IAM dell'account B che devono accedere alla risorsa. Ad esempio, la seguente politica mostra come è possibile 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 relativo [Amazon Resource Name \(ARN\)](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ram:Get*",
        "ram:List*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:<service>:us-east-1:<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 Console di gestione AWS 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 in alto a destra 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 tue 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 sottorete VPC

Scenario

Quando si tenta di AWS RAM condividere una sottorete VPC con un altro account, l'operazione di condivisione ha esito positivo. Tuttavia, l'account utente viene visualizzato LIMIT EXCEEDED per quella risorsa nella console. AWS RAM

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 (Amazon VPC) 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 — Condivisione VPC](#) nella 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 affinché la RAM rilevi la modifica.

Quote di servizio per AWS RAM



Your Account AWS ha i 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 [Supporto](#).

Note

Le seguenti definizioni si applicano alla descrizione nelle quote seguenti:

- **Risorsa:** un elemento Servizio AWS creato individualmente che desideri condividere, ad esempio un bucket Amazon S3 o un'istanza Amazon. EC2 Ogni risorsa referenziata in una condivisione di risorse conta come una risorsa ai fini di tale quota. Se condividi la stessa risorsa in tre diverse condivisioni di risorse, il conteggio per questa quota aumenta di tre.
- **Condivisione di risorse:** un contenitore AWS RAM creato che puoi utilizzare per condividere risorse. Ogni condivisione di risorse, indipendentemente dal numero di risorse che contiene, viene conteggiata come un'unica risorsa ai fini della quota.
- **Principio condiviso:** un identificatore che hai associato a una condivisione di risorse. Può essere un ruolo o un utente AWS Identity and Access Management (IAM), un Account AWS identificatore, un'unità organizzativa o un'intera organizzazione. Ogni principale condiviso a cui fai riferimento in una condivisione di risorse ne aggiunge uno all'utilizzo della quota. Se lo condividi con un'intera organizzazione facendo riferimento al relativo ID, ai fini di questa quota viene conteggiato solo uno.
- **Autorizzazione gestita dal cliente:** autorizzazioni gestite create per risolvere 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 tra tutte le condivisioni di risorse in un Regione AWS	25.000
<div data-bbox="142 949 181 989"></div> <p>Note</p> <p>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, 10 vengono conteggiate ai fini del limite.</p>	
Numero massimo di associazioni principali tra tutte le condivisioni di risorse in un Regione AWS	25.000
<div data-bbox="142 1524 181 1564"></div> <p>Note</p> <p>Ogni principale incluso in una condivisione di risorse viene conteggiato ai fini di questo limite. Se un capitale è incluso in 10 diverse condivisioni di risorse, 10 rientrano nel limite.</p>	

Risorsa	Limite predefinito
<p data-bbox="115 226 688 306">Numero massimo di inviti in sospeso per account di condivisione</p> <ul data-bbox="115 352 781 886" style="list-style-type: none"><li data-bbox="115 352 781 485">• Questa quota si applica solo agli account di invio che condividono con account che non fanno parte dello stesso. AWS Organizations<li data-bbox="115 506 781 638">• Non esiste una quota per limitare il numero di inviti in sospeso che un account ricevente può avere.<li data-bbox="115 659 781 886">• Gli inviti non vengono utilizzati per la condivisione tra account che fanno parte dello stesso AWS Organizations e hai attivato la condivisione delle risorse all'interno di. AWS Organizations	250

Utilizzo AWS RAM con un AWS SDK

AWS i kit di sviluppo software (SDKs) sono disponibili per molti dei linguaggi di programmazione più diffusi. Ogni SDK fornisce un'API, esempi di codice e documentazione che aiutano gli sviluppatori a creare applicazioni nella loro lingua preferita.

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

Esempio di disponibilità

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 feed AWS RAM RSS.

Modifica	Descrizione	Data
Aggiunto il supporto per la condivisione di CloudFront risorse Amazon	Ora puoi condividere Amazon CloudFront VPC Origins con altri membri Account AWS della tua organizzazione.	6 ottobre 2025
Aggiunto supporto per condividere le risorse di Billing and Cost Management	Ora puoi condividere i dashboard di Billing and Cost Management con Account AWS altri utenti o con la tua organizzazione. AWS RAM	19 agosto 2025
È stato aggiunto il supporto per la condivisione delle risorse AWS Cloud Map	Ora puoi condividere i AWS Cloud Map namespace con altri membri della tua Account AWS organizzazione.	14 agosto 2025
Aggiunto il supporto per condividere le risorse di Amazon Application Recovery Controller (ARC)	Ora puoi condividere i piani di Amazon Application Recovery Controller (ARC) con altre Account AWS persone o con la tua organizzazione AWS RAM.	31 luglio 2025
È stato aggiunto il supporto per la condivisione Oracle Database@AWS delle risorse	Ora puoi condividere l'infrastruttura Oracle Database@AWS Exadata e le reti ODB	30 giugno 2025

