Guida per l'utente

AWS Resource Groups

AWS Resource Groups: Guida per l'utente

Table of Contents

Cosa sono i gruppi di risorse?

Puoi utilizzare i gruppi di risorse per organizzare AWS le tue risorse. AWS Resource Groups è il servizio che consente di gestire e automatizzare le attività su un gran numero di risorse contemporaneamente. In questa guida viene illustrato come creare e gestire i gruppi di risorse in AWS Resource Groups. Le attività che è possibile eseguire su una risorsa variano in base al AWS servizio utilizzato. Per un elenco dei servizi che supportano AWS Resource Groups e una breve descrizione di ciò che ciascun servizio consente di fare con un gruppo di risorse, consultaAWS servizi che funzionano con AWS Resource Groups.

È possibile accedere a Resource Groups tramite uno dei seguenti punti di ingresso.

- Nella barra AWS Management Consoledi navigazione in alto, scegli Servizi. Quindi, in Management & Governance, scegli Resource Groups & Tag Editor.

  Link diretto: AWS Resource Groups console
- Utilizzando i Resource GroupsAPI, nei AWS CLI comandi o nei linguaggi AWS SDK di programmazione. Vedi il AWS Resource Groups APIriferimento per ulteriori informazioni.

Per lavorare con i gruppi di risorse AWS Management Console a casa

1. Accedi alla AWS Management Console.
2. Sulla barra di navigazione, scegli Services (Servizi).
3. In Management & Governance, scegli Resource Groups & Tag Editor.
4. Nel riquadro di navigazione a sinistra, scegli Saved Resource Groups per lavorare con un gruppo esistente o Crea un gruppo per crearne uno nuovo.

Risorse e relativi tipi di gruppo

In AWS, una risorsa è un'entità con cui è possibile lavorare. Gli esempi includono un'EC2istanza Amazon, uno AWS CloudFormation stack o un bucket Amazon S3. Se lavori con più risorse, potresti trovare utile gestirle in gruppo anziché passare da un AWS servizio all'altro per ogni attività. Se gestisci un gran numero di risorse correlate, ad esempio EC2 le istanze che costituiscono un livello applicativo, probabilmente dovrai eseguire azioni in blocco su queste risorse contemporaneamente. Esempi di azioni in blocco includono:

- Applicazione di aggiornamenti o patch e di sicurezza.
- Aggiornamento di applicazioni.
- Apertura o chiusura di porte al traffico di rete.
- Raccolta di dati di monitoraggio e di log specifici dal parco istanze.

Un gruppo di risorse è una raccolta di AWS risorse che sono tutte uguali Regione AWS e che corrispondono ai criteri specificati nella query del gruppo. In Resource Groups, esistono due tipi di query che è possibile utilizzare per creare un gruppo. Entrambi i tipi di query includono le risorse specificate nel formato `AWS::service::resource`.

- Tag-based (Basato su tag)

  Un gruppo di risorse basato su tag basa la propria appartenenza su una query che specifica un elenco di tipi di risorse e tag. I tag sono chiavi che consentono di identificare e ordinare le risorse all'interno della propria organizzazione. I tag possono includere valori per le chiavi.

  > **Important**
  >
  > Non archiviate informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. Utilizziamo i tag per fornirti servizi di fatturazione e amministrazione. I tag non sono destinati ad essere utilizzati per dati privati o sensibili.

- AWS CloudFormation basato su stack

  Un gruppo di risorse AWS CloudFormation basato sullo stack basa la propria appartenenza su una query che specifica uno AWS CloudFormation stack nell'account nell'area corrente. Facoltativamente, puoi scegliere i tipi di risorse all'interno dello stack che desideri inserire nel gruppo. È possibile basare la query su un AWS CloudFormation solo stack.

Gruppi di risorse collegati ai servizi

Alcuni Servizi AWS definiscono gruppi di risorse che è possibile creare e gestire solo utilizzando la console di quel servizio e. APIs Le cose che puoi fare con questi gruppi nella console Resource Groups sono limitate. Per ulteriori informazioni, consulta Configurazioni dei servizi per i gruppi di risorse nella Guida AWS Resource Groups API di riferimento.

I gruppi di risorse possono essere nested (nidificati); un gruppo di risorse può contenere gruppi di risorse esistenti nella stessa regione.

Casi d'uso per i gruppi di risorse

Per impostazione predefinita, AWS Management Console è organizzato per AWS servizio. Ma con Resource Groups, puoi creare una console personalizzata che organizza e consolida le informazioni in base ai criteri specificati nei tag o alle risorse in uno AWS CloudFormation stack. Di seguito sono elencati alcuni dei casi in cui il raggruppamento può aiutare a organizzare le risorse.

- Un'applicazione che ha diverse fasi, ad esempio sviluppo, gestione temporanea e produzione.
- Progetti gestiti da più reparti o da singoli individui.
- Un insieme di AWS risorse che utilizzate insieme per un progetto comune o che desiderate gestire o monitorare come gruppo.
- Un set di risorse correlate alle applicazioni eseguite su una determinata piattaforma, ad esempio Android o iOS.

Ad esempio, si sta sviluppando un'applicazione Web e si mantengono set di risorse separati per le fasi alfa, beta e di release. Ogni versione viene eseguita su Amazon EC2 con un volume di storage Amazon Elastic Block Store. Utilizzi Elastic Load Balancing per gestire il traffico e Route 53 per gestire il dominio. Senza Resource Groups, potrebbe essere necessario accedere a più console solo per controllare lo stato dei servizi o modificare le impostazioni per una versione dell'applicazione.

Con Resource Groups, usi un'unica pagina per visualizzare e gestire le tue risorse. Ad esempio, supponiamo che tu utilizzi lo strumento per creare un gruppo di risorse per ogni versione (alfa, beta e release) dell'applicazione. Per verificare le risorse per la versione alfa dell'applicazione, apri il tuo gruppo di risorse. Quindi visualizza le informazioni consolidate sulla pagina del tuo gruppo di risorse. Per modificare una risorsa specifica, scegli i collegamenti della risorsa sulla pagina del tuo gruppo di risorse per accedere alla console di servizio che ha le impostazioni necessarie.

AWS Resource Groups e autorizzazioni

Le autorizzazioni per la funzionalità Resource Groups sono a livello di account. Purché IAM i responsabili, come ruoli e utenti, che condividono il tuo account dispongano delle IAM autorizzazioni corrette, possono lavorare con i gruppi di risorse che crei.

I tag sono proprietà di una risorsa, pertanto sono condivisi nell'intero account. Gli utenti di un reparto o un gruppo specializzato possono utilizzare un comune vocabolario (tag) per creare gruppi di risorse significativi per i propri ruoli e responsabilità. Avere un pool comune di tag, inoltre, significa che gli

utenti che condividono un gruppo di risorse non devono preoccuparsi di informazioni mancanti o tag in conflitto.

AWS Resource Groups risorse

In Resource Groups, l'unica risorsa disponibile è un gruppo. Ai gruppi sono associati Amazon Resource Names (ARNs) univoci. Per ulteriori informazioni suARNs, consulta Amazon Resource Names (ARN) e AWS Service Namespaces nel. Riferimenti generali di Amazon Web Services

Tipo di risorsa	ARNFormato
Resource Group	`arn:aws:resource-groups:` *`region`*`:`*`account`*`:group/`*`group-name`*

Come funziona il tagging

I tag sono coppie di chiavi e valori che fungono da metadati per l'organizzazione AWS delle risorse. Con la maggior parte AWS delle risorse, hai la possibilità di aggiungere tag quando crei la risorsa, che si tratti di un'EC2istanza Amazon, di un bucket Amazon S3 o di un'altra risorsa. Tuttavia è possibile aggiungere tag contemporaneamente a più risorse supportate utilizzando l'editor di tag. È possibile creare una query per risorse di vario tipo, quindi aggiungere, eliminare o sostituire i tag per le risorse nei risultati di ricerca. Le query assegnano un operatore `AND` ai tag in modo da restituire le risorse che corrispondono ai tipi di risorsa specificati e a tutti i tag specificati.

> **Important**
>
> Non archiviare informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. Utilizziamo i tag per fornirti servizi di fatturazione e amministrazione. I tag non sono destinati ad essere utilizzati per dati privati o sensibili.

Per ulteriori informazioni sull'etichettatura, consulta la Guida per l'utente di Tag Editor. È possibile applicare tag alle risorse supportate utilizzando il Tag Editor e alcune risorse aggiuntive mediante la funzionalità di tagging nella console del servizio in cui si crea e si gestisce la risorsa.

Guida introduttiva con AWS Resource Groups

In AWS, una risorsa è un'entità con cui puoi lavorare. Gli esempi includono un'EC2istanza Amazon, un bucket Amazon S3 o una zona ospitata Amazon Route 53. Se lavori con più risorse, potresti trovare utile gestirle in gruppo anziché passare da un AWS servizio all'altro per ogni attività.

Questa sezione mostra come iniziare AWS Resource Groups. Innanzitutto, organizza AWS le risorse taggandole in Tag Editor. Quindi crea query in Resource Groups che includono i tipi di risorse che desideri inserire in un gruppo e i tag che hai applicato alle risorse.

Dopo aver creato i gruppi di risorse in Resource Groups, utilizza AWS Systems Manager strumenti come Automation per semplificare le attività di gestione dei gruppi di risorse.

Per ulteriori informazioni su come iniziare a utilizzare AWS Systems Manager funzionalità e strumenti, consulta la Guida AWS Systems Manager per l'utente.

Argomenti

Prerequisiti per lavorare con AWS Resource Groups

Prima di iniziare a lavorare con i gruppi di risorse, assicurati di averne uno attivo AWS account con risorse esistenti e diritti appropriati per etichettare le risorse e creare gruppi.

Argomenti

Iscriviti per AWS

Se non disponi di un Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.

2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

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

Creare risorse

È possibile creare un gruppo di risorse vuoto, ma non sarà possibile eseguire alcuna attività sui membri del gruppo di risorse finché non vi saranno risorse nel gruppo. Per ulteriori informazioni sui tipi di risorsa supportati, vedi Tipi di risorse utilizzabili con AWS Resource Groups e Tag Editor.

Impostazione delle autorizzazioni

Per utilizzare appieno i gruppi di risorse e l'editor di tag, potrebbero essere necessarie ulteriori autorizzazioni per le risorse di tag o per visualizzare chiavi e valori di tag di una risorsa. Tali autorizzazioni sono suddivise nelle seguenti categorie:

- Autorizzazioni per servizi singoli, che consentono di applicare tag alle risorse da tali servizi e includerle in gruppi di risorse.
- Autorizzazioni necessarie per utilizzare la console Tag Editor
- Autorizzazioni necessarie per utilizzare il AWS Resource Groups console e. API

Se sei un amministratore, puoi fornire le autorizzazioni agli utenti creando politiche tramite AWS Identity and Access Management (IAM) servizio. Per prima cosa crei i tuoi principali, come IAM ruoli o utenti, oppure associ identità esterne ai tuoi AWS ambiente che utilizza un servizio come AWS IAM Identity Center. Quindi applichi le politiche con le autorizzazioni di cui hanno bisogno i tuoi utenti. Per informazioni sulla creazione e l'associazione delle IAM politiche, consulta Lavorare con le politiche.

Autorizzazioni per singoli servizi

> **Important**
>
> Questa sezione descrive le autorizzazioni necessarie per etichettare risorse da altre console di servizio e APIs aggiungere tali risorse ai gruppi di risorse.

Come descritto in Risorse e relativi tipi di gruppo, ciascun gruppo di risorse rappresenta una raccolta di risorse di tipi specificati che condividono uno o più valori o chiavi di tag. Per aggiungere tag a una risorsa, è necessario disporre delle autorizzazioni necessarie per il servizio a cui appartiene la risorsa. Ad esempio, per etichettare EC2 le istanze Amazon, devi disporre delle autorizzazioni per le azioni di tagging di quel servizioAPI, come quelle elencate nella Amazon EC2 User Guide.

Per sfruttare tutte le funzionalità dei gruppi di risorse, sono necessarie altre autorizzazioni che consentono di accedere alla console di un servizio e di interagire con le relative risorse. Per esempi di tali politiche per AmazonEC2, consulta la sezione Politiche di esempio per lavorare nella EC2 console Amazon nella Amazon EC2 User Guide.

Autorizzazioni richieste per Resource Groups e Tag Editor

Per utilizzare Resource Groups e Tag Editor, è necessario aggiungere le seguenti autorizzazioni all'informativa di un utente inIAM. È possibile aggiungere uno dei due AWS-politiche gestite che vengono gestite e mantenute up-to-date da AWS, oppure è possibile creare e mantenere una politica personalizzata.

Utilizzo AWS politiche gestite per le autorizzazioni Resource Groups e Tag Editor

AWS Resource Groups e Tag Editor supportano quanto segue AWS politiche gestite che è possibile utilizzare per fornire un set predefinito di autorizzazioni agli utenti. È possibile allegare queste politiche gestite a qualsiasi utente, ruolo o gruppo proprio come qualsiasi altra politica creata dall'utente.

ResourceGroupsandTagEditorReadOnlyAccess

Questa politica concede al IAM ruolo o all'utente associato l'autorizzazione a chiamare le operazioni di sola lettura sia per Resource Groups che per Tag Editor. Per leggere i tag di una risorsa, devi inoltre disporre delle autorizzazioni per quella risorsa tramite una politica separata (vedi la seguente nota importante).

ResourceGroupsandTagEditorFullAccess

Questa politica concede al IAM ruolo o all'utente allegato l'autorizzazione a chiamare qualsiasi operazione Resource Groups e le operazioni di lettura e scrittura dei tag in Tag Editor. Per leggere o scrivere i tag di una risorsa, devi inoltre disporre delle autorizzazioni per quella risorsa tramite una politica separata (vedi la seguente Nota importante).

Important

Le due politiche precedenti concedono il permesso di chiamare le operazioni Resource Groups e Tag Editor e utilizzare tali console. Per le operazioni di Resource Groups, tali policy sono sufficienti e concedono tutte le autorizzazioni necessarie per lavorare con qualsiasi risorsa nella console Resource Groups.
Tuttavia, per le operazioni di tagging e la console Tag Editor, le autorizzazioni sono più granulari. È necessario disporre delle autorizzazioni non solo per richiamare l'operazione, ma anche delle autorizzazioni appropriate per la risorsa specifica di cui si sta tentando di accedere ai tag. Per concedere l'accesso ai tag, devi anche allegare una delle seguenti politiche:

- Il AWS-managed policy ReadOnlyAccessconcede le autorizzazioni per le operazioni di sola lettura per le risorse di ogni servizio. AWS mantiene automaticamente aggiornata questa politica con le nuove AWS servizi non appena diventano disponibili.
- Molti servizi forniscono una modalità di sola lettura specifica AWS-policy gestite che è possibile utilizzare per limitare l'accesso solo alle risorse fornite da quel servizio. Ad esempio, Amazon EC2 fornisce Amazon EC2ReadOnlyAccess.
- Potresti creare una politica personalizzata che conceda l'accesso solo a operazioni di sola lettura molto specifiche per i pochi servizi e risorse a cui desideri che i tuoi utenti accedano. Questa politica utilizza una strategia di «elenco consentito» o una strategia di elenco negato.

  Una strategia di elenco consentito sfrutta il fatto che l'accesso viene negato per impostazione predefinita fino a quando non lo si consente esplicitamente in una politica. Quindi puoi usare una politica come l'esempio seguente:

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

```
            "Effect": "Allow",
            "Action": [ "resource-groups:*" ],
            "Resource": "arn:aws:resource-groups:*:123456789012:group/*"
        }
    ]
}
```