	con altri membri della tua Account AWS organizzazione.	
<u>È stato aggiunto il supporto per la condivisione di risorse di approvazione multipartitiche</u>	Ora puoi condividere team di approvazione multipartitici con altri Account AWS o all'interno della tua organizzazione.	17 giugno 2025
<u>Aggiunto supporto per la condivisione di risorse Amazon SageMaker AI</u>	Ora puoi utilizzarle AWS RAM per condividere le app Amazon SageMaker AI Partner con altri Account AWS e con la tua organizzazione.	6 giugno 2025
<u>È stato aggiunto il supporto per la condivisione AWS Network Firewall delle risorse</u>	Ora puoi utilizzarli AWS RAM per condividere AWS Network Firewall i firewall con altri Account AWS e con la tua organizzazione.	28 maggio 2025
<u>È stato aggiunto il supporto per la condivisione di risorse AWS Systems Manager</u>	Puoi condividere una politica di AWS Systems Manager negazione dell'accesso con altre persone Account AWS o con le tue organizzazioni. AWS RAM	30 aprile 2025
<u>È stato aggiunto il supporto per la condivisione delle risorse AWS CodeConnections</u>	Ora puoi condividere connessioni di AWS CodeConnections codice con altri utenti Account AWS o all'interno dell'organizzazione.	5 marzo 2025
<u>È stato aggiunto il supporto per la condivisione di AWS Billing risorse</u>	Ora puoi condividere le AWS Billing visualizzazioni con altri membri Account AWS della tua organizzazione.	20 dicembre 2024

Aggiunto supporto per la condivisione delle configurazioni di risorse Amazon VPC Lattice	Ora puoi condividere le configurazioni delle risorse Amazon VPC Lattice con altri Account AWS	1 dicembre 2024
È stato aggiunto il supporto per la condivisione delle risorse di 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
Aggiunto supporto per la condivisione di risorse Amazon VPC	Ora puoi condividere i gruppi di Amazon VPC Security con altri Account AWS o all'interno della tua organizzazione.	30 ottobre 2024
È stato aggiunto il supporto per la condivisione di risorse AWS End User Messaging SMS	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 alla RAM utilizzando 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
È stato aggiunto il supporto per la condivisione delle risorse Elastic Load Balancing	Puoi condividere gli archivi di fiducia Elastic Load Balancing all'interno Account AWS o all'interno della tua organizzazione.	5 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 organizzazione.	1° agosto 2024
È stato aggiunto il supporto per la condivisione dei backup AWS CloudHSM	Puoi condividere i AWS CloudHSM backup con altre persone Account AWS o con le tue organizzazioni. AWS RAM	28 giugno 2024
È stato aggiunto il supporto per condividere le Model Registry risorse di SageMaker intelligenza artificiale di Amazon.	Ora puoi condividere parametri avanzati in modo sicuro ed efficiente all'interno della tua organizzazione Account AWS o all'interno di essa.	27 giugno 2024
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 organizzazione.	27 giugno 2024
È stato aggiunto il supporto per la condivisione Amazon Route 53 ResolverProfiles	Ora puoi AWS RAM utilizzarlo per condividere Amazon Route 53 Resolver Profiles con altri membri Account AWS 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

Aggiunto il supporto per condividere le istantanee di Amazon FSx for OpenZFS	Ora puoi condividere le istantanee di Amazon FSx for OpenZFS con altri membri della tua Account AWS organizzazione.	19 dicembre 2023
È stato aggiunto il supporto per la condivisione di risorse Amazon Simple Storage Service	Ora puoi condividere Amazon Simple Storage Service l'istanza di Access Grants con altre persone Account AWS o con AWS RAM la tua organizzazione.	27 novembre 2023
È stato aggiunto il supporto per condividere le visualizzazioni Esploratore di risorse AWS	Ora puoi condividere le Esploratore di risorse AWS visualizzazioni con altri membri Account AWS della tua organizzazione.	14 novembre 2023
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
Aggiunto il supporto per condividere le DataZone 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
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
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 i 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 di 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
Aggiornamento delle best practice di IAM	Guida aggiornata per l'allineamento alle best practice IAM. Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM .	3 gennaio 2023
È stato aggiunto il supporto per i gruppi di collocamento di Amazon EC2 come risorse condivisibili	Ora puoi condividere i gruppi di collocamento di Amazon EC2 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
Aggiunto 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 riceve le certificazioni SOC e ISO	AWS RAM è stato convalidato come conforme agli standard Service Organization Control (SOC) e International Organization for Standardization (ISO) ISO 9001, ISO 27001, ISO 27017, ISO 27018 e ISO 27701.	31 maggio 2022
AWS Resource Access Manager riceve la certificazione FedRAMP	AWS RAM è stato convalidato come conforme al Federal Risk and Authorization Management Program (FedRAMP).	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 l'individuazione di risorse IPAM di Amazon VPC come risorse condivisibili. Inoltre, ora puoi condividere i pool IPAM con account esterni all'organizzazione	Ora puoi condividere le scoperte di risorse IPAM 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 principali AWS Cloud WAN come risorse globali condivisibili	Ora puoi condividere le reti principali Cloud WAN con altri Account AWS.	2 dicembre 2021
Supporto per la condivisione di pool di Amazon VPC IP Address Manager (IPAM)	Puoi utilizzarlo AWS RAM per condividere i pool IPAM di Amazon VPC. Per ulteriori informazioni, consulta AWS Risorse condivisibili nella Guida per l'AWS RAM utente.	1° dicembre 2021
Supporto per la condivisione di risorse Amazon SageMaker AI	Puoi usarlo AWS RAM per condividere i gruppi di discendenza dell' SageMaker IA. Per ulteriori informazioni, consulta AWS Risorse condivisibili nella Guida per l'AWS RAM utente.	30 novembre 2021
Supporto 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 autorizzazione IAM gestite	Sono stati pubblicati dettagli sulle politiche di autorizzazione AWS gestite disponibili a cui puoi accedere nella console IAM e allegare ai principali IAM del tuo Account AWS	16 settembre 2021

<u>Aggiunto il supporto per la condivisione di S3 sulle risorse Outposts</u>	Ora puoi usarlo AWS RAM per condividere S3 su Outposts con altri. Account AWS	5 agosto 2021
<u>È stato aggiunto il supporto per autorizzazioni gestite aggiuntive e la condivisione di risorse con i responsabili IAM</u>	Per i tipi di risorse supportati, puoi scegliere tra autorizzazioni AWS RAM gestite aggiuntive e condividere risorse con singoli ruoli e utenti IAM.	10 giugno 2021
<u>È stato aggiunto il supporto per la condivisione delle risorse AWS di Systems Manager Incident Manager</u>	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
<u>È stato aggiunto il supporto per la condivisione di risorse Amazon Route 53</u>	Ora puoi usare AWS RAM per condividere i gruppi di regole del firewall DNS di Amazon Route 53 Resolver con altri. Account AWS	31 marzo 2021
<u>È stato aggiunto il supporto per la condivisione di risorse AWS Transit Gateway</u>	Ora puoi utilizzarli AWS RAM per condividere i domini multicast del gateway di transito con altri. Account AWS	10 dicembre 2020
<u>È stato aggiunto il supporto per la condivisione delle risorse AWS Network Firewall</u>	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	07 settembre 2020
È stato aggiunto il supporto per la condivisione delle risorse AWS Autorità di certificazione privata	Ora puoi usare AWS RAM per condividere le autorità di certificazione CA privata AWS private (CAs) con altri Account AWS.	17 agosto 2020
Aggiunto il supporto per la condivisione di cataloghi di dati, database e tabelle di AWS Glue	Ora puoi usare AWS RAM per condividere cataloghi di dati, database e tabelle di AWS Glue con altri Account AWS.	7 luglio 2020
Aggiunto il supporto per la condivisione degli elenchi di prefissi Amazon VPC	Ora puoi utilizzarlo AWS RAM per condividere elenchi di prefissi.	29 giugno 2020
È stato aggiunto il supporto per la condivisione degli indirizzi di proprietà AWS Outposts dei clienti IPv4	Ora puoi utilizzarlo AWS RAM per condividere gli indirizzi di AWS Outposts proprietà del cliente con altri IPv4 . 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 utilizzarlo 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 usare AWS RAM per condividere host dedicati di Amazon EC2, 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 prenotazioni 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 sottoreti Amazon VPC 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 transito Amazon VPC 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.