In alternativa, puoi utilizzare una strategia di «lista negata» che consente l'accesso a tutte le risorse tranne quelle che blocchi esplicitamente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
             "Action": [ "resource-groups:*" ],
            "Resource": "arn:aws:resource-groups:*:123456789012:group/*"
        }
    ]
}
```

Aggiungere manualmente le autorizzazioni Resource Groups e Tag Editor

- `resource-groups:*`(Questa autorizzazione consente tutte le azioni di Resource Groups. Se invece desideri limitare le azioni disponibili per un utente, puoi sostituire l'asterisco con un'azione specifica (Resource Groups) o con un elenco di azioni separate da virgole).
- `cloudformation:DescribeStacks`
- `cloudformation:ListStackResources`
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`
- `tag:getTagKeys`
- `tag:getTagValues`
- `resource-explorer:*`

> **Note**
>
> L'`resource-groups:SearchResources`autorizzazione consente a Tag Editor di elencare le risorse quando si filtra la ricerca utilizzando le chiavi o i valori dei tag. L'`resource-explorer:ListResources`autorizzazione consente a Tag Editor di elencare le risorse quando si cercano risorse senza definire i tag di ricerca.

Per utilizzare Resource Groups e Tag Editor nella console, è inoltre necessaria l'autorizzazione per eseguire l'`resource-groups:ListGroupResources`azione. Questa autorizzazione è necessaria per elencare i tipi di risorse disponibili nella regione corrente. L'utilizzo di condizioni politiche con non `resource-groups:ListGroupResources` è attualmente supportato.

Concessione delle autorizzazioni per l'utilizzo AWS Resource Groups e Tag Editor

Per aggiungere una politica per l'utilizzo AWS Resource Groups e Tag Editor per un utente, procedi come segue.

1. Apri la IAMconsole.
2. Nel pannello di navigazione, seleziona Utenti.
3. Trova l'utente a cui vuoi concedere AWS Resource Groups e le autorizzazioni di Tag Editor. Scegliere il nome dell'utente per aprire la pagina delle proprietà utente.
4. Scegli Aggiungi autorizzazioni.
5. Scegli Attach existing policies directly (Collega direttamente le policy esistenti).
6. Scegli Create Policy (Crea policy).
7. Nella JSONscheda, incolla la seguente dichiarazione politica.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
```

```
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:*"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Note**
>
> Questa dichiarazione politica di esempio concede le autorizzazioni solo per AWS Resource Groups e azioni Tag Editor. Non consente l'accesso a AWS Systems Manager attività in AWS Resource Groups console. Ad esempio, questa politica non concede le autorizzazioni per l'utilizzo dei comandi di Systems Manager Automation. Per eseguire attività di Systems Manager su gruppi di risorse, è necessario disporre delle autorizzazioni di Systems Manager allegate alla policy (ad esempio`ssm:*`). Per ulteriori informazioni sulla concessione dell'accesso a Systems Manager, vedere Configurazione dell'accesso a Systems Manager nella AWS Systems Manager Guida per l'utente.

8. Scegli Verifica policy.
9. Assegnare un nome e una descrizione alla nuova policy (ad esempio, `AWSResourceGroupsQueryAPIAccess`).
10. Scegli Create Policy (Crea policy).
11. Ora che la policy è stata salvata inIAM, puoi allegarla ad altri utenti. Per ulteriori informazioni su come aggiungere una politica a un utente, consulta Aggiungere autorizzazioni allegando politiche direttamente all'utente nella Guida per l'IAMutente.

Scopri di più sull' AWS Resource Groups autorizzazione e il controllo degli accessi

Resource Groups supporta quanto segue.

- Policy basate sulle operazioni. Ad esempio, è possibile creare una politica che consenta agli utenti di eseguire ListGroupsoperazioni, ma non altre.
- Autorizzazioni a livello di risorsa. Resource Groups supporta l'utilizzo ARNsper specificare singole risorse nella policy.

- Autorizzazione basata su tag. Resource Groups supporta l'utilizzo di tag di risorsa nelle condizioni di una politica. Ad esempio, puoi creare una politica che consenta agli utenti di Resource Groups l'accesso completo a un gruppo a cui hai assegnato un tag.
- Credenziali temporanee. Gli utenti possono assumere un ruolo con una politica che consente AWS Resource Groups le operazioni.

Resource Groups non supporta le politiche basate sulle risorse.

Per ulteriori informazioni sull'integrazione di Resource Groups e Tag Editor con AWS Identity and Access Management (IAM), consulta i seguenti argomenti nella Guida per l'AWS Identity and Access Management utente.

- AWS servizi che funzionano con IAM
- Azioni, risorse e chiavi di condizione per AWS Resource Groups
- Controllo dell'accesso tramite policy

AWS servizi che funzionano con AWS Resource Groups

Puoi utilizzare i seguenti AWS servizi con AWS Resource Groups.

AWS servizio	Utilizzo con Resource Groups
AWS CloudFormation— Crea gruppi di risorse AWS CloudFormation utilizzando un modello di pila.	Fornisci e organizza AWS le risorse allo stesso tempo. Organizza le risorse per tag. Organizza le risorse da un'altra pila. Raccogli informazi oni sulle tue AWS risorse in gruppi di risorse utilizzando Amazon CloudWatch o intrapren di azioni operative utilizzando AWS Systems Manager. Per ulteriori informazioni, consulta il riferimento al tipo di ResourceGroups risorsa nella Guida AWS CloudFormation per l'utente.
CloudTrail— Acquisisci tutte le azioni del gruppo di risorse utilizzando AWS CloudTrail.	Acquisisci informazioni sulle azioni eseguite sui tuoi gruppi di risorse, inclusi dettagli come chi ha eseguito l'azione (responsabile IAM,

AWS servizio	Utilizzo con Resource Groups
	ad esempio un ruolo, un utente o un Servizio AWS), quando è stata eseguita l'azione, dove si è verificata l'azione (l'indirizzo IP di origine) e altro ancora. Questi record possono quindi essere utilizzati per l'analisi o per attivare azioni di follow-up. Per ulteriori informazioni, vedere Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.
Amazon CloudWatch: abilita il monitoraggio in tempo reale delle tue AWS risorse e delle applicazioni su cui esegui AWS.	Concentra la tua visione per visualizzare metriche e allarmi provenienti da un singolo gruppo di risorse. Per ulteriori informazioni, consulta Concentrarsi su metriche e allarmi in un gruppo di risorse nella Amazon CloudWatch User Guide.
Informazioni sulle CloudWatch applicazioni Amazon: rileva i problemi più comuni con le tue applicazioni basate su .NET e SQL Server.	Monitora le risorse delle tue applicazioni.NET e SQL Server che appartengono a un gruppo di risorse. Per ulteriori informazioni, consulta Componenti applicativi supportati nella Amazon CloudWatch User Guide.
Gruppi di tabelle Amazon DynamoDB: organizza le tabelle DynamoDB in raggruppamenti logici per gestire più facilmente le risorse.	Crea, modifica ed elimina gruppi di tabelle DynamoDB dal menu Azione di DynamoDB. Per ulteriori informazioni, consulta la Amazon DynamoDB Developer Guide.

AWS servizio	Utilizzo con Resource Groups
Host dedicati Amazon EC2: utilizza le licenze software esistenti per socket, per core o per macchina virtuale, tra cui Windows Server, Microsoft SQL Server, SUSE e Linux Enterprise Server.	Avvia le istanze Amazon EC2 in gruppi di risorse host per massimizzare l'utilizzo degli host dedicati. Per ulteriori informazioni, consulta Lavorare con host dedicati nella Guida per l'utente di Amazon EC2.
Prenotazioni di capacità Amazon EC2: riserva di capacità per le tue istanze Amazon EC2 da utilizzare quando ne hai bisogno. Puoi specifica re gli attributi per la prenotazione della capacità in modo che funzioni solo con istanze Amazon EC2 avviate con attributi corrispondenti.	Avvia le tue istanze Amazon EC2 in gruppi di risorse che contengono una o più prenotazioni di capacità. Se il gruppo non dispone di una prenotazione di capacità con attributi corrispon denti e capacità disponibile per un'istanza richiesta, l'istanza viene eseguita come istanza su richiesta. Se successivamente aggiungi una prenotazione di capacità corrispondente al gruppo di destinazione, l'istanza viene automaticamente abbinata e spostata nella capacità riservata. Per ulteriori informazioni, consulta Work with Capacity Reservation groups nella Amazon EC2 User Guide.
AWS License Manager— Semplifica il processo di trasferimento delle licenze dei fornitori di software sul cloud.	Configura un gruppo di risorse host per consentire al License Manager di gestire i tuoi host dedicati. Per ulteriori informazioni, consulta Host Resource Groups in License Manager nella License Manager User Guide.

AWS servizio	Utilizzo con Resource Groups
AWS Resilience Hub: prepara e proteggi le tue applicazioni dalle interruzioni.	Scopri le tue applicazioni definite utilizzando Resource Groups. Per ulteriori informazioni, consulta Misura e migliora la resilienza delle applicazioni con AWS Resilience Hub nel AWS News Blog.
AWS Resource Access Manager— Condividi AWS risorse specifiche di tua proprietà con altri account.	Condividi i gruppi di risorse dell'host utilizzando AWS RAM. Per ulteriori informazioni, consulta Risorse condivisibili nella Guida per l'AWS RAM utente.
AWS Service Catalog AppRegistry— Definisci e gestisci le tue applicazioni e i relativi metadati.	Quando si crea un'applicazione in AppRegistry, tale servizio crea automaticamente un gruppo di risorse per quell'applicazione. Il gruppo di risorse dell'applicazione è una raccolta di tutte le risorse dell'applicazione. Il servizio crea anche un gruppo di risorse AWS CloudFormation basato sullo stack per ogni stack associato all'applicazione. Per ulteriori informazioni, consulta Using AppRegistry in the AWS Service Catalog Administrator Guide.

AWS servizio	Utilizzo con Resource Groups
AWS Systems Manager— Abilita la visibilità e il controllo delle tue AWS risorse.	Raccogli informazioni operative e intraprendi azioni collettive sulle tue applicazioni basate su gruppi di risorse. Nella AWS Systems Manager console, la pagina Applicazioni personalizzate di Application Manager importa e visualizza automaticamente i dati operativi per le applicazioni basate su gruppi di risorse. È possibile utilizzare le informazioni in Application Manager per determinare quali risorse di un'applicazione sono conformi e funzionano correttamente e quali risorse richiedono un intervento. Per ulteriori informazioni, vedere Utilizzo delle applicazioni in Application Manager nella Guida per l'AWS Systems Manager utente.
Amazon VPC Network Access Analyzer: identifica gli accessi di rete indesiderati alle tue risorse su. AWS	Puoi specificare le fonti e le destinazioni per i tuoi requisiti di accesso alla rete utilizzando. AWS Resource Groups Ciò consente di gestire l'accesso alla rete in tutto AWS l'ambiente, indipendentemente dalla configurazione della rete. Per ulteriori informazioni, consulta Use Resource Groups with Network Access Scopes nella Amazon Virtual Private Cloud User Guide.

Configurazioni di servizio per gruppi di risorse

I gruppi di risorse consentono di gestire le raccolte di AWS risorse come unità. Alcuni AWS servizi supportano questa funzionalità eseguendo le operazioni richieste su tutti i membri del gruppo. Tali servizi possono memorizzare le impostazioni da applicare ai membri del gruppo sotto forma di una struttura di JSONdati allegata al gruppo.

Questo argomento descrive le impostazioni di configurazione disponibili per AWS i servizi supportati.

Argomenti

Come accedere alla configurazione del servizio associata a un gruppo di risorse

I servizi che supportano i gruppi collegati ai servizi in genere impostano la configurazione automaticamente quando si utilizzano gli strumenti forniti da tale servizio, ad esempio la console di gestione del servizio o AWS CLI le AWS SDK relative operazioni. Alcuni servizi gestiscono completamente i propri gruppi collegati ai servizi e non è possibile modificarli in alcun modo, ad eccezione di quanto consentito dalla console o dai comandi forniti dal servizio proprietario. AWS Tuttavia, in alcuni casi, è possibile interagire con la configurazione del servizio utilizzando API le seguenti operazioni nel AWS SDKs o i loro equivalenti: AWS CLI

- È possibile allegare la propria configurazione a un gruppo quando si crea il gruppo utilizzando l'CreateGroupoperazione.
- È possibile modificare la configurazione corrente associata a un gruppo utilizzando l'PutGroupConfigurationoperazione.
- È possibile visualizzare la configurazione corrente di un gruppo di risorse chiamando l'GetGroupConfigurationoperazione.

JSONsintassi di una configurazione di servizio

Un gruppo di risorse può contenere una configurazione che definisce le impostazioni specifiche del servizio che si applicano alle risorse che fanno parte di quel gruppo.

Una configurazione è espressa come oggetto. JSON Al livello più alto, una configurazione è un array di elementi di configurazione di gruppo. Ogni elemento di configurazione di gruppo contiene due elementi: uno `Type` per la configurazione e un insieme `Parameters` definito da quel tipo. Ogni parametro contiene una `Name` matrice di uno o più`Values`. L'esempio seguente con *`placeholders`* mostra la sintassi di base per una configurazione per un singolo tipo di risorsa di esempio. Questo esempio mostra un tipo con due parametri e ogni parametro con due valori. I tipi, i parametri e i valori effettivamente validi vengono descritti nella sezione successiva.

```
[
    {
        "Type": "configuration-type",
        "Parameters": [
            {
                "Name": "parameter1-name",
                "Values": [
                    "value1",
                    "value2"
                ]
            },
            {
                "Name": "parameter2-name",
                "Values": [
                    "value3",
                    "value4"
                ]
            }
        ]
    }
]
```

Tipi e parametri di configurazione supportati

Resource Groups supporta l'utilizzo dei seguenti tipi di configurazione. Ogni tipo di configurazione dispone di un set di parametri validi per quel tipo.

Argomenti

- AWS::ResourceGroups::Generic
- AWS::AppRegistry::Application
- AWS::CloudFormation::Stack
- AWS::EC2::CapacityReservationPool
- AWS::EC2::HostManagement
- AWS::NetworkFirewall::RuleGroup

`AWS::ResourceGroups::Generic`

Questo tipo di configurazione specifica le impostazioni che impongono i requisiti di appartenenza al gruppo di risorse, anziché configurare il comportamento di un tipo di risorsa specifico per un

servizio. AWS Questo tipo di configurazione viene aggiunto automaticamente dai gruppi collegati ai servizi che lo richiedono, ad esempio i tipi and. `AWS::EC2::CapacityReservationPool` `AWS::EC2::HostManagment`

Quanto segue `Parameters` è valido per il gruppo collegato al `AWS::ResourceGroups::Generic` servizio. `Type`

- **`allowed-resource-types`**

  Questo parametro specifica che il gruppo di risorse può essere costituito solo da risorse del tipo o dei tipi specificati.

  Tipo di dati dei valori: String

  Valori consentiti:

  - `AWS::EC2::Host`— Un `Configuration` con questo parametro e valore è obbligatorio quando la configurazione del servizio contiene anche un `Configuration` di tipo`AWS::EC2::HostManagement`. Ciò garantisce che il `HostManagement` gruppo possa contenere solo host EC2 dedicati Amazon.
  - `AWS::EC2::CapacityReservation`— Un `Configuration` con questo parametro e valore è obbligatorio quando la configurazione del servizio contiene anche un `Configuration` elemento di tipo`AWS::EC2::CapacityReservationPool`. Ciò garantisce che un `CapacityReservation` gruppo possa contenere solo la capacità di prenotazione EC2 della capacità di Amazon.

  Obbligatorio: condizionale, basato su altri `Configuration` elementi collegati al gruppo di risorse. Vedi la voce precedente per Valori consentiti.

  L'esempio seguente limita i membri del gruppo alle sole istanze EC2 host Amazon.

```
[
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": ["AWS::EC2::Host"]
            }
        ]
    }
```

```
]
```

- **`deletion-protection`**

  Questo parametro specifica che il gruppo di risorse non può essere eliminato a meno che non contenga membri. Per ulteriori informazioni, vedere Eliminare un gruppo di risorse host nella Guida per l'utente di License Manager

  Tipo di dati di valori: matrice di stringhe

  Valori consentiti: l'unico valore consentito è `[ "UNLESS_EMPTY" ]` (il valore deve essere in lettere maiuscole).

  Obbligatorio: condizionale, basato su altri `Configuration` elementi collegati al gruppo di risorse. Questo parametro è obbligatorio solo quando il gruppo di risorse ha anche un altro `Configuration` elemento con `Type` of`AWS::EC2::HostManagement`.

  L'esempio seguente abilita la protezione da eliminazione per il gruppo a meno che il gruppo non abbia membri.

```
[
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "deletion-protection",
                "Values": [ "UNLESS_EMPTY" ]
            }
        ]
    }
]
```

`AWS::AppRegistry::Application`

Questo `Configuration` tipo specifica che il gruppo di risorse rappresenta un'applicazione creata da AWS Service Catalog AppRegistry.

I gruppi di risorse di questo tipo sono completamente gestiti dal AppRegistry servizio e non possono essere creati, aggiornati o eliminati da utenti diversi dall'utilizzo degli strumenti forniti da AppRegistry.

> **Note**
>
> Poiché i gruppi di risorse di questo tipo vengono creati e gestiti automaticamente dall'utente AWS e non sono gestiti dall'utente, tali gruppi di risorse non vengono conteggiati ai fini del limite di quota per il numero massimo di gruppi di risorse che è possibile creare nel proprio Account AWS.

Per ulteriori informazioni, vedere Using AppRegistry in the Service Catalog User Guide.

Quando AppRegistry crea un gruppo di risorse collegato ai servizi di questo tipo, crea automaticamente anche un gruppo separato e aggiuntivo AWS CloudFormation collegato ai servizi per ogni AWS CloudFormation stack associato all'applicazione.

AppRegistry nomina automaticamente i gruppi collegati ai servizi di questo tipo che crea con il prefisso seguito dal nome dell'applicazione`AWS_AppRegistry_Application-`: `AWS_AppRegistry_Application-`*`MyAppName`*

I seguenti parametri sono supportati per il tipo di gruppo collegato al `AWS::AppRegistry::Application` servizio.

- **`Name`**

  Questo parametro specifica il nome descrittivo dell'applicazione assegnato dall'utente al momento della creazione in. AppRegistry

  Tipo di dati dei valori: String

  Valori consentiti: qualsiasi stringa di testo consentita dal AppRegistry servizio per il nome di un'applicazione.

  Campo obbligatorio: sì

- **`Arn`**

  Questo parametro specifica il percorso Amazon Resource Name (ARN) dell'applicazione assegnata da AppRegistry.

  Tipo di dati di valori: String

Valori consentiti: un valore validoARN.

Campo obbligatorio: sì

> **Note**
>
> Per modificare uno qualsiasi di questi elementi, è necessario modificare l'applicazione utilizzando la AppRegistry console o le AWS CLI operazioni AWS SDK e i servizi in questione.

Questo gruppo di risorse applicative include automaticamente come membri del gruppo i gruppi di risorse creati per gli AWS CloudFormation stack associati all' AppRegistry applicazione. È possibile utilizzare l'ListGroupResourcesoperazione per visualizzare tali gruppi di bambini.

L'esempio seguente mostra l'aspetto della sezione di configurazione di un gruppo `AWS::AppRegistry::Application` collegato a un servizio.

```
[
    {
        "Type": "AWS::AppRegistry::Application",
        "Parameters":[
            {
                "Name": "Name",
                "Values": [
                    "MyApplication"
                ]
            },
            {
                "Name": "Arn",
                "Values": [
                    "arn:aws:servicecatalog:us-east-1:123456789012:/
applications/<application-id>"
                ]
            }
        ]
    }
]
```

`AWS::CloudFormation::Stack`

Questo `Configuration` tipo specifica che il gruppo rappresenta uno AWS CloudFormation stack e i suoi membri sono le AWS risorse create da quello stack.

I gruppi di risorse di questo tipo vengono creati automaticamente quando associ uno AWS CloudFormation stack al servizio. AppRegistry Non è possibile creare, aggiornare o eliminare questi gruppi se non utilizzando gli strumenti forniti da AppRegistry.

AppRegistry nomina automaticamente i gruppi collegati ai servizi di questo tipo che crea con il prefisso `AWS_CloudFormation_Stack-` seguito dal nome dello stack: `AWS_CloudFormation_Stack-`*`MyStackName`*

> **Note**
>
> Poiché i gruppi di risorse di questo tipo vengono creati e gestiti automaticamente dall'utente AWS e non sono gestiti dall'utente, questi gruppi di risorse non vengono conteggiati ai fini del limite di quota per il numero massimo di gruppi di risorse che è possibile creare nel proprio. Account AWS

Per ulteriori informazioni, vedere Using AppRegistry in the Service Catalog User Guide.

AppRegistry crea automaticamente un gruppo di risorse collegato ai servizi di questo tipo per ogni AWS CloudFormation stack associato all'applicazione. AppRegistry Questi gruppi di risorse diventano membri secondari del gruppo di risorse principale dell'applicazione. AppRegistry

I membri di questo gruppo di AWS CloudFormation risorse sono le AWS risorse create come parte dello stack.

I seguenti parametri sono supportati per il tipo di gruppo `AWS::CloudFormation::Stack` collegato al servizio.

- **`Name`**

  Questo parametro specifica il nome descrittivo dello AWS CloudFormation stack assegnato dall'utente al momento della creazione dello stack.

  Tipo di dati di valori: String

Valori consentiti: qualsiasi stringa di testo consentita dal AWS CloudFormation servizio per un nome di pila.

Campo obbligatorio: sì

- **`Arn`**

  Questo parametro specifica il percorso Amazon Resource Name (ARN) dello AWS CloudFormation stack collegato all'applicazione in. AppRegistry

  Tipo di dati di valori: String

  Valori consentiti: un valore validoARN.

  Campo obbligatorio: sì

> **Note**
>
> Per modificare uno qualsiasi di questi elementi, è necessario modificare l'applicazione utilizzando la AppRegistry console o l'equivalente AWS SDK e AWS CLI le operazioni.

L'esempio seguente mostra l'aspetto della sezione di configurazione di un gruppo `AWS::CloudFormation::Stack` collegato a un servizio.

```
[
    {
        "Type": "AWS::CloudFormation::Stack",
        "Parameters":[
            {
                "Name": "Name",
                "Values": [
                    "MyStack"
                ]
            },
            {
                "Name": "Arn",
                "Values": [
                    "arn:aws:cloudformation:us-
east-1:123456789012:stack/MyStack/<stack-id>"
```

```
                ]
            }
        ]
    }
]
```

AWS::EC2::CapacityReservationPool

Questo `Configuration` tipo specifica che il gruppo di risorse rappresenta un pool comune di capacità fornito dai membri del gruppo. I membri di questo gruppo di risorse devono essere titolari di prenotazioni EC2 di capacità Amazon. Un gruppo di risorse può includere sia prenotazioni di capacità che possiedi nel tuo account sia prenotazioni di capacità condivise con te da altri account utilizzando AWS Resource Access Manager. Ciò consente di avviare un'EC2istanza Amazon utilizzando questo gruppo di risorse come valore per il parametro di prenotazione della capacità. Quando esegui questa operazione, l'istanza utilizza la capacità riservata disponibile nel gruppo. Se il gruppo di risorse non ha capacità disponibile, l'istanza viene avviata come istanza on-demand autonoma all'esterno del pool. Per ulteriori informazioni, consulta Working with Capacity Reservation groups nella Amazon EC2 User Guide.

Se configuri un gruppo di risorse collegato al servizio con un `Configuration` elemento di questo tipo, devi specificare anche `Configuration` elementi separati con i seguenti valori:

- Un `AWS::ResourceGroups::Generic` tipo con un solo parametro:
  - Il parametro `allowed-resource-types` e un valore singolo di`AWS::EC2::CapacityReservation`. Ciò garantisce che solo le prenotazioni EC2 di capacità di Amazon possano far parte del gruppo di risorse.

L'`AWS::EC2::CapacityReservationPool`elemento in una configurazione di gruppo non supporta alcun parametro.

L'esempio seguente mostra l'aspetto della `Configuration` sezione di tale gruppo.

```
[
    {
        "Type": "AWS::EC2::CapacityReservationPool"
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
```

```
                "Name": "allowed-resource-types",
                "Values": [ "AWS::EC2::CapacityReservation" ]
            }
        ]
    }
]
```

AWS::EC2::HostManagement

Questo identificatore specifica le impostazioni per la gestione degli EC2 host di Amazon e AWS License Manager che vengono applicate ai membri del gruppo. Per ulteriori informazioni, consulta Host resource groups in. AWS License Manager

Se configuri un gruppo di risorse collegato al servizio con un `Configuration` elemento di questo tipo, devi anche specificare `Configuration` elementi separati con i seguenti valori:

- Un `AWS::ResourceGroups::Generic` tipo, con un parametro `allowed-resource-types` e un valore singolo di. `AWS::EC2::Host` Ciò garantisce che solo gli host EC2 dedicati di Amazon possano essere membri del gruppo.
- Un `AWS::ResourceGroups::Generic` tipo, con un parametro `deletion-protection` e un valore singolo di`UNLESS_EMPTY`. Ciò garantisce che il gruppo non possa essere eliminato a meno che non sia vuoto.

I seguenti parametri sono supportati per il tipo di gruppo `AWS::EC2::HostManagement` collegato al servizio.

- **`auto-allocate-host`**

  Questo parametro specifica se le istanze vengono avviate su un host dedicato specifico o su qualsiasi host disponibile con una configurazione corrispondente. Per ulteriori informazioni, consulta Comprendere il posizionamento automatico e l'affinità nella Amazon EC2 User Guide.

  Tipo di dati di valori: booleano

  Valori consentiti: «true» o «false» (devono essere minuscoli).

  Required: No

```
[
    {
```

```
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "auto-allocate-host",
                "Values": [ "true" ]
            },
            {
                "Name": "any-host-based-license-configuration",
                "Values": ["true"]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": [ "AWS::EC2::Host" ]
            },
            {
                "Name": "deletion-protection",
                "Values": [ "UNLESS_EMPTY" ]
            }
        ]
    }
]
```

- **`auto-release-host`**

  Questo parametro specifica se un host dedicato del gruppo viene rilasciato automaticamente dopo la chiusura dell'ultima istanza in esecuzione. Per ulteriori informazioni, consulta Releasing Dedicated Hosts nella Amazon EC2 User Guide.

  Tipo di valori di dati: booleano

  Valori consentiti: «true» o «false» (devono essere minuscoli).

  Required: No

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
```

```
            {
                "Name": "auto-release-host",
                "Values": [ "false" ]
            },
            {
                "Name": "any-host-based-license-configuration",
                "Values": ["true"]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": [ "AWS::EC2::Host" ]
            },
            {
                "Name": "deletion-protection",
                "Values": [ "UNLESS_EMPTY" ]
            }
        ]
    }
]
```

- **`allowed-host-families`**

  Questo parametro specifica quali famiglie di tipi di istanze possono essere utilizzate dalle istanze che sono membri di questo gruppo.

  Tipo di dati di valori: una matrice di stringhe.

  Valori consentiti: ognuno deve essere un identificatore di famiglia di tipi di EC2 istanze Amazon valido, ad esempio`C4`, `M5P3dn`, o`R5d`.

  Required: No

  L'elemento di configurazione di esempio seguente specifica che le istanze avviate possono essere solo membri delle famiglie di tipi di istanze C5 o M5.

```
[
    {
        "Type": "AWS::EC2::HostManagement",
```

```
        "Parameters": [
            {
                "Name": "allowed-host-families",
                "Values": ["c5", "m5"]
            },
            {
                "Name": "any-host-based-license-configuration",
                "Values": ["true"]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": ["AWS::EC2::Host"]
            },
            {
                "Name": "deletion-protection",
                "Values": ["UNLESS_EMPTY"]
            }
        ]
    }
]
```

- **`allowed-host-based-license-configurations`**

  Questo parametro specifica i percorsi Amazon Resource Name (ARN) di una o più configurazioni di licenza basate su core/socket che desideri applicare ai membri del gruppo.

  Tipo di dati di valori: una matrice di. ARNs

  Valori consentiti: ognuno deve essere una configurazione di License Manager validaARN.

  Obbligatorio: condizionale. È necessario specificare questo parametro o`any-host-based-license-configuration`, ma non entrambi. Si escludono a vicenda.

  L'elemento di configurazione di esempio seguente specifica che i membri del gruppo possono utilizzare le due configurazioni di License Manager specificate.

```
[
    {
```

```
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "allowed-host-based-license-configurations",
                "Values": [
                    "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-6eb6586f508a786a2ba41EXAMPLE1111",
                    "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-8a786a26f50ba416eb658EXAMPLE2222"
                ]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": [ "AWS::EC2::Host" ]
            },
            {
                "Name": "deletion-protection",
                "Values": [ "UNLESS_EMPTY" ]
            }
        ]
    }
]
```

- **`any-host-based-license-configuration`**

  Questo parametro specifica che non si desidera associare una configurazione di licenza specifica al gruppo. In questo caso, tutte le configurazioni di licenza basate su core/socket sono disponibili per i membri del gruppo di risorse host. Utilizzate questa impostazione se disponete di un numero illimitato di licenze e desiderate ottimizzarle per l'utilizzo dell'host.

  Tipo di valori di dati: booleano

  Valori consentiti: «true» o «false» (devono essere minuscoli).

  Obbligatorio: condizionale. È necessario specificare questo parametro o`allowed-host-based-license-configurations`, ma non entrambi. Si escludono a vicenda.

L'elemento di configurazione di esempio seguente specifica che i membri del gruppo possono utilizzare qualsiasi configurazione di licenza basata su core/socket.

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "any-host-based-license-configuration",
                "Values": ["true"]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": ["AWS::EC2::Host"]
            },
            {
                "Name": "deletion-protection",
                "Values": ["UNLESS_EMPTY"]
            }
        ]
    }
]
```

L'esempio seguente illustra come includere tutte le impostazioni di gestione dell'host in un'unica configurazione.

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "auto-allocate-host",
                "Values": ["true"]
            },
            {
                "Name": "auto-release-host",
```

```
                "Values": ["false"]
            },
            {
                "Name": "allowed-host-families",
                "Values": ["c5", "m5"]
            },
            {
                "Name": "allowed-host-based-license-configurations",
                "Values": [
                    "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-6eb6586f508a786a2ba41EXAMPLE1111",
                    "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-8a786a26f50ba416eb658EXAMPLE2222"
                ]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": ["AWS::EC2::Host"]
            },
            {
                "Name": "deletion-protection",
                "Values": ["UNLESS_EMPTY"]
            }
        ]
    }
]
```

AWS::NetworkFirewall::RuleGroup

Questo identificatore specifica le impostazioni per i gruppi di AWS Network Firewall regole che vengono applicate ai membri del gruppo. Gli amministratori ARN del firewall possono specificare l'appartenenza a un gruppo di risorse di questo tipo per risolvere automaticamente gli indirizzi IP dei membri del gruppo per una regola firewall anziché dover elencare ogni indirizzo manualmente. Per ulteriori informazioni, vedere Utilizzo di gruppi di risorse basati su tag in. AWS Network Firewall

È possibile creare gruppi di risorse di questo tipo di configurazione utilizzando la console Network Firewall o eseguendo un AWS CLI comando o un' AWS SDKoperazione.

I gruppi di risorse di questo tipo di configurazione presentano le seguenti restrizioni:

- I membri del gruppo sono costituiti solo da risorse dei tipi supportati da Network Firewall.
- Il gruppo deve contenere una query basata su tag per gestire l'appartenenza al gruppo; tutte le risorse dei tipi supportati con tag che corrispondono alla query sono automaticamente membri del gruppo.
- Non sono `Parameters` supportate per questo tipo di configurazione.
- Per eliminare un gruppo di risorse di questo tipo di configurazione, nessun gruppo di regole Network Firewall può farvi riferimento.

L'esempio seguente illustra le `ResourceQuery` sezioni `Configuration` e per un gruppo di questo tipo.

```
{
    "Configuration": [
        {
            "Type": "AWS::NetworkFirewall::RuleGroup",
            "Parameters": []
        }
    ],
    "ResourceQuery": {
        "Query": "{\"ResourceTypeFilters\":[\"AWS::EC2::Instance\"],\"TagFilters\":
[{\"Key\":\"environment\",\"Values\":[\"production\"]}]}",
        "Type": "TAG_FILTERS_1_0"
    }
}
```

Il AWS CLI comando di esempio seguente crea un gruppo di risorse con la configurazione e la query precedenti.

```
$ aws resource-groups create-group \
    --name test-group \
    --resource-query '{"Type": "TAG_FILTERS_1_0", "Query": "{\"ResourceTypeFilters\":
 [\"AWS::EC2::Instance\"], \"TagFilters\": [{\"Key\": \"environment\", \"Values\":
 [\"production\"]}]}"}' \
    --configuration '[{"Type": "AWS::NetworkFirewall::RuleGroup", "Parameters": []}]'
{
    "Group":{
        "GroupArn":"arn:aws:resource-groups:us-west-2:123456789012:group/test-group",
        "Name":"test-group",
```

```
        "OwnerId":"123456789012"
    },
    "Configuration": [
        {
            "Type": "AWS::NetworkFirewall::RuleGroup",
            "Parameters": []
        }
    ],
    "ResourceQuery": {
        "Query": "{\"ResourceTypeFilters\":[\"AWS::EC2::Instance\"],\"TagFilters\":
[{\"Key\":\"environment\",\"Values\":[\"production\"]}]}",
        "Type": "TAG_FILTERS_1_0"
    }
}
```

Creazione di gruppi basati su query in AWS Resource Groups

Tipi di interrogazioni relative ai gruppi di risorse

In AWS Resource Groups, una query è la base di un gruppo basato su query. È possibile basare un gruppo di risorse su uno dei due tipi di query.

Tag-based (Basato su tag)

Le interrogazioni basate su tag includono elenchi di tipi di risorse specificati nel formato `AWS::service::resource` seguente e tag. I Tags (tag) sono chiavi che consentono di identificare e ordinare le risorse all'interno della propria organizzazione. I tag possono includere valori per le chiavi.

Per una query basata su tag, è anche possibile specificare i tag condivisi dalle risorse che si desidera siano membri del gruppo. Ad esempio, se desideri creare un gruppo di risorse che contenga tutte le EC2 istanze Amazon e i bucket Amazon S3 che utilizzi per eseguire la fase di test di un'applicazione e disponi di istanze e bucket etichettati in questo modo, scegli `AWS::EC2::Instance` i tipi di risorse `AWS::S3::Bucket` e dall'elenco a discesa, quindi specifica la chiave del tag, con un valore di tag **`Stage`** di. **`Test`**

La sintassi del `ResourceQuery` parametro di un gruppo di risorse basato su tag contiene i seguenti elementi:

- `Type`

  Questo elemento indica il tipo di interrogazione che definisce questo gruppo di risorse. Per creare un gruppo di risorse basato su tag, specificate il valore `TAG_FILTERS_1_0` nel modo seguente:

  ```
  "Type": "TAG_FILTERS_1_0"
  ```

- `Query`

  Questo elemento definisce l'interrogazione effettiva utilizzata per il confronto con le risorse. Contiene una rappresentazione in formato stringa di una JSON struttura con i seguenti elementi:

- `ResourceTypeFilters`

  Questo elemento limita i risultati solo ai tipi di risorse che corrispondono al filtro. Puoi specificare le seguenti valori:

  - `"AWS::AllSupported"`— specificare che i risultati possono includere risorse di qualsiasi tipo che corrispondono alla query e che sono attualmente supportate dal servizio Resource Groups.
  - `"AWS::`*`service-id`*`::`*`resource-type`*— un elenco separato da virgole di stringhe di specifiche del tipo di risorsa con questo formato:, ad esempio. `"AWS::EC2::Instance"`

- `TagFilters`

  Questo elemento specifica le coppie di stringhe chiave/valore che vengono confrontate con i tag allegati alle risorse. Nel gruppo sono incluse quelle con una chiave di tag e un valore che corrispondono al filtro. Ogni filtro è composto dai seguenti elementi:

  - `"Key"`— una stringa con un nome chiave. Solo le risorse con tag con un nome chiave corrispondente corrispondono al filtro e sono membri del gruppo.
  - `"Values"`— una stringa con un elenco di valori separati da virgole per la chiave specificata. Solo le risorse con una chiave di tag corrispondente e un valore che corrisponde a uno in questo elenco sono membri del gruppo.

Tutti questi JSON elementi devono essere combinati in una rappresentazione di stringa a riga singola della JSON struttura. Ad esempio, si consideri una struttura `Query` con la seguente JSON struttura di esempio. Questa query è pensata per abbinare solo EC2 le istanze Amazon che hanno un tag «Stage» con un valore «Test».

```
{
    "ResourceTypeFilters": [ "AWS::EC2::Instance" ],
    "TagFilters": [
        {
            "Key": "Stage",
            "Values": [ "Test" ]
        }
    ]
}
```

JSONPuò essere rappresentata come la seguente stringa a riga singola e utilizzata come valore dell'`Query`elemento. Poiché il valore di una JSON struttura deve essere una stringa tra virgolette

doppie, è necessario evitare le virgolette o i caratteri barra incorporati facendo precedere ciascuno di essi da una barra rovesciata, come illustrato di seguito:

```
"Query":"{\"ResourceTypeFilters\":[\"AWS::AllSupported\"],\"TagFilters\":[{\"Key\":
\"Stage\",\"Values\":[\"Test\"]}]}"
```

La `ResourceQuery` stringa completa viene quindi rappresentata come illustrato di seguito, come parametro di comando: CLI

```
--resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters\":
[\"AWS::AllSupported\"],\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":[\"Test
\"]}]}"}'
```

AWS CloudFormation basato su stack

In una query AWS CloudFormation basata sullo stack, scegli uno AWS CloudFormation stack nel tuo account nell'area corrente, quindi scegli i tipi di risorse nello stack che desideri inserire nel gruppo. È possibile basare la query su un solo stack. AWS CloudFormation

> **Note**
>
> Uno AWS CloudFormation stack può contenere altri stack AWS CloudFormation «secondari». Tuttavia, un gruppo di risorse basato su uno stack «principale» non ottiene tutte le risorse degli stack secondari come membri del gruppo. I gruppi di risorse aggiungono gli stack secondari al gruppo di risorse dello stack principale come membri singoli del gruppo e non li espandono.

Resource Groups supporta le query basate su AWS CloudFormation stack con uno dei seguenti stati.

- `CREATE_COMPLETE`
- `CREATE_IN_PROGRESS`
- `DELETE_FAILED`
- `DELETE_IN_PROGRESS`
- `REVIEW_IN_PROGRESS`

> **Important**
>
> Solo le risorse create direttamente come parte dello stack della query sono incluse nel gruppo di risorse. Le risorse create successivamente dai membri dello AWS CloudFormation stack non diventano membri del gruppo. Ad esempio, se un gruppo con scalabilità automatica viene creato AWS CloudFormation da come parte dello stack, quel gruppo con scalabilità automatica è un membro del gruppo. Tuttavia, un'EC2istanza Amazon creata da quel gruppo di auto-scaling come parte del suo funzionamento non fa parte del gruppo di risorse basato sullo stack AWS CloudFormation .

Se crei un gruppo basato su uno AWS CloudFormation stack e lo stato dello stack cambia in uno che non è più supportato come base per una query di gruppo, ad esempio, il gruppo di risorse esiste ancora`DELETE_COMPLETE`, ma non ha risorse membri.

Dopo aver creato un gruppo di risorse, è possibile eseguire attività sulle risorse del gruppo.

La sintassi del `ResourceQuery` parametro di un gruppo di risorse CloudFormation basato sullo stack contiene i seguenti elementi:

- `Type`

  Questo elemento indica il tipo di interrogazione che definisce questo gruppo di risorse.

  Per creare un gruppo di risorse AWS CloudFormation basato sullo stack, specificate il valore nel modo `CLOUDFORMATION_STACK_1_0` seguente:

  ```
  "Type": "CLOUDFORMATION_STACK_1_0"
  ```

- `Query`

  Questo elemento definisce l'interrogazione effettiva utilizzata per il confronto con le risorse. Contiene una rappresentazione in formato stringa di una JSON struttura con i seguenti elementi:

  - `ResourceTypeFilters`

    Questo elemento limita i risultati solo ai tipi di risorse che corrispondono al filtro. Puoi specificare le seguenti valori:

  - `"AWS::AllSupported"`— per specificare che i risultati possono includere risorse di qualsiasi tipo che corrispondono alla query.
  - `"AWS::`*`service-id`*`::`*`resource-type`*— un elenco separato da virgole di stringhe di specificazione del tipo di risorsa con questo formato:, ad esempio. `"AWS::EC2::Instance"`
- `StackIdentifier`

  Questo elemento specifica l'Amazon Resource Name (ARN) dello AWS CloudFormation stack di cui desideri includere le risorse nel gruppo.

Tutti questi JSON elementi devono essere combinati in una rappresentazione di stringa a riga singola della struttura. JSON Ad esempio, si consideri una struttura `Query` con la seguente JSON struttura di esempio. Questa query è pensata per corrispondere solo ai bucket Amazon S3 che fanno parte dello stack specificato. AWS CloudFormation

```
{
    "ResourceTypeFilters": [ "AWS::S3::Bucket" ],
    "StackIdentifier": "arn:aws:cloudformation:us-
west-2:123456789012:stack/MyCloudFormationStackName/fb0d5000-aba8-00e8-
aa9e-50d5cEXAMPLE"
}
```

Questa JSON può essere rappresentata come la seguente stringa a riga singola e utilizzata come valore dell'elemento. `Query` Poiché il valore di una JSON struttura deve essere una stringa tra virgolette doppie, è necessario evitare le virgolette o i caratteri barra incorporati facendo precedere ciascuno di essi da una barra rovesciata, come illustrato di seguito:

```
"Query":"{\"ResourceTypeFilters\":[\"AWS::S3::Bucket\"],\"StackIdentifier\":
\"arn:aws:cloudformation:us-west-2:123456789012:stack\/MyCloudFormationStackName\/
fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\"
```

La `ResourceQuery` stringa completa viene quindi rappresentata come illustrato di seguito, come parametro di comando: CLI

```
--resource-query '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::S3::Bucket\"],\"StackIdentifier\":\"arn:aws:cloudformation:us-
west-2:123456789012:stack\/MyCloudFormationStackName\/fb0d5000-aba8-00e8-
aa9e-50d5cEXAMPLE\"}'
```

Crea una query basata su tag e crea un gruppo

Le procedure seguenti mostrano come creare una query basata su tag e utilizzarla per creare un gruppo di risorse.

Console

1. Accedere alla console AWS Resource Groups.
2. Nel riquadro di navigazione, scegli Crea gruppo di risorse.
3. Nella pagina Crea gruppo basato su query, in Tipo di gruppo, scegli il tipo di gruppo basato su tag.
4. In Criteri di raggruppamento, scegli i tipi di risorse che desideri includere nel tuo gruppo di risorse. È possibile avere un massimo di 20 tipi di risorse in una query. Per questa procedura dettagliata, scegli AWS::: :Instance eAWS: EC2 :S3: :Bucket.
5. Sempre in Criteri di raggruppamento, per i tag, specifica una chiave di tag o una coppia chiave-valore di tag, per limitare le risorse corrispondenti in modo da includere solo quelle contrassegnate con i valori specificati. Scegliere Add (Aggiungi) o premere Invio al completamento del tag. In questo esempio, vengono filtrate le risorse con la chiave di tag di Stage (Fase). Il valore di tag è opzionale, ma restringe ulteriormente i risultati della query. È possibile aggiungere più valori per una chiave di tag aggiungendo un `OR` operatore tra i valori dei tag. Per aggiungere ulteriori tag, scegliere Add (Aggiungi). Le query assegnano un operatore `AND` ai tag in modo da restituire le risorse che corrispondono ai tipi di risorsa specificati e a tutti i tag specificati.
6. Sempre in Criteri di raggruppamento, scegli Anteprima delle risorse del gruppo per visualizzare l'elenco delle EC2 istanze e dei bucket S3 presenti nell'account che corrispondono alla chiave o alle chiavi di tag specificate.
7. Dopo aver ottenuto i risultati desiderati, crea un gruppo basato su questa query.

    a. In Dettagli del gruppo, in Nome del gruppo, digita un nome per il tuo gruppo di risorse.

    Il nome di un gruppo di risorse può avere un massimo di 128 caratteri, inclusi lettere, numeri, trattini, punti e trattini bassi. Il nome non può iniziare per `AWS` o `aws`, poiché sono riservati. Il nome di un gruppo di risorse deve essere univoco nella regione corrente del tuo account.

    b. (Facoltativo) In Group description (Descrizione gruppo), immettere una descrizione del tuo gruppo.

c. (Facoltativo) Nell'area Group tags (Tag gruppo), aggiungere una chiave di tag e coppie di valore che si applicano solo al gruppo di risorse, non alle risorse membri del gruppo.

   I tag del gruppo sono utili se si prevede di rendere questo gruppo un membro di un gruppo più grande. Poiché è necessario specificare almeno una chiave di tag per creare un gruppo, assicurarsi di aggiungere almeno una chiave di tag in Group tags (Tag gruppo) ai gruppi che si prevede di annidare in gruppi più grandi.

8. Quando hai finito, scegli Crea gruppo.

AWS CLI & AWS SDKs

Un gruppo basato su tag si basa su un tipo di query `TAG_FILTERS_1_0`.

1. In una AWS CLI sessione, digita quanto segue, quindi premi Invio, sostituendo i valori per il nome del gruppo, la descrizione, i tipi di risorse, le chiavi dei tag e i valori dei tag con i tuoi. Le descrizioni possono avere un massimo di 512 caratteri, inclusi lettere, numeri, trattini, trattini bassi, punteggiatura e spazi. È possibile avere un massimo di 20 tipi di risorse in una query. Il nome di un gruppo di risorse può avere un massimo di 128 caratteri, inclusi lettere, numeri, trattini, punti e trattini bassi. Il nome non può iniziare per `AWS` o `aws`, poiché sono riservati. Il nome di un gruppo di risorse deve essere univoco nell'account.

   Almeno un valore per `ResourceTypeFilters` è obbligatorio. Per specificare tutti i tipi di risorse, utilizzare `AWS::AllSupported` come valore di `ResourceTypeFilters`.

```
$ aws resource-groups create-group \
    --name resource-group-name \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"resource_type1\",\"resource_type2\"],\"TagFilters\":[{\"Key\":\"Key1\",
\"Values\":[\"Value1\",\"Value2\"]},{\"Key\":\"Key2\",\"Values\":[\"Value1\",
\"Value2\"]}]}"}'
```

   Il comando seguente è un esempio.

```
$ aws resource-groups create-group \
    --name my-resource-group \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::EC2::Instance\"],\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":
[\"Test\"]}]}"}'
```

Il comando seguente è un esempio che include tutti i tipi di risorse supportati.

```
$ aws resource-groups create-group \
    --name my-resource-group \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::AllSupported\"],\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":[\"Test
\"]}]}"}'
```

2. I seguenti risultati vengono restituiti in risposta al comando.

   - Una descrizione completa del gruppo creato.
   - La query delle risorse utilizzata per creare il gruppo.
   - I tag associati al gruppo.

Crea un gruppo basato su AWS CloudFormation stack

Le procedure seguenti mostrano come creare una query basata sullo stack e utilizzarla per creare un gruppo di risorse.

Console

1. Accedere alla console AWS Resource Groups.
2. Nel riquadro di navigazione, scegli Crea gruppo di risorse.
3. In Crea gruppo basato su query, in Tipo di gruppo, scegli il tipo di gruppo basato sullo CloudFormation stack.
4. Scegli lo stack che si desidera sia alla base del gruppo. Un gruppo di risorse può essere basato su un solo stack. Per filtrare l'elenco di stack, iniziare a digitare il nome dello stack. Solo gli stack con gli stati supportati sono riportati nell'elenco.
5. Scegliere i tipi di risorse nello stack che si desidera includere nel gruppo. Per questo scenario, mantenere l'impostazione predefinita, All supported resource types (Tutti i tipi di risorse supportati). Per ulteriori informazioni su quali tipi di risorse sono supportati e possono essere presenti nel gruppo, vedere Tipi di risorse utilizzabili con AWS Resource Groups e Tag Editor.
6. Scegli Visualizza le risorse del gruppo per visualizzare l'elenco delle risorse nello AWS CloudFormation stack che corrispondono ai tipi di risorse selezionati.
7. Dopo aver ottenuto i risultati desiderati, crea un gruppo basato su questa query.

a. In Dettagli del gruppo, in Nome del gruppo, digita un nome per il tuo gruppo di risorse.

   Il nome di un gruppo di risorse può avere un massimo di 128 caratteri, inclusi lettere, numeri, trattini, punti e trattini bassi. Il nome non può iniziare per `AWS` o `aws`, poiché sono riservati. Il nome di un gruppo di risorse deve essere univoco nella regione corrente del tuo account.

b. (Facoltativo) In Group description (Descrizione gruppo), immettere una descrizione del tuo gruppo.

c. (Facoltativo) Nell'area Group tags (Tag gruppo), aggiungere una chiave di tag e coppie di valore che si applicano solo al gruppo di risorse, non alle risorse membri del gruppo.

   I tag del gruppo sono utili se si prevede di rendere questo gruppo un membro di un gruppo più grande. Poiché è necessario specificare almeno una chiave di tag per creare un gruppo, assicurarsi di aggiungere almeno una chiave di tag in Group tags (Tag gruppo) ai gruppi che si prevede di annidare in gruppi più grandi.

8. Quando hai finito, scegli Crea gruppo.

AWS CLI & AWS SDKs

Un gruppo AWS CloudFormation basato sullo stack si basa su una query di tipo. `CLOUDFORMATION_STACK_1_0`

1. Esegui il comando seguente, sostituendo i valori per il nome del gruppo, la descrizione, l'identificatore dello stack e i tipi di risorse con i tuoi. Le descrizioni possono avere un massimo di 512 caratteri, inclusi lettere, numeri, trattini, trattini bassi, punteggiatura e spazi.

   Se non si specificano i tipi di risorse, Resource Groups include tutti i tipi di risorse supportati nello stack. È possibile avere un massimo di 20 tipi di risorse in una query. Il nome di un gruppo di risorse può avere un massimo di 128 caratteri, inclusi lettere, numeri, trattini, punti e trattini bassi. Il nome non può iniziare per `AWS` o `aws`, poiché sono riservati. Il nome di un gruppo di risorse deve essere univoco nell'account.

   Il *`stack_identifier`* è lo stackARN, come illustrato nel comando di esempio.

```
$ aws resource-groups create-group \
    --name group_name \
    --description "description" \
```

```
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"stack_identifier\",\"ResourceTypeFilters\":[\"resource_type1\",
\"resource_type2\"]}"}'
```

Il comando seguente è un esempio.

```
$ aws resource-groups create-group \
    --name My-CFN-stack-group \
    --description "My first CloudFormation stack-based group" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"arn:aws:cloudformation:us-west-2:123456789012:stack\/AWStestuseraccount\/
fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\",\"ResourceTypeFilters\":
[\"AWS::EC2::Instance\",\"AWS::S3::Bucket\"]}"}'
```

2. I seguenti risultati vengono restituiti in risposta al comando.

   - Una descrizione completa del gruppo creato.
   - La query delle risorse utilizzata per creare il gruppo.

Aggiornamento dei gruppi in AWS Resource Groups

Per aggiornare un gruppo di risorse basato su tag in Resource Groups, puoi modificare la query e i tag che sono alla base del tuo gruppo. È possibile aggiungere e rimuovere le risorse dal gruppo solo apportando modifiche alla query o ai tag. Non è possibile selezionare risorse specifiche da aggiungere o rimuovere dal gruppo. Il modo migliore per aggiungere o rimuovere una risorsa specifica da un gruppo è modificare i tag della risorsa. Verifica quindi che la query relativa ai tag del gruppo di risorse includa o meno il tag, a seconda che tu voglia inserire la risorsa nel gruppo.

Per aggiornare un gruppo di risorse AWS CloudFormation basato sullo stack, puoi scegliere uno stack diverso. Puoi anche aggiungere o rimuovere tipi di risorse dallo stack di cui desideri far parte del gruppo. Per modificare le risorse disponibili nello stack, aggiorna il AWS CloudFormation modello utilizzato per creare lo stack, quindi aggiorna lo stack. AWS CloudFormationPer ulteriori informazioni su come aggiornare uno AWS CloudFormation stack,AWS CloudFormation consulta gli aggiornamenti degli stack nella Guida per l'utente.AWS CloudFormation

In AWS CLI, aggiorni i gruppi con due comandi.

- `update-group`, che si esegue per aggiornare la descrizione di un gruppo.
- `update-group-query`, che si esegue per aggiornare la query e i tag delle risorse che determinano le risorse membri del gruppo.

Nella console, non è possibile modificare un gruppo AWS CloudFormation basato sullo stack in un gruppo di query basato su tag o viceversa. Tuttavia, è possibile farlo utilizzando i Resource GroupsAPI, incluso in AWS CLI.

Aggiornare i gruppi di query basati su tag

Le seguenti procedure mostrano come aggiornare un gruppo di query basato su tag.

Console

Aggiorna un gruppo basato su tag modificando i tipi di risorse o tag nella query su cui il gruppo si basa. È anche possibile aggiungere o modificare la descrizione del gruppo.

1. Accedere alla console AWS Resource Groups.
2. Nel riquadro di navigazione, in Saved Resource Groups, scegli il nome del gruppo, quindi scegli Modifica.

> **Note**
>
> Puoi aggiornare solo i gruppi di risorse di cui sei proprietario. La colonna Proprietario mostra la proprietà dell'account per ogni gruppo di risorse. Tutti i gruppi con un proprietario dell'account diverso da quello a cui hai effettuato l'accesso sono stati creati AWS License Manager. Per ulteriori informazioni, consulta Host resource groups AWS License Manager nella License Manager User Guide.

3. Nella pagina Modifica gruppo, in Criteri di raggruppamento, aggiungi o rimuovi i tipi di risorse. È possibile avere un massimo di 20 tipi di risorse in una query. Per rimuovere un tipo di risorsa, scegli la X sull'etichetta del tipo di risorsa. Scegli View group resources (Visualizza risorse gruppo) per visualizzare l'effetto delle modifiche sui membri risorse del gruppo. In questa procedura dettagliata, aggiungiamo il tipo di risorsa AWS:::RDS: DBInstance alla query.
4. Sempre in Criteri di raggruppamento, modifica i tag in base alle esigenze. In questo esempio, filtriamo le risorse che hanno la chiave di tag Stage (Fase) e aggiungiamo il valore di tag Test. Il valore di tag è opzionale, ma restringe ulteriormente i risultati della query. Per rimuovere un tag, scegliere X sull'etichetta del tag.
5. Nell'area Additional information (Ulteriori informazioni), è possibile modificare la descrizione del gruppo. Non è possibile modificare il nome del gruppo dopo aver creato il gruppo.
6. (Facoltativo) Nei tag di gruppo, puoi aggiungere o rimuovere tag. I tag del gruppo sono metadati relativi al gruppo di risorse. Non incidono sulle risorse membro. Per modificare le risorse restituite dalla query del gruppo di risorse, modifica i tag che si trovano in Criteri di raggruppamento.

   I tag del gruppo sono utili se si prevede di rendere questo gruppo un membro di un gruppo più grande. Per creare un gruppo è necessario specificare almeno una chiave di tag. Pertanto, assicuratevi di aggiungere almeno una chiave tag nei tag di gruppo ai gruppi che intendete raggruppare in gruppi più grandi.
7. Scegli Preview group resources per recuperare l'elenco aggiornato di EC2 istanze, bucket S3 e istanze di RDS database Amazon nel tuo account che corrispondono alle chiavi di tag specificate. Se le risorse non vengono visualizzare nell'elenco previsto, verificare che abbiano i tag specificati nell'area Grouping criteria (Criteri di raggruppamento).
8. Al termine, scegliere Save changes (Salva le modifiche).

AWS CLI & AWS SDKs

In AWS CLI, aggiorni la query di un gruppo e aggiorni la descrizione di un gruppo di risorse utilizzando due comandi diversi. Non è possibile modificare il nome di un gruppo esistente. In AWS CLI, è possibile modificare un gruppo basato su tag in un gruppo basato CloudFormation su stack o viceversa.

1. Se non desideri modificare la descrizione del gruppo, salta questa fase e passa a quella successiva. In una AWS CLI sessione, digitate quanto segue, quindi premete Invio, sostituendo i valori per il nome e la descrizione del gruppo con i vostri.

   ```
   $ aws resource-groups update-group \
       --group-name resource-group-name \
       --description "description_text"
   ```

   Il comando seguente è un esempio.

   ```
   $ aws resource-groups update-group \
       --group-name my-resource-group \
       --description "EC2 instances, S3 buckets, and RDS DBs that we are using for
    the test stage."
   ```

   Il comando restituisce una descrizione completa aggiornata del gruppo.

2. Per aggiornare la query e i tag di un gruppo, digitate il comando seguente. Sostituisci i valori per il nome del gruppo, i tipi di risorse, le chiavi dei tag e i valori dei tag con i tuoi. Quindi premi Invio. È possibile avere un massimo di 20 tipi di risorse in una query.

   ```
   $ aws resource-groups update-group-query \
       --group-name resource-group-name \
       --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
   \":[\"resource_type1\",\"resource_type2\"],\"TagFilters\":[{\"Key\":\"Key1\",
   \"Values\":[\"Value1\",\"Value2\"]},{\"Key\":\"Key2\",\"Values\":[\"Value1\",
   \"Value2\"]}]}"}'
   ```

   Il comando seguente è un esempio.

   ```
   $ aws resource-groups update-group-query \
       --group-name my-resource-group \
   ```

```
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::EC2::Instance\",\"AWS::S3::Bucket\",\"AWS::RDS::DBInstance\"],
\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":[\"Test\"]}]}"}'
```

Il comando restituisce la query aggiornata.

Aggiorna un gruppo basato sullo AWS CloudFormation stack

Le seguenti procedure mostrano come aggiornare un gruppo basato sullo CloudFormation stack.

Console

Non è possibile modificare un gruppo basato AWS CloudFormation sullo stack in un gruppo basato su tag in. AWS Management Console Tuttavia, è possibile modificare lo stack su cui si basa il gruppo o modificare i tipi di risorse dello stack che si desidera includere nel gruppo. È anche possibile aggiungere o modificare la descrizione del gruppo.

1. Accedere alla console AWS Resource Groups.
2. Nel riquadro di navigazione, in Gruppi di risorse salvati, scegli il nome del gruppo, quindi scegli Modifica.
3.
> **Note**
>
> Puoi aggiornare solo i gruppi di risorse di cui sei proprietario. La colonna Proprietario mostra la proprietà dell'account per ogni gruppo di risorse. Tutti i gruppi con un proprietario dell'account diverso da quello a cui hai effettuato l'accesso sono stati creati AWS License Manager. Per ulteriori informazioni, consulta Host resource groups AWS License Manager nella License Manager User Guide.

4. Nella pagina Modifica gruppo, in Criteri di raggruppamento, per modificare lo stack su cui si basa il gruppo, scegli lo stack dall'elenco a discesa. Un gruppo di risorse può essere basato su un solo stack. Per filtrare l'elenco di stack, iniziare a digitare il nome dello stack. Solo gli stack con gli stati supportati sono riportati nell'elenco. Per un elenco di stati supportati, vedere Creazione di gruppi basati su query in AWS Resource Groups in questa guida.
5. Aggiungere o rimuovere i tipi di risorse. Solo i tipi di risorse disponibili nello stack sono riportati nell'elenco a discesa. L'impostazione predefinita è All supported resource types (Tutti i tipi di risorse supportati). È possibile avere un massimo di 20 tipi di risorse in una query. Per rimuovere un tipo di risorsa, scegli la X sull'etichetta del tipo di risorsa. Per ulteriori

informazioni su quali tipi di risorse sono supportati e possono essere presenti nel gruppo, vedere Tipi di risorse utilizzabili con AWS Resource Groups e Tag Editor.

6. Scegli Anteprima delle risorse del gruppo per recuperare l'elenco delle risorse nello AWS CloudFormation stack che corrispondono ai tipi di risorse selezionati.
7. Nell'area Additional information (Ulteriori informazioni), è possibile modificare la descrizione del gruppo. Non è possibile modificare il nome del gruppo dopo aver creato il gruppo.
8. In Group tags (Tag gruppo), aggiungere o rimuovere i tag. I tag del gruppo sono metadati relativi al gruppo di risorse. Non incidono sulle risorse membro. Per modificare le risorse restituite dalla query del gruppo di risorse, modificare i tag nell'area Grouping criteria (Criteri di raggruppamento).

   I tag del gruppo sono utili se si prevede di rendere questo gruppo un membro di un gruppo più grande. Per creare un gruppo è necessario specificare almeno una chiave di tag. Pertanto, assicuratevi di aggiungere almeno una chiave tag nei tag di gruppo ai gruppi che intendete raggruppare in gruppi più grandi.
9. Al termine, scegliere Save changes (Salva le modifiche).

AWS CLI & AWS SDKs

In AWS CLI, aggiorni la query di un gruppo e aggiorni la descrizione di un gruppo di risorse utilizzando due comandi diversi. Non è possibile modificare il nome di un gruppo esistente. In AWS CLI, è possibile modificare un gruppo basato su tag in un gruppo basato CloudFormation su stack o viceversa.

1. Se non desideri modificare la descrizione del gruppo, salta questa fase e passa a quella successiva. Esegui il comando seguente, sostituendo i valori per il nome e la descrizione del gruppo con i tuoi.

```
$ aws resource-groups update-group \
    --group-name "resource-group-name" \
    --description "description_text"
```

   Il comando seguente è un esempio.

```
$ aws resource-groups update-group \
    --group-name "My-CFN-stack-group" \
```

```
    --description "EC2 instances, S3 buckets, and RDS DBs that we are using for
 the test stage."
```

Il comando restituisce una descrizione completa aggiornata del gruppo.

2. Per aggiornare la query e i tag di un gruppo, esegui il comando seguente. Sostituisci i valori per il nome del gruppo, l'identificatore dello stack e i tipi di risorse con i tuoi. Per aggiungere tipi di risorse, fornire l'elenco completo dei tipi di risorse nel comando, non solo i tipi di risorse che si stanno aggiungendo. È possibile avere un massimo di 20 tipi di risorse in una query.

   Il *`stack_identifier`* è lo stackARN, come illustrato nel comando di esempio.

```
$ aws resource-groups update-group-query \
    --group-name resource-group-name \
    --description "description" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"stack_identifier\",\"ResourceTypeFilters\":[\"resource_type1\",
\"resource_type2\"]}"}'
```

   Il comando seguente è un esempio.

```
$ aws resource-groups update-group-query \
    --group-name "my-resource-group" \
    --description "Updated CloudFormation stack-based group" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"arn:aws:cloudformation:us-west-2:810000000000:stack\/AWStestuseraccount
\/fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\",\"ResourceTypeFilters\":
[\"AWS::EC2::Instance\",\"AWS::S3::Bucket\"]}"}'
```

   Il comando restituisce la query aggiornata.

Eventi del ciclo di vita del gruppo: monitoraggio dei gruppi di risorse per rilevare eventuali modifiche

Dopo aver organizzato AWS Resource Groups le risorse in gruppi, puoi monitorare tali gruppi per rilevare eventuali modifiche che ti vengono mostrate come eventi. Puoi ricevere una notifica su un evento di gruppo come segnale per intraprendere qualche tipo di azione. Ad esempio, è possibile configurare una notifica da inviare ogni volta che l'appartenenza a un gruppo cambia. È possibile utilizzare un evento derivante dall'aggiunta di un nuovo membro del gruppo per attivare una funzione Lambda che esamina a livello di codice la modifica per garantire che i nuovi membri del gruppo soddisfino i requisiti di conformità stabiliti dall'organizzazione. Tale funzione Lambda potrebbe eseguire la riparazione automatica per tutti i nuovi membri del gruppo che non soddisfano tali requisiti. Un evento causato dalla rimozione di un membro del gruppo potrebbe attivare una funzione Lambda che esegue qualsiasi operazione di pulizia richiesta, ad esempio l'eliminazione delle risorse collegate.

Attivando gli eventi del ciclo di vita dei gruppi per i tuoi gruppi di risorse, consenti che gli eventi relativi alle modifiche ai tuoi gruppi vengano acquisiti da Amazon EventBridge e resi disponibili per tutti i vari servizi di destinazione EventBridge supportati. Puoi quindi configurare questi servizi di destinazione in modo che intraprendano automaticamente le azioni richieste dallo scenario. Questi obiettivi includono una varietà di AWS servizi come Amazon Simple Notification Service (AmazonSNS), Amazon Simple Queue Service (AmazonSQS) e AWS Lambda. Con servizi come Lambda, i tuoi eventi possono attivare risposte programmatiche che utilizzano il codice per eseguire qualsiasi azione richiesta. Per un elenco dei AWS servizi che puoi utilizzare come target EventBridge, consulta Amazon EventBridge targets nella Amazon EventBridge User Guide.

Quando attivi gli eventi del ciclo di vita di gruppo, AWS Resource Groups crea i seguenti elementi:

- Un ruolo collegato al servizio AWS Identity and Access Management (IAM) autorizzato a monitorare le tue risorse per eventuali modifiche ai relativi tag e gli AWS CloudFormation stack per eventuali modifiche alle risorse che fanno parte di uno stack.
- Una EventBridge regola gestita da Resource Groups che acquisisce i dettagli di qualsiasi modifica apportata ai tag o allo stack delle risorse. EventBridge utilizza questa regola per notificare a Resource Groups tali modifiche. Quindi, Resource Groups genera eventi di iscrizione a cui inviare EventBridge per l'elaborazione delle regole personalizzate.

Il ruolo collegato al servizio può essere assunto solo dal servizio Resource Groups. Per ulteriori informazioni sul ruolo collegato ai servizi utilizzato da Resource Groups per questa funzionalità, vedere. Utilizzo di ruoli collegati ai servizi per i Resource Groups

Quando questa funzionalità è attivata, Resource Groups genera un evento quando apporti una delle seguenti modifiche a un gruppo di risorse:

- Crea un nuovo gruppo di risorse.
- Aggiorna la query che definisce l'appartenenza al gruppo di risorse basato sulla query.
- Aggiorna la configurazione di un gruppo di risorse collegato al servizio.
- Aggiorna la descrizione di un gruppo di risorse.
- Eliminare un gruppo di risorse.
- Modifica l'appartenenza a un gruppo di risorse aggiungendo o rimuovendo una risorsa dal gruppo. Una modifica dell'appartenenza può avvenire anche quando i tag cambiano o quando cambia uno AWS CloudFormation stack.

Important

- Per ricevere e rispondere correttamente agli eventi di gruppo, è necessario apportare modifiche sia a Resource Groups che a EventBridge. È possibile eseguire le modifiche in qualsiasi ordine, ma nessun evento di gruppo viene pubblicato sugli EventBridge obiettivi fino a quando non si apportano modifiche a entrambi i servizi.

- Le modifiche al gruppo di risorse non includono modifiche ai tag allegati al gruppo di risorse stesso. Per generare eventi in base alle modifiche dei tag apportate ai gruppi, è necessario utilizzare una EventBridge regola che utilizzi la `aws.tag` fonte anziché la `aws.resource-groups` fonte. Per ulteriori informazioni, consulta gli eventi di modifica dei tag su AWS Resources nella Amazon EventBridge User Guide.

Argomenti

- Attivazione degli eventi del ciclo di vita dei gruppi in Resource Groups
- Creazione di una EventBridge regola per acquisire gli eventi del ciclo di vita del gruppo e pubblicare notifiche
- Disattivazione degli eventi relativi al ciclo di vita del gruppo

- Struttura e sintassi degli eventi del ciclo di vita di Resource Groups

Attivazione degli eventi del ciclo di vita dei gruppi in Resource Groups

Per ricevere notifiche sulle modifiche del ciclo di vita dei gruppi di risorse, puoi attivare gli eventi del ciclo di vita dei gruppi. Resource Groups fornisce quindi informazioni sulle modifiche dei tuoi gruppi ad Amazon EventBridge. Inoltre EventBridge, puoi valutare e agire di conseguenza utilizzando le regole che definisci nel EventBridge servizio.

> **Autorizzazioni minime**
>
> Per attivare gli eventi del ciclo di vita di gruppo nel tuo Account AWS account, devi accedere come preside AWS Identity and Access Management (IAM) con le seguenti autorizzazioni:
>
> - `resource-groups:UpdateAccountSettings`
> - `iam:CreateServiceLinkedRole`
> - `events:PutRule`
> - `events:PutTargets`
> - `events:DescribeRule`
> - `events:ListTargetsByRule`
> - `cloudformation:DescribeStacks`
> - `cloudformation:ListStackResources`
> - `tag:GetResources`

Quando inizialmente si attivano gli eventi del ciclo di vita del gruppo in un Account AWS, Resource Groups crea un ruolo collegato al servizio denominato. `AWSServiceRoleForResourceGroups` Questo ruolo gestito è autorizzato a utilizzare una EventBridge regola gestita da Resource Groups. La regola monitora i tag allegati alle tue risorse e gli AWS CloudFormation stack del tuo account per rilevare eventuali modifiche. Resource Groups pubblica quindi tali modifiche nel bus di eventi predefinito in Amazon EventBridge. Il servizio crea anche una regola EventBridge gestita denominata`Managed.ResourceGroups.TagChangeEvents`. Questa regola acquisisce i dettagli delle modifiche ai tag delle tue risorse. Ciò consente a Resource Groups di generare eventi di appartenenza a cui inviare EventBridge per l'elaborazione delle regole personalizzate. EventBridge

Le tue regole possono quindi rispondere agli eventi inviando notifiche agli obiettivi configurati delle regole.

Dopo aver completato questi passaggi, le regole che cercano questi eventi dovrebbero iniziare a riceverli in pochi minuti.

Puoi attivare gli eventi del ciclo di vita di gruppo utilizzando AWS Management Console o utilizzando un comando dalle AWS CLI o da una delle API SDK.

> **Note**
>
> Non puoi attivare gli eventi del ciclo di vita del gruppo se la quota dei gruppi di risorse è troppo alta. Per ulteriori informazioni, consulta Visualizzazione delle quote di servizio.

AWS Management Console

Per attivare gli eventi del ciclo di vita del gruppo nella console Resource Groups

1. Apri la pagina Impostazioni nella console Resource Groups.
2. Nella sezione Eventi del ciclo di vita del gruppo, scegli l'opzione accanto a Le notifiche sono disattivate.
3. Nella finestra di dialogo di conferma, scegli Attiva notifiche.

   L'interruttore di funzionalità mostra Le notifiche sono attivate.

Questo completa la prima parte del processo. Dopo aver attivato le notifiche degli eventi, puoi creare regole in Amazon EventBridge che acquisiscono gli eventi e li inviano a specifiche aree Servizi AWS per l'elaborazione.

AWS CLI

Per attivare gli eventi del ciclo di vita di gruppo utilizzando gli SDK AWS CLI o AWS

L'esempio seguente mostra come utilizzare per attivare gli eventi del ciclo AWS CLI di vita del gruppo in Resource Groups. Immettete il comando con il parametro service principal esattamente come mostrato. L'output mostra sia lo stato corrente che lo stato desiderato della feature.

```
$ aws resource-groups update-account-settings \
```

```
    --group-lifecycle-events-desired-status ACTIVE
{
    "AccountSettings": {
        "GroupLifecycleEventsDesiredStatus": "ACTIVE",
        "GroupLifecycleEventsStatus": "IN_PROGRESS"
    }
}
```

È possibile confermare che la funzionalità è attivata eseguendo il seguente comando di esempio. Quando entrambi i campi di stato mostrano lo stesso valore, l'operazione è completa.

```
$ aws resource-groups get-account-settings
{
    "AccountSettings": {
        "GroupLifecycleEventsDesiredStatus": "ACTIVE",
        "GroupLifecycleEventsStatus": "ACTIVE"
    }
}
```

Per ulteriori informazioni, consulta le seguenti risorse:

- AWS CLI — aws resource-groups e aws resource-groups update-account-settings get-account-settings
- UpdateAccountSettingsAPI — e GetAccountSettings

Creazione di una EventBridge regola per acquisire gli eventi del ciclo di vita del gruppo e pubblicare notifiche

Puoi attivare gli eventi del ciclo di vita dei gruppi per i tuoi gruppi di risorse per AWS Resource Groups pubblicare eventi su Amazon. EventBridge Quindi, puoi creare EventBridge regole che rispondano a tali eventi inviandole ad altri Servizi AWS per un'ulteriore elaborazione.

AWS CLI

Il processo di creazione di una regola EventBridge che acquisisce gli eventi e li invia al servizio di destinazione desiderato richiede due comandi CLI separati:

1. Crea la EventBridge regola per acquisire gli eventi che desideri
2. Associa alla EventBridge regola un obiettivo in grado di elaborare gli eventi

Passaggio 1: creare la EventBridge regola per acquisire gli eventi

Il comando di AWS CLI `put-rule` esempio seguente crea una EventBridge regola che acquisisce tutte le modifiche degli eventi del ciclo di vita di Resource Groups.

```
$ aws events put-rule \
    --name "CatchAllResourceGroupEvents" \
    --event-pattern '{"source":["aws.resource-groups"]}'
{
    "RuleArn": "arn:aws:events:us-east-1:123456789012:rule/
CatchAllResourceGroupEvents"
}
```

L'output include l'Amazon Resource Name (ARN) della nuova regola.

> **Note**
>
> I valori dei parametri che includono stringhe tra virgolette hanno regole di formattazione diverse in base al sistema operativo e alla shell utilizzati. Per gli esempi di questa guida, mostriamo i comandi che funzionano su una shell BASH Linux. Per istruzioni sulla formattazione delle stringhe con virgolette incorporate per altri sistemi operativi, come il prompt dei comandi di Windows, consultate Uso delle virgolette all'interno delle stringhe nella Guida per l'utente. AWS Command Line Interface Man mano che le stringhe di parametri diventano più complesse, può essere più semplice e meno soggetto a errori accettare il valore di un parametro da un file di testo anziché digitarlo direttamente nella riga di comando.

Il seguente schema di eventi limita gli eventi solo a quelli correlati al gruppo specificato, identificato dal relativo ARN. Questo modello di eventi è una stringa JSON complessa che è molto meno leggibile se compressa in una stringa JSON a riga singola con escape appropriato. Puoi invece archiviarlo in un file.

Memorizza la stringa JSON del pattern di eventi in un file. Nel seguente esempio di codice, il file è`eventpattern.txt`.

```
{
    "source": [ "aws.resource-groups" ],
    "detail": {
```

```
        "group": {
            "arn": [ "my-resource-group-arn" ]
        }
    }
}
```

Quindi, esegui il seguente comando per creare la regola, recuperando il modello di evento personalizzato dal file.

```
$ aws events put-rule \
    --name "CatchResourceGroupEventsForMyGroup" \
    --event-pattern file://eventpattern.txt
{
    "RuleArn": "arn:aws:events:us-east-1:123456789012:rule/
CatchResourceGroupEventsForMyGroup"
}
```

Per acquisire altri tipi di eventi Resource Groups, sostituisci la `--event-pattern` stringa con filtri come quelli presentati nella sezioneEsempi di modelli di eventi EventBridge personalizzati per diversi casi d'uso.

Passaggio 2: Associare alla EventBridge regola un obiettivo in grado di elaborare gli eventi

Ora che hai una regola che cattura gli eventi che ti interessano, puoi allegare uno o più obiettivi per eseguire qualche tipo di elaborazione sugli eventi.

Il AWS CLI `put-targets` comando seguente collega un argomento Amazon Simple Notification Service (Amazon SNS) denominato `my-sns-topic` alla regola creata nell'esempio precedente. Tutti gli abbonati all'argomento ricevono una notifica quando viene apportata una modifica al gruppo specificato nella regola.

```
$ aws events put-targets \
    --rule CatchResourceGroupEventsForMyGroup \
    --targets Id=1,Arn=arn:aws:sns:us-east-1:123456789012:my-sns-topic
{
    "FailedEntryCount": 0,
    "FailedEntries": []
}
```

A questo punto, tutte le modifiche al gruppo che corrispondono allo schema degli eventi nella regola vengono inviate automaticamente alla destinazione o alle destinazioni configurate.

Se, come nell'esempio precedente, la destinazione è un argomento di Amazon SNS, tutti gli abbonati all'argomento ricevono un messaggio contenente l'evento come descritto in. Struttura e sintassi degli eventi del ciclo di vita di Resource Groups

Per ulteriori informazioni, consulta le seguenti risorse:

- AWS CLI— aws events put-rule e aws events put-targets
- PutRuleAPI — e PutTargets

Creazione di una regola per acquisire solo tipi specifici di eventi del ciclo di vita del gruppo

Puoi creare una regola con un modello di evento personalizzato che catturi solo gli eventi che ti interessano. Per informazioni complete su come filtrare gli eventi in arrivo utilizzando un pattern di eventi personalizzato, consulta Amazon EventBridge events nella Amazon EventBridge User Guide.

Ad esempio, supponiamo di volere che una regola elabori solo le notifiche di Resource Groups che indicano la creazione di un nuovo gruppo di risorse. È possibile utilizzare un modello di eventi personalizzato simile all'esempio seguente.

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group State Change" ],
    "detail": {
        "state-change": "create"
    }
}
```

Questo filtro cattura solo gli eventi che hanno quei valori esatti nei campi specificati. Per un elenco completo dei campi disponibili da abbinare, consultaStruttura e sintassi degli eventi del ciclo di vita di Resource Groups.

Disattivazione degli eventi relativi al ciclo di vita del gruppo

Puoi disattivare gli eventi del ciclo di vita di gruppo perAWS Resource Groups impedirne l'emissione ad Amazon EventBridge. È possibile eseguire questa operazione utilizzando laAWS Management Console, un comando dellaAWS CLI o una delle API SDK.

Note

La disattivazione degli eventi del ciclo di vita dei gruppi comporta l'eliminazione della EventBridge regola gestita dei Resource Groups utilizzata per analizzare i tag e gliAWS CloudFormation stack di risorse alla ricerca di modifiche. Resource Groups non possono più trasferire tali modifiche a EventBridge. Qualsiasi regola definita negli EventBridge eventi di ricerca dei Resource Groups interrompe la ricezione di eventi da elaborare. Se intendi attivare nuovamente gli eventi del ciclo di vita di gruppo in future, puoi disabilitare le tue regole. Se non desideri utilizzare di nuovo le regole, è possibile eliminarle. Per ulteriori informazioni, consulta Disattivazione o eliminazione di una EventBridge regola nella Guida per l' EventBridge utente di Amazon.
La disattivazione degli eventi del ciclo di vita del gruppo non elimina il ruolo collegato al servizio. È possibile eliminare il ruolo collegato ai servizi manualmente, se si desidera utilizzando IAM. Se in seguito è necessario attivare nuovamente gli eventi del ciclo di vita del gruppo e il ruolo collegato al servizio non esiste, Resource Groups lo ricrea automaticamente.

Autorizzazioni minime

Per disattivare gli eventi relativi al ciclo di vita del gruppo in usoAccount AWS, devi accedere come titolareAWS Identity and Access Management (IAM) con le seguenti autorizzazioni:

- `resource-groups:UpdateAccountSettings`
- `events:DeleteRule`
- `events:RemoveTargets`
- `events:DescribeRule`
- `events:ListTargetsByRule`

AWS Management Console

Per disattivare le notifiche degli eventi relativi al ciclo di vita del gruppo a EventBridge

1. Apri la pagina Impostazioni nella console Resource Groups.
2. Nella sezione Eventi del ciclo di vita del gruppo, scegli l'interruttore accanto a Le notifiche sono attivate.

3. Nella finestra di dialogo di conferma, scegliere Disattiva (disattiva).

   Viene visualizzato l'interruttore di funzionalità: le notifiche degli eventi sono disattivate.

A questo punto, Resource Groups non invia più gli eventi al bus degli eventi EventBridge predefinito e tutte le regole che non hai più ricevono eventi di notifica di gruppo da elaborare. Facoltativamente, puoi eliminare queste regole per completare la pulizia.

AWS CLI

Per disattivare le notifiche degli eventi relativi al ciclo di vita del gruppo a EventBridge

L'esempio seguente mostra come utilizzare il perAWS CLI disattivare gli eventi del ciclo di vita dei gruppi in Resource Groups.

```
$ aws resource-groups update-account-settings \
    ----group-lifecycle-events-desired-status INACTIVE
{
    "AccountSettings": {
        "GroupLifecycleEventsDesiredStatus": "INACTIVE",
        "GroupLifecycleEventsStatus": "INACTIVE"
    }
}
```

Per ulteriori informazioni, consulta le seguenti risorse :

- AWS CLI— gruppi di risorse aws update-account-settings e gruppi di risorse aws get-account-settings
- API — UpdateAccountSettingse GetAccountSettings

Struttura e sintassi degli eventi del ciclo di vita di Resource Groups

Argomenti

- Struttura del detail campo
- Esempi di modelli di eventi EventBridge personalizzati per diversi casi d'uso

Gli eventi del ciclo di vita AWS Resource Groups assumono la forma di stringhe di JSONoggetti nel seguente formato generale.

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group ... Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/MyGroupName"
    ],
    "detail": {
        ...
    }
}
```

Per dettagli sui campi comuni a tutti gli EventBridge eventi Amazon, consulta Amazon EventBridge events nella Amazon EventBridge User Guide. I dettagli specifici di Resource Groups sono illustrati nella tabella seguente.

Nome del campo	Type	Descrizione
`detail-type`	Stringa	Per Resource Groups, il `detail-type` campo è sempre uno dei seguenti valori: • `ResourceGroups Group State Change` — Rappresenta le modifiche allo stato generale del gruppo e alle relative proprietà. • `ResourceGroups Group Membership Change`— Rappresenta le modifiche all'appar tenenza al gruppo.
`source`	Stringa	Per Resource Groups, questo valore è sempre`"aws.resource-groups"` .
`resources`	Una serie di nomi di risorse Amazon (ARNs)	Questo campo include sempre il nome della risorsa Amazon (ARN) del gruppo con la modifica che ha attivato questo evento.

Nome del campo	Type	Descrizione
		Questo campo può anche includere tutte ARNs le risorse aggiunte o rimosse dal gruppo, se applicabi le.
`detail`	JSONstringa di oggetti	Questo è il payload dell'evento. Il contenuto del `detail` campo varia in base al valore di`detail-type` . Per ulteriori informazioni, consulta la sezione successiva.

Struttura del **`detail`** campo

Il `detail` campo include tutti i dettagli specifici del servizio Resource Groups su una modifica specifica. Il `detail` campo può assumere due forme, una modifica dello stato del gruppo o una modifica dell'appartenenza, in base al valore del `detail-type` campo descritto nella sezione precedente.

> **Important**
>
> I gruppi di risorse in questi eventi sono identificati da una combinazione del gruppo ARN e da un `"unique-id"` campo che contiene un UUID. Includendo un UUID come parte dell'identità di un gruppo di risorse, è possibile distinguere tra un gruppo eliminato e un gruppo diverso che viene successivamente creato con lo stesso nome. È consigliabile considerare la concatenazione dell'ARNID univoco come chiave per il gruppo nei programmi che interagiscono con questi eventi.

Modifica dello stato del gruppo

```
"detail-type": "ResourceGroups Group State Change"
```

Questo `detail-type` valore indica che lo stato del gruppo stesso, inclusi i relativi metadati, è cambiato. Questa modifica si verifica quando un gruppo viene creato, aggiornato o eliminato, come indicato dal `"change"` campo all'`detail`interno di.

Le informazioni incluse nella `details` sezione quando questo `detail-type` viene specificato includono i campi descritti nella tabella seguente.

Nome del campo	Type	Descrizione
`event-sequence`	Doppio	Un numero monotonicamente crescente che specifica la sequenza di eventi per un gruppo specifico. Il numero viene reimpostato quando si elimina il gruppo e si crea un altro gruppo con lo stesso nome.
`group`	`Group`JSONoggetto	L'oggetto di gruppo associato all'evento in base al suo ARN nome e ID univoco.
`state-change`	Stringa	Il tipo di modifica dello stato che si è verificata. Può essere uno dei seguenti valori: • `create` • `update` • `delete`
`old-state`	`GroupState` JSONoggetto	Lo stato del gruppo prima della modifica. L'oggetto include solo i valori delle proprietà modificate.
`new-state`	`GroupState` JSONoggetto	Lo stato del gruppo dopo la modifica. L'oggetto include solo i valori delle proprietà modificate.

L'`group`JSONoggetto contiene gli elementi descritti nella tabella seguente.

Nome del campo	Type	Descrizione
`arn`	Stringa	Il ARN gruppo.
`name`	Stringa	Il nome descrittivo del gruppo.
`unique-id`	GUID	Un GUID valore univoco che distingue tra un gruppo eliminato e un gruppo diverso che è stato successivamente creato con lo stesso nome eARN. Utilizzate la concatenazione di ARN e

Nome del campo	Type	Descrizione
		questo valore come chiave univoca per il gruppo quando utilizzate questi eventi nel codice.

Gli `GroupState` JSON oggetti contengono gli elementi descritti nella tabella seguente.

Nome del campo	Type	Descrizione
`description`	Stringa	La descrizione del gruppo di risorse fornita dal cliente.
`resource-query`	`ResourceQuery` JSONoggetto	Una JSON rappresentazione della query che definisce i membri del gruppo. Questo campo è presente solo per i gruppi basati su una query. La sintassi di questo campo è definita dal tipo di ResourceQuery API dati. Alcuni esempi di ciò sono inclusi negli esempi di eventi Create and Update.
`group-configuration`	`Configuration` JSONoggetto	Una JSON rappresentazione dei parametri di configurazione associati a un gruppo collegato al servizio. Per ulteriori informazioni, vedere Configurazioni dei servizi per i gruppi di risorse nella Guida di riferimento.AWS Resource Groups API

Ciascuno dei seguenti esempi di codice illustra il contenuto del `detail` campo per ogni `state-change` tipo.

Crea

```
"state-change": "create"
```

L'evento indica che è stato creato un nuovo gruppo. L'evento contiene tutte le proprietà dei metadati di gruppo impostate durante la creazione del gruppo. Questo evento è in genere seguito da uno o più eventi di appartenenza al gruppo, a meno che il gruppo non sia vuoto. Le proprietà con un valore nullo non vengono visualizzate nel corpo dell'evento.

L'evento di esempio seguente indica un gruppo di risorse appena creato denominato`my-service-group`. In questo esempio, il gruppo utilizza una query basata su tag che corrisponde solo alle istanze Amazon Elastic Compute Cloud EC2 (Amazon) che dispongono del tag. `"project"="my-service"`

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group State Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-group"
    ],
    "detail": {
        "event-sequence": 1.0,
        "state-change": "create",
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-
group",
            "name": "my-service-group",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        },
        "new-state": {
            "resource-query": {
                "type": "TAG_FILTERS_1_0",
                "query": "{
                    \"ResourceTypeFilters\": [\"AWS::EC2::Instance\"],
                    \"TagFilters\": [{\"Key\":\"project\", \"Values\":[\"my-service\"}]
                }"
            }
        }
    }
}
```

Aggiornamento

`"state-change": "update"`

L'evento indica che un gruppo esistente è stato modificato in qualche modo. L'evento contiene solo le proprietà modificate rispetto allo stato precedente. Le proprietà che non sono state modificate non vengono visualizzate nel corpo dell'evento.

L'evento di esempio seguente indica che la query basata su tag nel gruppo di risorse dell'esempio precedente è stata modificata per includere anche le risorse di EC2 volume Amazon nel gruppo.


```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group State Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-group"
    ],
    "detail": {
        "event-sequence": 3.0,
        "state-change": "update",
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-
group",
            "name": "my-service",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        },
        "new-state": {
            "resource-query": {
                "type": "TAG_FILTERS_1_0",
                "query": "{
                    \"ResourceTypeFilters\": [\"AWS::EC2::Instance\",
 \"AWS::EC2::Volume\"],
                    \"TagFilters\": [{\"Key\":\"project\", \"Values\":[\"my-service\"}]
                }"
            }
        },
        "old-state": {
            "resource-query": {
                "type": "TAG_FILTERS_1_0",
                "query": "{
                    \"ResourceTypeFilters\": [\"AWS::EC2::Instance\"],
                    \"TagFilters\": [{\"Key\":\"Project\", \"Values\":[\"my-service\"}]
```

```
                }"
            }
        }
    }
}
```

Eliminazione

`"state-change": "delete"`

L'evento indica che un gruppo esistente è stato eliminato. Il campo dei dettagli non include metadati sul gruppo oltre alla sua identificazione. Il `event-sequence` campo viene ripristinato dopo questo evento in quanto è, per definizione, l'ultimo evento di questo `arn` e`unique-id`.

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group State Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service"
    ],
    "detail": {
        "event-sequence": 4.0,
        "state-change": "delete",
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
            "name": "my-service",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        }
    }
}
```

Modifica dell'appartenenza al gruppo

`"detail-type": "ResourceGroups Group Membership Change"`

Questo `detail-type` valore indica che l'appartenenza al gruppo è stata modificata dall'aggiunta o dalla rimozione di una risorsa dal gruppo. Quando `detail-type` viene specificato, il `resources`

campo di primo livello include il ARN nome del gruppo la cui appartenenza è stata modificata e le ARNs eventuali risorse aggiunte o rimosse dal gruppo.

Le informazioni incluse nella `details` sezione quando questo `detail-type` viene specificato includono i campi descritti nella tabella seguente.

Nome del campo	Type	Descrizione
`event-sequence`	Doppio	Un numero monotonicamente crescente che indica la sequenza di eventi per un gruppo specifico. Il numero viene reimpostato quando il gruppo viene eliminato e il relativo ID univoco cambia.
`group`	`Group`JSONoggetto	Identifica l'oggetto di gruppo associato all'evento tramite il relativo ARN nome e ID univoco.
`resources`	Matrice di oggetti `ResourceChange` JSON	Una serie di risorse la cui appartenenza al gruppo è cambiata. Questo `ResourceChange` oggetto contiene i seguenti campi per ogni risorsa: • `membership-change` — Il valore è `"add"` o`"remove"`. • `arn`— La ARN risorsa aggiunta o rimossa. • `resource-type` — Il tipo di risorsa aggiunta o rimossa.

Il seguente esempio di codice illustra il contenuto dell'evento per un tipo tipico di modifica dell'iscrizione. Questo esempio mostra una risorsa che viene aggiunta al gruppo e una risorsa che viene rimossa dal gruppo.

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group Membership Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
```

```
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-efef2222"
    ],
    "detail": {
        "event-sequence": 2.0,
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
            "name": "my-service",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        },
        "resources": [
            {
                "membership-change": "add",
                "arn": "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111",
                "resource-type": "AWS::EC2::Instance"
            },
            {
                "membership-change": "remove",
                "arn": "arn:aws:ec2:us-east-1:123456789012:instance/i-efef2222",
                "resource-type": "AWS::EC2::Instance"
            }
        ]
    }
}
```

Esempi di modelli di eventi EventBridge personalizzati per diversi casi d'uso

I modelli di eventi EventBridge personalizzati seguenti filtrano gli eventi generati da Resource Groups solo in base a quelli che ti interessano per una regola e un obiettivo di evento specifici.

Nei seguenti esempi di codice, se è necessario un gruppo o una risorsa specifici, sostituiteli tutti *`user input placeholder`* con le tue informazioni.

Tutti gli eventi Resource Groups

```
{
    "source": [ "aws.resource-groups" ]
}
```

Eventi di modifica dello stato o dell'appartenenza al gruppo

Il seguente esempio di codice riguarda tutte le modifiche allo stato del gruppo.

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group State Change " ]
}
```

Il seguente esempio di codice riguarda tutte le modifiche relative all'appartenenza ai gruppi.

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ]
}
```

Eventi per un gruppo specifico

```
{
    "source": [ "aws.resource-groups" ],
    "detail": {
        "group": {
            "arn": [ "my-group-arn" ]
        }
    }
}
```

L'esempio precedente acquisisce le modifiche al gruppo specificato. L'esempio seguente esegue la stessa operazione e acquisisce anche le modifiche quando il gruppo è una risorsa membro di un altro gruppo.

```
{
    "source": [ "aws.resource-groups" ],
    "resources": [ "my-group-arn" ]
}
```

Eventi per una risorsa specifica

È possibile filtrare solo gli eventi di modifica dell'appartenenza al gruppo per risorse specifiche dei membri.

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change " ],
    "resources": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ]
}
```

Eventi per un tipo di risorsa specifico

È possibile utilizzare la corrispondenza del prefisso con ARNs per abbinare gli eventi per un tipo di risorsa specifico.

```
{
    "source": [ "aws.resource-groups" ],
    "resources": [
        { "prefix": "arn:aws:ec2:us-east-1:123456789012:instance" }
    ]
}
```

In alternativa, è possibile utilizzare la corrispondenza esatta utilizzando `resource-type` identificatori, che potenzialmente corrispondono a più di un tipo in modo conciso. A differenza dell'esempio precedente, l'esempio seguente corrisponde solo agli eventi di modifica dell'appartenenza al gruppo perché gli eventi di modifica dello stato del gruppo non includono un `resources` campo nel loro campo. `detail`

```
{
    "source": [ "aws.resource-groups" ],
    "detail": {
        "resources": {
                "resource-type": [ "AWS::EC2::Instance", "AWS::EC2::Volume" ]
         }
    }
}
```

Tutti gli eventi di rimozione delle risorse

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ],
    "detail": {
        "resources": {
                "membership-change": [ "remove" ]
```

```
        }
    }
}
```

Tutti gli eventi di rimozione delle risorse per una risorsa specifica

```
 {
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ],
    "detail": {
        "resources": {
                "membership-change": [ "remove" ],
                "arn": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ]
         }
    }
}
```

Non è possibile utilizzare l'`resources`array di primo livello utilizzato nel primo esempio di questa sezione per questo tipo di filtro degli eventi. Questo perché una risorsa nell'`resources`elemento di primo livello potrebbe essere una risorsa aggiunta a un gruppo e l'evento continuerebbe a corrispondere. In altre parole, il seguente esempio di codice potrebbe restituire eventi imprevisti. Utilizzate invece la sintassi mostrata nell'esempio precedente.

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ],
    "resources": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ],
    "detail": {
        "resources": {
                "membership-change": [ "remove" ]
         }
     }
}
```

Eliminazione di gruppi di risorse da AWS Resource Groups

È possibile utilizzare la AWS Resource Groups console o AWS CLI eliminare i gruppi di risorse da AWS Resource Groups. L'eliminazione di un gruppo di risorse non elimina le risorse membri del gruppo o i tag sulle risorse membri. Questa operazione elimina solo la struttura del gruppo e qualsiasi tag a livello di gruppo.

Console

Per eliminare i gruppi di risorse

1. Accedere alla console AWS Resource Groups.
2. Nel riquadro di navigazione, scegli Saved Resource Groups.
3. Scegli il nome del gruppo di risorse che desideri eliminare, quindi scegli Visualizza dettagli.
4. Nella pagina dei dettagli del gruppo, scegli Elimina nell'angolo in alto a destra.
5. Quando viene richiesto di confermare l'eliminazione, scegliere Delete (Elimina).

AWS CLI & AWS SDKs

Per eliminare i gruppi di risorse

1. Esegui il comando seguente, sostituendo *resource_group_name* con il nome del tuo gruppo.

```
$ aws resource-groups delete-group \
    --group-name resource_group_name
```

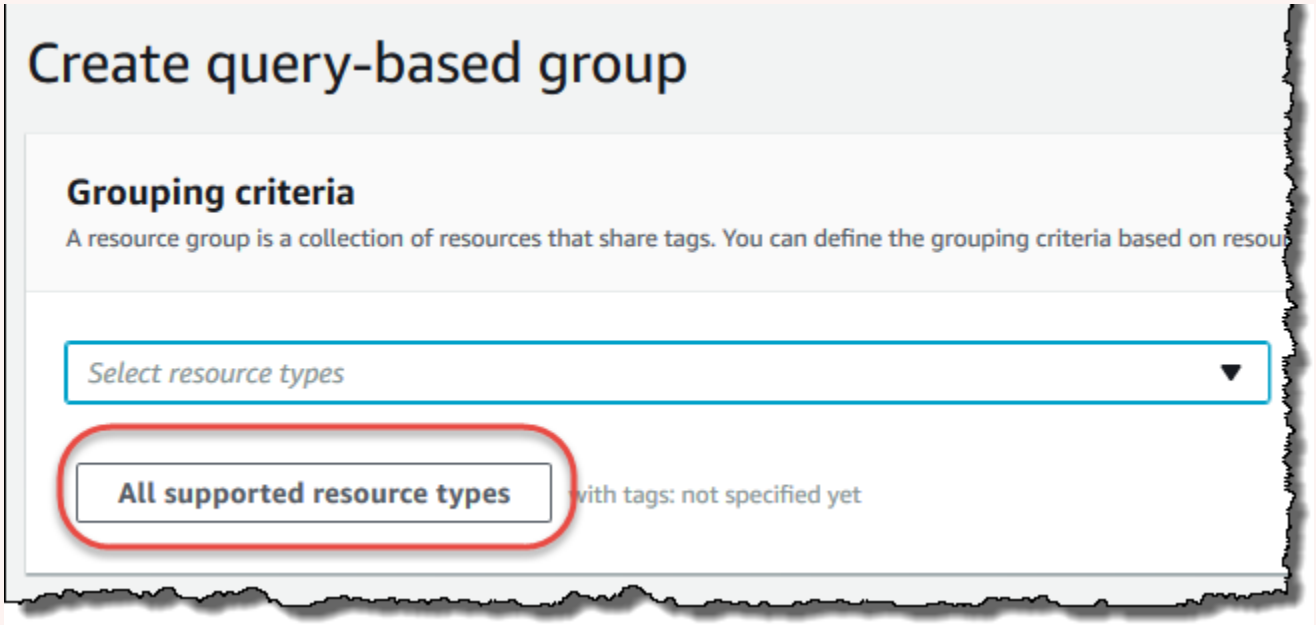
2. Quando viene richiesto di confermare l'eliminazione, digitare `yes`, quindi premere Enter (Invio).

Tipi di risorse utilizzabili con AWS Resource Groups e Tag Editor

Puoi usare AWS Management Console o the AWS CLI per creare gruppi di risorse e quindi interagire con le risorse dei membri tramite tali gruppi. È possibile aggiungere tag a molte AWS risorse e quindi utilizzare tali tag per gestire l'appartenenza al gruppo. Questo argomento descrive i tipi di AWS risorse che è possibile includere nei gruppi di risorse utilizzando AWS Resource Groups e i tipi di risorse che è possibile etichettare utilizzando Tag Editor.

Important

Un gruppo di risorse basato su una query per Tutti i tipi di risorse supportati può aggiungere membri automaticamente nel tempo, poiché le nuove risorse sono supportate da Resource Groups. Quando esegui automazioni o altre attività in blocco su un gruppo di risorse esistente basato su Tutti i tipi di risorse supportati, tieni presente che le azioni potrebbero essere eseguite su molte più risorse rispetto a quelle presenti nel gruppo quando hai creato il gruppo per la prima volta. Ciò potrebbe anche significare che le automazioni o le attività create per altre risorse vengono applicate a risorse probabilmente non intenzionali o a risorse su cui le attività non possono essere completate con successo. In questi casi, puoi aggiungere un filtro per i tipi di risorse per specificare che solo le risorse dei tipi specificati possono far parte del gruppo.



Le tabelle seguenti elencano i tipi di risorse supportati per l'aggiunta di tag in Tag Editor, per l'appartenenza a gruppi basati su query di tag e per l'appartenenza a AWS CloudFormation gruppi basati su stack.

Definizioni delle colonne

- Etichettatura di Tag Editor: puoi etichettare risorse di questo tipo utilizzando la console Tag Editor. In caso contrario, è necessario utilizzare i servizi di tagging AWS Resource Groups Tagging APIo i servizi di tagging supportati nativamente dal servizio proprietario della risorsa.
- Gruppi basati su tag: è possibile includere risorse di questo tipo in gruppi di risorse la cui appartenenza è determinata dai tag allegati alle risorse. Il gruppo specifica i nomi e i valori delle chiavi dei tag e tutte le risorse con tag corrispondenti fanno automaticamente parte del gruppo
- AWS CloudFormation Gruppi basati su stack: è possibile includere risorse di questo tipo in gruppi di risorse la cui appartenenza è costituita dalle risorse create come parte di uno stack. CloudFormation Il gruppo specifica l'ARN dello stack e tutte le relative risorse sono automaticamente membri del gruppo. L'aggiunta di tag a uno AWS CloudFormation stack causa un aggiornamento dello stack.

Per un elenco dei tipi di risorse obsoleti e non più supportati da Resource Groups, vedere la sezione alla Tipi di risorse obsoleti fine di questo argomento.

> **Note**
>
> Resource Groups e Tag Editor supportano i tipi di risorse riportati nella tabella seguente, ma alcuni tipi di risorse potrebbero non essere disponibili nella tua Regione AWS.

Amazon API Gateway

Risorse	Etichettatura in Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::ApiGateway::Account`	✗ No	✗ No	✓ Sì
`AWS::ApiGateway::ApiKey`	✗ No	✓ Sì	✓ Sì
`AWS::ApiGateway::ClientCertificate`	✗ No	✓ Sì	✗ No
`AWS::ApiGateway::DomainName`	✗ No	✗ No	✓ Sì
`AWS::ApiGateway::RestApi`	✗ No	✓ Sì	✓ Sì
`AWS::ApiGateway::Stage`	✗ No	✓ Sì	✗ No
`AWS::ApiGateway::UsagePlan`	✗ No	✓ Sì	✓ Sì

Gateway Amazon API V2

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::ApiGatewayV2::Api`	✗ No	✓ Sì	✗ No

Sistema di analisi degli accessi AWS IAM

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::AccessAnalyzer::Analyzer`	✗ No	✓ Sì	✗ No

AWS Amplify

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Amplify::App`	✗ No	✓ Sì	✗ No

AWS App Mesh

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::AppMesh::Mesh`	✗ No	✓ Sì	✗ No

Amazon AppStream

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::AppStream::AppBlock`	✗ No	✓ Sì	✗ No
`AWS::AppStream::Application`	✗ No	✓ Sì	✗ No
`AWS::AppStream::Fleet`	✓ Sì	✓ Sì	✓ Sì
`AWS::AppStream::ImageBuilder`	✓ Sì	✓ Sì	✓ Sì
`AWS::AppStream::Stack`	✓ Sì	✓ Sì	✓ Sì

AWS AppSync

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::AppSync::DataSource`	✗ No	✗ No	✓ Sì
`AWS::AppSync::GraphQLApi`	✗ No	✗ No	✓ Sì

Amazon Athena

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Athena::DataCatalog`	✗ No	✓ Sì	✗ No
`AWS::Athena::WorkGroup`	✗ No	✓ Sì	✗ No

AWS Backup

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Backup::BackupPlan`	✗ No	✓ Sì	✗ No
`AWS::Backup::BackupVault`	✗ No	✓ Sì	✗ No
`AWS::Backup::ReportPlan`	✗ No	✓ Sì	✗ No

AWS Batch

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Batch::ComputeEnvironment`	✗ No	✓ Sì	✗ No
`AWS::Batch::JobQueue`	✗ No	✓ Sì	✗ No
`AWS::Batch::SchedulingPolicy`	✗ No	✓ Sì	✗ No

AWS Billing Conductor

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::BillingConductor::BillingGroup`	✗ No	✓ Sì	✓ Sì
`AWS::BillingConductor::CustomLineItem`	✗ No	✓ Sì	✓ Sì
`AWS::BillingConductor::PricingPlan`	✗ No	✓ Sì	✓ Sì
`AWS::BillingConductor::PricingRule`	✗ No	✓ Sì	✓ Sì

Amazon Braket

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Braket::Job`	✗ No	✓ Sì	✗ No
`AWS::Braket::QuantumTask`	✓ Sì	✓ Sì	✗ No

AWS Certificate Manager

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::CertificateManager::Certificate`	✓ Sì	✓ Sì	✓ Sì

AWS Certificate Manager Autorità di certificazione privata

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::ACMPCA::CertificateAuthority`	✗ No	✓ Sì	✗ No

AWS Cloud9

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Cloud9::Environment`	✓ Sì	✓ Sì	✗ No

AWS CloudFormation

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::CloudFormation::Stack`	✓ Sì	✓ Sì	✓ Sì

Amazon CloudFront

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::CloudFront::Distribution`	✓ Sì[1]	✓ Sì[2]	✓ Sì[2]

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::CloudFront::StreamingDistribution`	✓ Sì[1]	✓ Sì[2]	✓ Sì[2]

[1] Questa è una risorsa per un servizio globale ospitato nella regione Stati Uniti orientali (Virginia settentrionale). Per utilizzare Tag Editor per creare o modificare tag per questo tipo di risorsa, è necessario `us-east-1` includerli dall'elenco Seleziona regioni sotto Trova risorse da etichettare nella console Tag Editor.

[2] Questa è una risorsa per un servizio globale ospitato nella regione Stati Uniti orientali (Virginia settentrionale). Poiché i Resource Groups vengono gestiti separatamente per ogni regione, è necessario passare AWS Management Console a Regione AWS quello che contiene le risorse che si desidera includere nel gruppo. Per creare un gruppo di risorse che contenga una risorsa globale, devi AWS Management Console configurare US-east-1 in US East (Virginia settentrionale) utilizzando il selettore Regione nell'angolo in alto a destra di. AWS Management Console

AWS Cloud Map

Risorse	Tag Editor: etichettatura	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::ServiceDiscovery::Service`	✗ No	✓ Sì	✗ No

AWS CloudTrail

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::CloudTrail::Channel`	✗ No	✓ Sì	✗ No
`AWS::CloudTrail::EventDataStore`	✗ No	✓ Sì	✗ No
`AWS::CloudTrail::Trail`	✓ Sì	✓ Sì	✓ Sì

Amazon CloudWatch

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::CloudWatch::Alarm`	✓ Sì	✓ Sì	✓ Sì
`AWS::CloudWatch::Dashboard`	✗ No	✗ No	✓ Sì
`AWS::CloudWatch::InsightRule`	✗ No	✓ Sì	✗ No
`AWS::CloudWatch::MetricStream`	✗ No	✓ Sì	✗ No
`AWS::CloudWatch::ServiceLevelObjective`	✗ No	✓ Sì	✗ No

CloudWatch Registri Amazon

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Logs::Destination`	✗ No	✓ Sì	✗ No
`AWS::Logs::LogGroup`	✗ No	✓ Sì	✓ Sì

Amazon CloudWatch Synthetics

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Synthetics::Canary`	✗ No	✓ Sì	✓ Sì

AWS CodeArtifact

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::CodeArtifact::Domain`	✓ Sì	✓ Sì	✓ Sì

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::CodeArtifact::Repository`	✓ Sì	✓ Sì	✓ Sì

AWS CodeBuild

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::CodeBuild::Project`	✓ Sì	✓ Sì	X No

AWS CodeCommit

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::CodeCommit::Repository`	✓ Sì	✓ Sì	X No

AWS CodeDeploy

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::CodeDeploy::Application`	✗ No	✓ Sì	✓ Sì
`AWS::CodeDeploy::DeploymentConfig`	✗ No	✗ No	✓ Sì

CodeGuru Revisore Amazon

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::CodeGuruReviewer::RepositoryAssociation`	✓ Sì	✓ Sì	✓ Sì

Amazon CodeGuru Profiler

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::CodeGuruProfiler::ProfilingGroup`	✗ No	✓ Sì	✗ No

AWS CodePipeline

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::CodePipeline::CustomActionType`	✗ No	✓ Sì	✗ No
`AWS::CodePipeline::Pipeline`	✓ Sì	✓ Sì	✓ Sì
`AWS::CodePipeline::Webhook`	✓ Sì	✓ Sì	✓ Sì

AWS CodeConnections

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::CodeStarConnections::Connection`	✗ No	✓ Sì	✗ No

Amazon Cognito

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Cognito::IdentityPool`	✓ Sì	✓ Sì	✓ Sì
`AWS::Cognito::UserPool`	✓ Sì	✓ Sì	✓ Sì

Amazon Comprehend

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Comprehend::DocumentClassifier`	✓ Sì	✓ Sì	✗ No

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Comprehend::EntityRecognizer`	✓ Sì	✓ Sì	✗ No

AWS Config

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Config::AggregationAuthorization`	✗ No	✓ Sì	✗ No
`AWS::Config::ConfigRule`	✓ Sì	✓ Sì	✗ No
`AWS::Config::ConfigurationAggregator`	✗ No	✓ Sì	✗ No
`AWS::Config::StoredQuery`	✗ No	✓ Sì	✗ No

Amazon Connect

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Connect::Instance`	✗ No	✓ Sì	✗ No
`AWS::Connect::PhoneNumber`	✗ No	✓ Sì	✗ No

Amazon Connect Wisdom

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Wisdom::Assistant`	✗ No	✓ Sì	✓ Sì
`AWS::Wisdom::AssistantAssociation`	✗ No	✓ Sì	✓ Sì
`AWS::Wisdom::Content`	✗ No	✓ Sì	✗ No
`AWS::Wisdom::KnowledgeBase`	✗ No	✓ Sì	✓ Sì
`AWS::Wisdom::Session`	✗ No	✓ Sì	✗ No

AWS Data Exchange

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::DataExchange::DataSet`	✓ Sì	✓ Sì	✗ No
`AWS::DataExchange::Revision`	✗ No	✓ Sì	✗ No

AWS Data Pipeline

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::DataPipeline::Pipeline`	✓ Sì	✓ Sì	✓ Sì

AWS DataSync

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::DataSync::Task`	✗ No	✓ Sì	✗ No

AWS Database Migration Service

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::DMS::Certificate`	✓ Sì	✓ Sì	✗ No
`AWS::DMS::Endpoint`	✓ Sì	✓ Sì	✓ Sì
`AWS::DMS::EventSubscription`	✓ Sì	✓ Sì	✗ No
`AWS::DMS::ReplicationInstance`	✓ Sì	✓ Sì	✓ Sì
`AWS::DMS::ReplicationSubnetGroup`	✓ Sì	✓ Sì	✗ No
`AWS::DMS::ReplicationTask`	✓ Sì	✓ Sì	✗ No

AWS Device Farm

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::DeviceFarm::InstanceProfile`	✗ No	✓ Sì	✗ No
`AWS::DeviceFarm::Project`	✗ No	✓ Sì	✗ No
`AWS::DeviceFarm::TestGridProject`	✗ No	✓ Sì	✗ No

Amazon DynamoDB

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::DynamoDB::Table`	✓ Sì	✓ Sì	✓ Sì

Amazon EMR

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::EMR::Cluster`	✓ Sì	✓ Sì	✓ Sì

Contenitori Amazon EMR

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::EMRContainers::JobRun`	✗ No	✓ Sì	✗ No
`AWS::EMRContainers::VirtualCluster`	✓ Sì	✓ Sì	✓ Sì

Amazon EMR Serverless

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::EMRServerless::Application`	✗ No	✓ Sì	✓ Sì
`AWS::EMRServerless::JobRun`	✗ No	✓ Sì	✗ No

Amazon ElastiCache

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::ElastiCache::CacheCluster`	✓ Sì	✓ Sì	✓ Sì
`AWS::ElastiCache::ParameterGroup`	✗ No	✓ Sì	✗ No
`AWS::ElastiCache::SecurityGroup`	✗ No	✓ Sì	✗ No
`AWS::ElastiCache::Snapshot`	✓ Sì	✓ Sì	✗ No
`AWS::ElastiCache::SubnetGroup`	✗ No	✓ Sì	✗ No
`AWS::ElastiCache::User`	✗ No	✓ Sì	✗ No
`AWS::ElastiCache::UserGroup`	✗ No	✓ Sì	✗ No

AWS Elastic Beanstalk

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::ElasticBeanstalk::Application`	✓ Sì	✓ Sì	× No
`AWS::ElasticBeanstalk::ApplicationVersion`	× No	✓ Sì	× No
`AWS::ElasticBeanstalk::ConfigurationTemplate`	× No	✓ Sì	× No
`AWS::ElasticBeanstalk::Environment`	× No	✓ Sì	× No

Amazon Elastic Compute Cloud (Amazon EC2)

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::EC2::CapacityReservation`	× No	✓ Sì	× No
`AWS::EC2::CapacityReservationFleet`	× No	✓ Sì	× No
`AWS::EC2::CarrierGateway`	× No	✓ Sì	× No
`AWS::EC2::ClientVpnEndpoint`	× No	✓ Sì	× No
`AWS::EC2::CoipPool`	× No	✓ Sì	× No

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
AWS::EC2::CustomerGateway	✓ Sì	✓ Sì	✓ Sì
AWS::EC2::DHCPOptions	✓ Sì	✓ Sì	✓ Sì
AWS::EC2::EC2Fleet	× No	✓ Sì	× No
AWS::EC2::EgressOnlyInternetGateway	× No	✓ Sì	× No
AWS::EC2::EIP	✓ Sì	✓ Sì	× No
AWS::EC2::ExportImageTask	× No	✓ Sì	× No
AWS::EC2::ExportInstanceTask	× No	✓ Sì	× No
AWS::EC2::FlowLog	× No	✓ Sì	× No
AWS::EC2::FpgaImage	× No	✓ Sì	× No
AWS::EC2::Host	× No	✓ Sì	× No
AWS::EC2::HostReservation	× No	✓ Sì	× No
AWS::EC2::Image	✓ Sì	✓ Sì	× No
AWS::EC2::ImportImageTask	× No	✓ Sì	× No
AWS::EC2::ImportSnapshotTask	× No	✓ Sì	× No
AWS::EC2::Instance	✓ Sì	✓ Sì	✓ Sì
AWS::EC2::InstanceEventWindow	× No	✓ Sì	× No
AWS::EC2::InternetGateway	✓ Sì	✓ Sì	✓ Sì

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
AWS::EC2::IPv4Pool	✗ No	✓ Sì	✗ No
AWS::EC2::IPv6Pool	✗ No	✓ Sì	✗ No
AWS::EC2::KeyPair	✗ No	✓ Sì	✗ No
AWS::EC2::LaunchTemplate	✗ No	✓ Sì	✓ Sì
AWS::EC2::LocalGateway	✗ No	✓ Sì	✗ No
AWS::EC2::LocalGatewayRouteTable	✗ No	✓ Sì	✗ No
AWS::EC2::LocalGatewayRouteTableVirtualInterfaceGroupAssociation	✗ No	✓ Sì	✗ No
AWS::EC2::LocalGatewayRouteTableVPCAssociation	✗ No	✓ Sì	✗ No
AWS::EC2::LocalGatewayVirtualInterface	✗ No	✓ Sì	✗ No
AWS::EC2::LocalGatewayVirtualInterfaceGroup	✗ No	✓ Sì	✗ No
AWS::EC2::NatGateway	✓ Sì	✓ Sì	✓ Sì
AWS::EC2::NetworkAcl	✓ Sì	✓ Sì	✓ Sì
AWS::EC2::NetworkInsightsAccessScope	✗ No	✓ Sì	✗ No
AWS::EC2::NetworkInsightsAccessScopeAnalysis	✗ No	✓ Sì	✗ No

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
AWS::EC2::NetworkInsightsAnalysis	✗ No	✓ Sì	✗ No
AWS::EC2::NetworkInsightsPath	✗ No	✓ Sì	✗ No
AWS::EC2::NetworkInterface	✓ Sì	✓ Sì	✓ Sì
AWS::EC2::PlacementGroup	✗ No	✓ Sì	✓ Sì
AWS::EC2::PrefixList	✗ No	✓ Sì	✗ No
AWS::EC2::ReplaceRootVolumeTask	✗ No	✓ Sì	✗ No
AWS::EC2::ReservedInstance	✓ Sì	✓ Sì	✗ No
AWS::EC2::RouteTable	✓ Sì	✓ Sì	✓ Sì
AWS::EC2::SecurityGroup	✓ Sì	✓ Sì	✓ Sì
AWS::EC2::Snapshot	✓ Sì	✓ Sì	✗ No
AWS::EC2::SpotFleet	✗ No	✓ Sì	✗ No
AWS::EC2::SpotInstanceRequest	✓ Sì	✓ Sì	✗ No
AWS::EC2::Subnet	✓ Sì	✓ Sì	✓ Sì
AWS::EC2::SubnetCidrReservation	✗ No	✓ Sì	✗ No
AWS::EC2::TrafficMirrorFilter	✗ No	✓ Sì	✗ No
AWS::EC2::TrafficMirrorSession	✗ No	✓ Sì	✗ No
AWS::EC2::TrafficMirrorTarget	✗ No	✓ Sì	✗ No

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
AWS::EC2::TransitGateway	✗ No	✓ Sì	✗ No
AWS::EC2::TransitGatewayAttachment	✗ No	✓ Sì	✗ No
AWS::EC2::TransitGatewayConnectPeer	✗ No	✓ Sì	✗ No
AWS::EC2::TransitGatewayMulticastDomain	✗ No	✓ Sì	✗ No
AWS::EC2::TransitGatewayPolicyTable	✗ No	✓ Sì	✗ No
AWS::EC2::TransitGatewayRouteTable	✗ No	✓ Sì	✗ No
AWS::EC2::TransitGatewayRouteTableAnnouncement	✗ No	✓ Sì	✗ No
AWS::EC2::VerifiedAccessEndpoint	✗ No	✓ Sì	✗ No
AWS::EC2::VerifiedAccessGroup	✗ No	✓ Sì	✗ No
AWS::EC2::VerifiedAccessInstance	✗ No	✓ Sì	✗ No
AWS::EC2::VerifiedAccessTrustProvider	✗ No	✓ Sì	✗ No
AWS::EC2::Volume	✓ Sì	✓ Sì	✓ Sì
AWS::EC2::VPC	✓ Sì	✓ Sì	✓ Sì
AWS::EC2::VPCEndpoint	✗ No	✓ Sì	✗ No
AWS::EC2::VPCEndpointConnection	✗ No	✓ Sì	✗ No
AWS::EC2::VPCEndpointService	✗ No	✓ Sì	✗ No

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::EC2::VPCEndpointServicePermissions`	✗ No	✓ Sì	✗ No
`AWS::EC2::VPCPeeringConnection`	✗ No	✓ Sì	✓ Sì
`AWS::EC2::VPNConnection`	✓ Sì	✓ Sì	✓ Sì
`AWS::EC2::VPNGateway`	✓ Sì	✓ Sì	✓ Sì

Amazon Elastic Container Registry

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::ECR::Repository`	✗ No	✓ Sì	✗ No

Amazon Elastic Container Service

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::ECS::CapacityProvider`	✗ No	✓ Sì	✗ No
`AWS::ECS::Cluster`	✓ Sì	✓ Sì	✗ No
`AWS::ECS::ContainerInstance`	✗ No	✓ Sì	✗ No
`AWS::ECS::Service`	✗ No	✓ Sì	✗ No
`AWS::ECS::Task`	✗ No	✓ Sì	✗ No
`AWS::ECS::TaskDefinition`	✓ Sì	✓ Sì	✗ No
`AWS::ECS::TaskSet`	✗ No	✓ Sì	✗ No

Amazon Elastic File System

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::EFS::FileSystem`	✓ Sì	✓ Sì	✓ Sì

Amazon Elastic Inference

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::ElasticInference::ElasticInferenceAccelerator`	✓ Sì	✓ Sì	✗ No

Amazon Elastic Kubernetes Service (Amazon EKS)

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::EKS::Addon`	✗ No	✓ Sì	✗ No
`AWS::EKS::Cluster`	✓ Sì	✓ Sì	✓ Sì

Sistema di bilanciamento del carico elastico

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::ElasticLoadBalancing::LoadBalancer`	✓ Sì	✓ Sì	✓ Sì
`AWS::ElasticLoadBalancingV2::Listener`	× No	✓ Sì	✓ Sì
`AWS::ElasticLoadBalancingV2::ListenerRule`	× No	✓ Sì	✓ Sì
`AWS::ElasticLoadBalancingV2::LoadBalancer`	✓ Sì	✓ Sì	✓ Sì
`AWS::ElasticLoadBalancingV2::TargetGroup`	✓ Sì	✓ Sì	✓ Sì

OpenSearch Servizio Amazon

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Elasticsearch::Domain`	✓ Sì	✓ Sì	✓ Sì

CloudWatch Eventi Amazon

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Events::EventBus`	✗ No	✓ Sì	✗ No
`AWS::Events::Rule`	✓ Sì	✓ Sì	✓ Sì

> **Note**
>
> Le regole nei bus di eventi personalizzati non sono supportate in Tag Editor.

EventBridge Schemi Amazon

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::EventSchemas::Discoverer`	✗ No	✓ Sì	✗ No
`AWS::EventSchemas::Registry`	✗ No	✓ Sì	✗ No
`AWS::EventSchemas::Schema`	✗ No	✓ Sì	✗ No

Amazon FSx

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::FSx::FileSystem`	✓ Sì	✓ Sì	✗ No
`AWS::FSx::StorageVirtualMachine`	✗ No	✓ Sì	✗ No
`AWS::FSx::Volume`	✗ No	✓ Sì	✗ No

Amazon Forecast

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Forecast::Dataset`	✓ Sì	✓ Sì	✗ No
`AWS::Forecast::DatasetGroup`	✓ Sì	✓ Sì	✗ No
`AWS::Forecast::DatasetImportJob`	✓ Sì	✓ Sì	✗ No
`AWS::Forecast::Forecast`	✓ Sì	✓ Sì	✗ No
`AWS::Forecast::ForecastExportJob`	✓ Sì	✓ Sì	✗ No
`AWS::Forecast::Predictor`	✓ Sì	✓ Sì	✗ No

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Forecast::PredictorBacktestExportJob`	✓ Sì	✓ Sì	× No

Amazon Fraud Detector

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::FraudDetector::Detector`	✓ Sì	✓ Sì	× No
`AWS::FraudDetector::DetectorVersion`	× No	✓ Sì	× No
`AWS::FraudDetector::EntityType`	✓ Sì	✓ Sì	× No
`AWS::FraudDetector::EventType`	✓ Sì	✓ Sì	× No
`AWS::FraudDetector::ExternalModel`	✓ Sì	✓ Sì	× No
`AWS::FraudDetector::Label`	✓ Sì	✓ Sì	× No
`AWS::FraudDetector::Model`	✓ Sì	✓ Sì	× No
`AWS::FraudDetector::ModelVersion`	× No	✓ Sì	× No
`AWS::FraudDetector::Outcome`	✓ Sì	✓ Sì	× No
`AWS::FraudDetector::Rule`	× No	✓ Sì	× No

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::FraudDetector::Variable`	✓ Sì	✓ Sì	✗ No

Amazon GameLift

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::GameLift::Alias`	✗ No	✓ Sì	✗ No
`AWS::GameLift::GameSessionQueue`	✗ No	✓ Sì	✗ No
`AWS::GameLift::Location`	✗ No	✓ Sì	✗ No
`AWS::GameLift::MatchmakingConfiguration`	✗ No	✓ Sì	✗ No
`AWS::GameLift::MatchmakingRuleSet`	✗ No	✓ Sì	✗ No

AWS Global Accelerator

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::GlobalAccelerator::Accelerator`	✗ No	✓ Sì	✗ No

AWS Glue

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Glue::Crawler`	✓ Sì	✓ Sì	✗ No
`AWS::Glue::Database`	✗ No	✓ Sì	✓ Sì
`AWS::Glue::Job`	✓ Sì	✓ Sì	✗ No
`AWS::Glue::MLTransform`	✗ No	✓ Sì	✗ No
`AWS::Glue::Registry`	✗ No	✓ Sì	✗ No
`AWS::Glue::Trigger`	✓ Sì	✓ Sì	✗ No
`AWS::Glue::Workflow`	✗ No	✓ Sì	✗ No

AWS Glue DataBrew

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::DataBrew::Dataset`	✓ Sì	✓ Sì	✓ Sì
`AWS::DataBrew::Job`	✓ Sì	✓ Sì	✓ Sì
`AWS::DataBrew::Project`	✓ Sì	✓ Sì	✓ Sì
`AWS::DataBrew::Recipe`	✓ Sì	✓ Sì	✓ Sì
`AWS::DataBrew::Schedule`	✓ Sì	✓ Sì	✓ Sì

AWS Ground Station

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::GroundStation::Config`	✗ No	✓ Sì	✗ No
`AWS::GroundStation::DataflowEndpointGroup`	✗ No	✓ Sì	✗ No
`AWS::GroundStation::MissionProfile`	✗ No	✓ Sì	✗ No

Amazon GuardDuty

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::GuardDuty::Detector`	✗ No	✓ Sì	✓ Sì
`AWS::GuardDuty::Filter`	✗ No	✓ Sì	✗ No
`AWS::GuardDuty::IPSet`	✗ No	✓ Sì	✗ No
`AWS::GuardDuty::ThreatIntelSet`	✗ No	✓ Sì	✗ No

Amazon Interactive Video Service

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::IVS::Channel`	✗ No	✓ Sì	✗ No
`AWS::IVS::RecordingConfiguration`	✗ No	✓ Sì	✗ No
`AWS::IVS::StreamKey`	✗ No	✓ Sì	✗ No

AWS Identity and Access Management

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::IAM::InstanceProfile`	✓ Sì[1]	✓ Sì[2]	× No
`AWS::IAM::ManagedPolicy`	✓ Sì[1]	✓ Sì[2]	× No
`AWS::IAM::OpenIDConnectProvider`	✓ Sì[1]	✓ Sì[2]	× No
`AWS::IAM::Role`	× No	× No	✓ Sì[2]
`AWS::IAM::SAMLProvider`	✓ Sì[1]	✓ Sì[2]	× No
`AWS::IAM::ServerCertificate`	✓ Sì[1]	✓ Sì[2]	× No
`AWS::IAM::VirtualMFADevice`	✓ Sì[1]	✓ Sì[2]	× No

[1] Questa è una risorsa per un servizio globale ospitato nella regione Stati Uniti orientali (Virginia settentrionale). Per utilizzare Tag Editor per creare o modificare tag per questo tipo di risorsa, è necessario `us-east-1` includerli dall'elenco Seleziona regioni sotto Trova risorse da etichettare nella console Tag Editor.

[2] Questa è una risorsa per un servizio globale ospitato nella regione Stati Uniti orientali (Virginia settentrionale). Poiché i Resource Groups vengono gestiti separatamente per ogni regione, è necessario passare AWS Management Console a Regione AWS quello che contiene le risorse che si desidera includere nel gruppo. Per creare un gruppo di risorse che contenga una risorsa globale, devi AWS Management Console configurare US-east-1 in US East (Virginia settentrionale) utilizzando il selettore Regione nell'angolo in alto a destra di. AWS Management Console

EC2 Image Builder

Risorse	Tag Editor: etichettatura	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::ImageBuilder::Component`	✗ No	✓ Sì	✗ No
`AWS::ImageBuilder::ContainerRecipe`	✗ No	✓ Sì	✗ No
`AWS::ImageBuilder::DistributionConfiguration`	✗ No	✓ Sì	✗ No
`AWS::ImageBuilder::Image`	✗ No	✓ Sì	✗ No
`AWS::ImageBuilder::ImagePipeline`	✗ No	✓ Sì	✗ No
`AWS::ImageBuilder::ImageRecipe`	✗ No	✓ Sì	✗ No
`AWS::ImageBuilder::InfrastructureConfiguration`	✗ No	✓ Sì	✗ No

Amazon Inspector

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Inspector::AssessmentTemplate`	✗ No	✓ Sì	✓ Sì

AWS IoT

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
AWS::IoT::Authorizer	✗ No	✓ Sì	✗ No
AWS::IoT::BillingGroup	✗ No	✓ Sì	✗ No
AWS::IoT::CACertificate	✗ No	✓ Sì	✗ No
AWS::IoT::CustomMetric	✗ No	✓ Sì	✗ No
AWS::IoT::Dimension	✗ No	✓ Sì	✗ No
AWS::IoT::JobTemplate	✗ No	✓ Sì	✗ No
AWS::IoT::MitigationAction	✗ No	✓ Sì	✗ No
AWS::IoT::Policy	✗ No	✓ Sì	✗ No
AWS::IoT::RoleAlias	✗ No	✓ Sì	✗ No
AWS::IoT::ScheduledAudit	✗ No	✓ Sì	✗ No
AWS::IoT::SecurityProfile	✗ No	✓ Sì	✗ No
AWS::IoT::ThingGroup	✗ No	✓ Sì	✗ No
AWS::IoT::ThingType	✗ No	✓ Sì	✗ No
AWS::IoT::TopicRule	✗ No	✓ Sì	✓ Sì

AWS IoT Analytics

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::IoTAnalytics::Channel`	✗ No	✓ Sì	✗ No
`AWS::IoTAnalytics::Dataset`	✓ Sì	✓ Sì	✗ No
`AWS::IoTAnalytics::Datastore`	✗ No	✓ Sì	✗ No
`AWS::IoTAnalytics::Pipeline`	✗ No	✓ Sì	✗ No

AWS IoT Events

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::IoTEvents::AlarmModel`	✗ No	✓ Sì	✗ No
`AWS::IoTEvents::DetectorModel`	✓ Sì	✓ Sì	✓ Sì
`AWS::IoTEvents::Input`	✓ Sì	✓ Sì	✓ Sì

AWS IoT FleetWise

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::IoTFleetWise::Campaign`	✗ No	✓ Sì	✓ Sì
`AWS::IoTFleetWise::DecoderManifest`	✗ No	✓ Sì	✓ Sì
`AWS::IoTFleetWise::Fleet`	✗ No	✓ Sì	✓ Sì
`AWS::IoTFleetWise::ModelManifest`	✗ No	✓ Sì	✓ Sì
`AWS::IoTFleetWise::SignalCatalog`	✗ No	✓ Sì	✓ Sì
`AWS::IoTFleetWise::Vehicle`	✗ No	✓ Sì	✓ Sì

AWS IoT Greengrass

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Greengrass::ConnectorDefinition`	✓ Sì	✓ Sì	✗ No
`AWS::Greengrass::CoreDefinition`	✓ Sì	✓ Sì	✗ No
`AWS::Greengrass::DeviceDefinition`	✓ Sì	✓ Sì	✗ No
`AWS::Greengrass::FunctionDefinition`	✓ Sì	✓ Sì	✗ No

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Greengrass::Group`	✓ Sì	✓ Sì	✗ No
`AWS::Greengrass::LoggerDefinition`	✓ Sì	✓ Sì	✗ No
`AWS::Greengrass::ResourceDefinition`	✓ Sì	✓ Sì	✗ No
`AWS::Greengrass::SubscriptionDefinition`	✓ Sì	✓ Sì	✗ No

AWS IoT Greengrass Version 2

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::GreengrassV2::ComponentVersion`	✗ No	✓ Sì	✗ No

Console AWS IoT SiteWise

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::IoTSiteWise::Asset`	✗ No	✓ Sì	✗ No
`AWS::IoTSiteWise::AssetModel`	✗ No	✓ Sì	✗ No
`AWS::IoTSiteWise::Dashboard`	✗ No	✓ Sì	✗ No
`AWS::IoTSiteWise::Gateway`	✗ No	✓ Sì	✗ No
`AWS::IoTSiteWise::Portal`	✗ No	✓ Sì	✗ No
`AWS::IoTSiteWise::Project`	✗ No	✓ Sì	✗ No

AWS IoT Wireless

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::IoTWireless::Destination`	✗ No	✓ Sì	✗ No
`AWS::IoTWireless::DeviceProfile`	✗ No	✓ Sì	✗ No
`AWS::IoTWireless::FuotaTask`	✗ No	✓ Sì	✗ No
`AWS::IoTWireless::MulticastGroup`	✗ No	✓ Sì	✗ No

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
AWS::IoTWireless::NetworkAnalyzerConfiguration	✗ No	✓ Sì	✗ No
AWS::IoTWireless::ServiceProfile	✗ No	✓ Sì	✗ No
AWS::IoTWireless::TaskDefinition	✗ No	✓ Sì	✗ No
AWS::IoTWireless::WirelessDevice	✗ No	✓ Sì	✗ No
AWS::IoTWireless::WirelessGateway	✗ No	✓ Sì	✗ No

AWS Key Management Service

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
AWS::KMS::Alias	✗ No	✗ No	✓ Sì
AWS::KMS::Key	✓ Sì	✓ Sì	✓ Sì

Amazon Keyspaces (per Apache Cassandra)

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Cassandra::Keyspace`	✗ No	✓ Sì	✓ Sì
`AWS::Cassandra::Table`	✗ No	✓ Sì	✗ No

Amazon Kinesis

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Kinesis::Stream`	✓ Sì	✓ Sì	✓ Sì

Servizio gestito da Amazon per Apache Flink

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::KinesisAnalytics::Application`	✓ Sì	✓ Sì	✓ Sì

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::KinesisAnalyticsV2::Application`	✗ No	✗ No	✓ Sì

Amazon Data Firehose

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::KinesisFirehose::DeliveryStream`	✗ No	✓ Sì	✓ Sì

AWS Lambda

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Lambda::Alias`	✗ No	✗ No	✓ Sì
`AWS::Lambda::EventSourceMapping`	✗ No	✗ No	✓ Sì
`AWS::Lambda::Function`	✓ Sì	✓ Sì	✓ Sì

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Lambda::LayerVersion`	✗ No	✗ No	✓ Sì
`AWS::Lambda::Version`	✗ No	✗ No	✓ Sì

Amazon Lightsail

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Lightsail::Bucket`	✗ No	✓ Sì	✗ No
`AWS::Lightsail::Certificate`	✗ No	✓ Sì	✗ No
`AWS::Lightsail::Container`	✗ No	✓ Sì	✗ No
`AWS::Lightsail::Disk`	✗ No	✓ Sì	✗ No
`AWS::Lightsail::Distribution`	✗ No	✓ Sì	✗ No
`AWS::Lightsail::Instance`	✗ No	✓ Sì	✗ No
`AWS::Lightsail::StaticIp`	✗ No	✓ Sì	✗ No

Amazon MQ

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::AmazonMQ::Broker`	✓ Sì	✓ Sì	✗ No
`AWS::AmazonMQ::Configuration`	✓ Sì	✓ Sì	✗ No

Amazon Macie

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Macie::ClassificationJob`	✓ Sì	✓ Sì	✗ No
`AWS::Macie::CustomDataIdentifier`	✓ Sì	✓ Sì	✓ Sì
`AWS::Macie::FindingsFilter`	✓ Sì	✓ Sì	✓ Sì
`AWS::Macie::Member`	✓ Sì	✓ Sì	✗ No

Blockchain gestita da Amazon

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::ManagedBlockchain::Accessor`	✗ No	✓ Sì	✗ No

Amazon Managed Streaming per Apache Kafka

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Kafka::Cluster`	✓ Sì	✓ Sì	✗ No

AWS Elemental MediaConnect

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::MediaConnect::Flow`	✗ No	✓ Sì	✗ No
`AWS::MediaConnect::FlowEntitlement`	✗ No	✓ Sì	✗ No

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::MediaConnect::FlowOutput`	✗ No	✓ Sì	✗ No
`AWS::MediaConnect::FlowSource`	✗ No	✓ Sì	✗ No

AWS Elemental MediaPackage

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::MediaPackage::Channel`	✗ No	✓ Sì	✗ No
`AWS::MediaPackage::PackagingConfiguration`	✗ No	✓ Sì	✗ No
`AWS::MediaPackage::PackagingGroup`	✗ No	✓ Sì	✗ No

AWS Network Manager

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::NetworkManager::CoreNetwork`	✗ No	✓ Sì	✗ No
`AWS::NetworkManager::Device`	✗ No	✓ Sì	✗ No
`AWS::NetworkManager::GlobalNetwork`	✗ No	✓ Sì	✗ No
`AWS::NetworkManager::Link`	✗ No	✓ Sì	✗ No
`AWS::NetworkManager::Site`	✗ No	✓ Sì	✗ No
`AWS::NetworkManager::VpcAttachment`	✗ No	✓ Sì	✗ No

OpenSearch Servizio Amazon OpenSearch

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::OpenSearchService::Domain`	✓ Sì	✓ Sì	✓ Sì

AWS OpsWorks

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::OpsWorks::Instance`	✗ No	✓ Sì	✓ Sì
`AWS::OpsWorks::Layer`	✗ No	✓ Sì	✓ Sì
`AWS::OpsWorks::Stack`	✗ No	✓ Sì	✓ Sì

AWS Organizations

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Organizations::Account`	✓ Sì	✓ Sì	✗ No
`AWS::Organizations::OrganizationalUnit`	✗ No	✓ Sì	✗ No
`AWS::Organizations::Policy`	✗ No	✓ Sì	✗ No
`AWS::Organizations::Root`	✓ Sì	✓ Sì	✗ No

Amazon Pinpoint

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Pinpoint::App`	✗ No	✓ Sì	✓ Sì
`AWS::Pinpoint::EmailTemplate`	✗ No	✓ Sì	✓ Sì
`AWS::Pinpoint::PushTemplate`	✗ No	✓ Sì	✓ Sì
`AWS::Pinpoint::SmsTemplate`	✗ No	✓ Sì	✓ Sì
`AWS::Pinpoint::VoiceTemplate`	✗ No	✓ Sì	✗ No

API SMS e Voce di Amazon Pinpoint

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::PinpointSMSVoiceV2::Pool`	✗ No	✓ Sì	✗ No

Database Amazon Quantum Ledger (Amazon QLDB)

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::QLDB::Ledger`	✓ Sì	✓ Sì	✓ Sì
`AWS::QLDB::Stream`	× No	✓ Sì	✓ Sì

Amazon Redshift

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Redshift::Cluster`	✓ Sì	✓ Sì	✓ Sì
`AWS::Redshift::ClusterParameterGroup`	✓ Sì	✓ Sì	✓ Sì
`AWS::Redshift::ClusterSecurityGroup`	× No	✓ Sì	✓ Sì
`AWS::Redshift::ClusterSubnetGroup`	✓ Sì	✓ Sì	✓ Sì
`AWS::Redshift::DBGroup`	× No	✓ Sì	× No
`AWS::Redshift::DBName`	× No	✓ Sì	× No
`AWS::Redshift::DBUser`	× No	✓ Sì	× No
`AWS::Redshift::EventSubscription`	× No	✓ Sì	× No

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
AWS::Redshift::HSMClientCertificate	✓ Sì	✓ Sì	✗ No
AWS::Redshift::HSMConfiguration	✗ No	✓ Sì	✗ No
AWS::Redshift::Namespace	✗ No	✓ Sì	✗ No
AWS::Redshift::Snapshot	✗ No	✓ Sì	✗ No
AWS::Redshift::SnapshotCopyGrant	✗ No	✓ Sì	✗ No
AWS::Redshift::SnapshotSchedule	✗ No	✓ Sì	✗ No
AWS::Redshift::UsageLimit	✗ No	✓ Sì	✗ No

Amazon Relational Database Service (Amazon RDS)

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
AWS::RDS::CustomDBEngineVersion	✗ No	✓ Sì	✗ No
AWS::RDS::DBCluster	✓ Sì	✓ Sì	✓ Sì
AWS::RDS::DBClusterEndpoint	✗ No	✓ Sì	✗ No
AWS::RDS::DBClusterParameterGroup	✓ Sì	✓ Sì	✓ Sì

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
AWS::RDS::DBClusterSnapshot	✓ Sì	✓ Sì	✗ No
AWS::RDS::DBInstance	✓ Sì	✓ Sì	✓ Sì
AWS::RDS::DBParameterGroup	✓ Sì	✓ Sì	✓ Sì
AWS::RDS::DBProxy	✗ No	✓ Sì	✗ No
AWS::RDS::DBProxyEndpoint	✗ No	✓ Sì	✗ No
AWS::RDS::DBProxyTargetGroup	✗ No	✓ Sì	✗ No
AWS::RDS::DBSecurityGroup	✓ Sì	✓ Sì	✓ Sì
AWS::RDS::DBSnapshot	✓ Sì	✓ Sì	✗ No
AWS::RDS::DBSubnetGroup	✓ Sì	✓ Sì	✓ Sì
AWS::RDS::Deployment	✗ No	✓ Sì	✗ No
AWS::RDS::EventSubscription	✓ Sì	✓ Sì	✗ No
AWS::RDS::OptionGroup	✓ Sì	✓ Sì	✗ No
AWS::RDS::ReservedDBInstance	✓ Sì	✓ Sì	✗ No

AWS Resource Access Manager

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::RAM::ResourceShare`	✓ Sì	✓ Sì	✗ No

AWS Resource Groups

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::ResourceGroups::Group`	✓ Sì	✓ Sì	✓ Sì

AWS Robomaker

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::RoboMaker::DeploymentJob`	✗ No	✓ Sì	✗ No
`AWS::RoboMaker::Fleet`	✗ No	✓ Sì	✗ No

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::RoboMaker::Robot`	✗ No	✓ Sì	✗ No
`AWS::RoboMaker::RobotApplication`	✓ Sì	✓ Sì	✗ No
`AWS::RoboMaker::SimulationApplication`	✓ Sì	✓ Sì	✗ No
`AWS::RoboMaker::SimulationJob`	✓ Sì	✓ Sì	✗ No

Amazon Route 53

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Route53::Domain`	✓ Sì[1]	✓ Sì[2]	✗ No
`AWS::Route53::HealthCheck`	✓ Sì[1]	✓ Sì[2]	✓ Sì[2]
`AWS::Route53::HostedZone`	✓ Sì[1]	✓ Sì[2]	✓ Sì[2]

[1] Questa è una risorsa per un servizio globale ospitato nella regione Stati Uniti orientali (Virginia settentrionale). Per utilizzare Tag Editor per creare o modificare tag per questo tipo di risorsa, è necessario `us-east-1` includerli dall'elenco Seleziona regioni sotto Trova risorse da etichettare nella console Tag Editor.

² Questa è una risorsa per un servizio globale ospitato nella regione Stati Uniti orientali (Virginia settentrionale). Poiché i Resource Groups vengono gestiti separatamente per ogni regione, è necessario passare AWS Management Console a Regione AWS quello che contiene le risorse che si desidera includere nel gruppo. Per creare un gruppo di risorse che contenga una risorsa globale, devi AWS Management Console configurare US-east-1 in US East (Virginia settentrionale) utilizzando il selettore Regione nell'angolo in alto a destra di. AWS Management Console

Amazon Route 53 Resolver

Risorse	Tag Editor: etichettatura	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Route53Resolver::FirewallDomainList`	✗ No	✓ Sì²	✗ No
`AWS::Route53Resolver::FirewallRuleGroup`	✗ No	✓ Sì²	✗ No
`AWS::Route53Resolver::FirewallRuleGroupAssociation`	✗ No	✓ Sì²	✗ No
`AWS::Route53Resolver::ResolverEndpoint`	✓ Sì¹	✓ Sì²	✗ No
`AWS::Route53Resolver::ResolverQueryLoggingConfig`	✗ No	✓ Sì²	✗ No
`AWS::Route53Resolver::ResolverRule`	✓ Sì¹	✓ Sì²	✗ No

¹ Questa è una risorsa per un servizio globale ospitato nella regione Stati Uniti orientali (Virginia settentrionale). Per utilizzare Tag Editor per creare o modificare tag per questo tipo di risorsa, è necessario `us-east-1` includerli dall'elenco Seleziona regioni sotto Trova risorse da etichettare nella console Tag Editor.

² Questa è una risorsa per un servizio globale ospitato nella regione Stati Uniti orientali (Virginia settentrionale). Poiché i Resource Groups vengono gestiti separatamente per ogni regione, è necessario passare AWS Management Console a Regione AWS quello che contiene le risorse che si desidera includere nel gruppo. Per creare un gruppo di risorse che contenga una risorsa globale, devi AWS Management Console configurare US-east-1 in US East (Virginia settentrionale) utilizzando il selettore Regione nell'angolo in alto a destra di. AWS Management Console

Amazon S3 Glacier

Risorse	Tag Editor: etichettatura	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Glacier::Vault`	✓ Sì	✓ Sì	✗ No

Amazon SageMaker

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::SageMaker::AppImageConfig`	✗ No	✓ Sì	✗ No
`AWS::SageMaker::CodeRepository`	✗ No	✓ Sì	✗ No
`AWS::SageMaker::Endpoint`	✗ No	✓ Sì	✓ Sì
`AWS::SageMaker::EndpointConfig`	✗ No	✓ Sì	✓ Sì

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
AWS::SageMaker::HyperParameterTuningJob	✗ No	✓ Sì	✗ No
AWS::SageMaker::Image	✗ No	✓ Sì	✗ No
AWS::SageMaker::LabelingJob	✗ No	✓ Sì	✗ No
AWS::SageMaker::Model	✗ No	✓ Sì	✓ Sì
AWS::SageMaker::ModelPackageGroup	✗ No	✓ Sì	✓ Sì
AWS::SageMaker::NotebookInstance	✓ Sì	✓ Sì	✓ Sì
AWS::SageMaker::Pipeline	✗ No	✓ Sì	✗ No
AWS::SageMaker::Project	✗ No	✓ Sì	✓ Sì
AWS::SageMaker::TrainingJob	✗ No	✓ Sì	✗ No
AWS::SageMaker::TransformJob	✗ No	✓ Sì	✗ No
AWS::SageMaker::Workteam	✗ No	✓ Sì	✗ No

AWS Secrets Manager

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::SecretsManager::Secret`	✓ Sì	✓ Sì	✓ Sì

AWS Service Catalog

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::ServiceCatalog::CloudFormationProduct`	✗ No	✓ Sì	✓ Sì
`AWS::ServiceCatalog::Portfolio`	✗ No	✓ Sì	✓ Sì

AWS Service Catalog AppRegistry

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::ServiceCatalogAppRegistry::Application`	✗ No	✓ Sì	✗ No
`AWS::ServiceCatalogAppRegistry::AttributeGroup`	✗ No	✓ Sì	✗ No

Service Quotas (Quote di Servizio)

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::ServiceQuotas::Quota`	✗ No	✓ Sì	✗ No

Amazon Simple Email Service

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::SES::ConfigurationSet`	✓ Sì	✓ Sì	✓ Sì
`AWS::SES::ContactList`	✓ Sì	✓ Sì	✓ Sì
`AWS::SES::DedicatedIpPool`	✓ Sì	✓ Sì	× No
`AWS::SES::Identity`	✓ Sì	✓ Sì	× No

Amazon Simple Notification Service

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::SNS::Topic`	✓ Sì	✓ Sì	✓ Sì

Amazon Simple Queue Service

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::SQS::Queue`	✓ Sì	✓ Sì	✓ Sì

Amazon Simple Storage Service (Amazon S3)

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::S3::Bucket`	✓ Sì	✓ Sì	✓ Sì
`AWS::S3::Job`	X No	✓ Sì	X No
`AWS::S3::StorageLens`	X No	✓ Sì	X No

AWS Step Functions

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::StepFunctions::Activity`	✓ Sì	✓ Sì	✓ Sì
`AWS::StepFunctions::StateMachine`	✓ Sì	✓ Sì	✓ Sì

Storage Gateway

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::StorageGateway::Gateway`	✓ Sì	✓ Sì	X No
`AWS::StorageGateway::Volume`	X No	✓ Sì	X No

AWS Systems Manager

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
AWS::SSM::Association	✗ No	✓ Sì	✗ No
AWS::SSM::AutomationExecution	✗ No	✓ Sì	✗ No
AWS::SSM::Document	✗ No	✓ Sì	✓ Sì
AWS::SSM::MaintenanceWindow	✗ No	✓ Sì	✗ No
AWS::SSM::ManagedInstance	✗ No	✓ Sì	✗ No
AWS::SSM::OpsItem	✗ No	✓ Sì	✗ No
AWS::SSM::OpsMetadata	✗ No	✓ Sì	✗ No
AWS::SSM::Parameter	✓ Sì	✓ Sì	✓ Sì
AWS::SSM::PatchBaseline	✗ No	✓ Sì	✓ Sì

AWS Systems Manager per SAP

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
AWS::SystemsManagerSAP::Application	✗ No	✓ Sì	✓ Sì

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::SystemsManagerSAP::Database`	✗ No	✓ Sì	✗ No

Amazon Timestream

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Timestream::ScheduledQuery`	✗ No	✓ Sì	✓ Sì

AWS Transfer Family

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Transfer::Certificate`	✗ No	✓ Sì	✗ No
`AWS::Transfer::Connector`	✗ No	✓ Sì	✗ No
`AWS::Transfer::Profile`	✗ No	✓ Sì	✗ No

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::Transfer::Workflow`	✗ No	✓ Sì	✗ No

AWS WAF

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::WAF::Rule`	✗ No	✓ Sì	✗ No
`AWS::WAF::WebACL`	✗ No	✓ Sì	✗ No

Amazon WorkSpaces

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::WorkSpaces::Workspace`	✓ Sì	✓ Sì	✓ Sì

AWS X-Ray

Risorse	Etichettatura con Tag Editor	Gruppi basati su tag	AWS CloudFormation Gruppi basati su stack
`AWS::XRay::Group`	✗ No	✓ Sì	✗ No
`AWS::XRay::SamplingRule`	✗ No	✓ Sì	✗ No

Tipi di risorse obsoleti

I seguenti tipi di risorse non sono più supportati per la funzionalità specificata.

Servizio	Tipo di risorsa	Modifica del supporto	Data
AWS RoboMaker	`AWS::RoboMaker::Robot`	Non più supportato da Tag Editor.	2 maggio 2022
AWS RoboMaker	`AWS::RoboMaker::Fleet`	Non più supportato da Tag Editor.	2 maggio 2022
AWS RoboMaker	`AWS::RoboMaker::DeploymentJob`	Non più supportato da Tag Editor.	2 maggio 2022

Creazione di gruppi di risorse con AWS CloudFormation

AWS Resource Groups è integrato con AWS CloudFormation, un servizio che consente di modellare e configurare le AWS risorse in modo da dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. È possibile creare un modello che descrive tutte le AWS risorse desiderate (ad esempio i gruppi di risorse) e fornisce e AWS CloudFormation configura tali risorse al posto dell'utente.

Quando lo utilizzi AWS CloudFormation, puoi riutilizzare il modello per configurare i gruppi di risorse in modo coerente e ripetuto. Descrivi i tuoi gruppi di risorse una sola volta, quindi fornisci gli stessi gruppi di risorse più e più volte in più Account AWS regioni.

Resource Groups e AWS CloudFormation modelli

Per fornire e configurare le risorse per Resource Groups e i servizi correlati, è necessario conoscere AWS CloudFormation i modelli. I modelli sono file di testo formattati in JSON oYAML. Questi modelli descrivono le risorse che desideri inserire nei tuoi AWS CloudFormation stack. Se non conosci JSON oYAML, puoi usare AWS CloudFormation Designer per iniziare a usare i AWS CloudFormation modelli. Per ulteriori informazioni, consulta Cos'è AWS CloudFormation Designer? nella Guida AWS CloudFormation per l'utente.

Resource Groups supporta la creazione di gruppi di risorse in AWS CloudFormation. Per ulteriori informazioni, inclusi esempi JSON e YAML modelli per i gruppi di risorse, consulta il riferimento ai tipi di AWS Resource Groups risorse nella Guida per l'AWS CloudFormation utente.

Scopri di più su AWS CloudFormation

Per ulteriori informazioni AWS CloudFormation, consulta le seguenti risorse:

- AWS CloudFormation
- AWS CloudFormation Guida per l'utente
- AWS CloudFormation APIRiferimento
- AWS CloudFormation Guida per l'utente dell'interfaccia a riga di comando

Sicurezza in AWS Resource Groups

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, puoi trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza.

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

- La sicurezza del cloud:AWS è responsabile della protezione dell'infrastruttura che esegue i servizi AWS nel AWS Cloud. AWS fornisce, inoltre, servizi utilizzabili in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformità AWS. Per ulteriori informazioni sui programmi di conformità che si applicano a AWS Resource Groups, consulta Servizi coperti dal programma di conformitàAWS.
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che viene utilizzato. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e leggi e normative applicabili.

Questa documentazione aiuta a comprendere come applicare il modello di responsabilità condivisa quando si usa Resource Groups. I seguenti argomenti illustrano come configurare i Resource Groups per soddisfare gli obiettivi di sicurezza e conformità. È inoltre illustrato come utilizzare gli altriAWSservizi che possono aiutarti a monitorare e proteggere le Resource Groups di risorse.

Argomenti

Protezione dei dati in AWS Resource Groups

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

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

- Usa l'autenticazione a più fattori (MFA) con ogni account.
- UsaSSL/TLSper comunicare con AWS risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per l'acquisizione AWS attività, vedi Lavorare con i CloudTrail sentieri in AWS CloudTrail Guida per l'utente.
- Utilizzo AWS soluzioni di 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 sono necessari FIPS 140-3 moduli crittografici convalidati per l'accesso AWS tramite un'interfaccia a riga di comando o unAPI, utilizza un endpoint. FIPS Per ulteriori informazioni sugli FIPS endpoint disponibili, vedere Federal Information Processing Standard (FIPS) 140-3.

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

Crittografia dei dati

Rispetto ad altri AWS servizi, AWS Resource Groups ha una superficie di attacco minima, in quanto non consente di modificare, aggiungere o eliminare AWS risorse ad eccezione dei gruppi. Resource Groups raccoglie dall'utente le seguenti informazioni specifiche sul servizio.

- Nomi di gruppo (non crittografati, non privati)
- Descrizioni dei gruppi (non crittografate, ma private)
- Risorse dei membri in gruppi (queste sono archiviate in registri, che non sono crittografati)

Crittografia a riposo

Non esistono altri modi per isolare il traffico di servizio o di rete specifico per Resource Groups. Se applicabile, utilizzare AWS-isolamento specifico. È possibile utilizzare Resource Groups API e la console per VPC massimizzare la privacy e la sicurezza dell'infrastruttura.

Crittografia in transito

AWS Resource Groups i dati vengono crittografati in transito verso il database interno del servizio per il backup. Questa opzione non è configurabile dall'utente.

Gestione delle chiavi

AWS Resource Groups non è attualmente integrato con AWS Key Management Service e non supporta AWS KMS keys.

Riservatezza del traffico Internet

AWS Resource Groups usi HTTPS per tutte le trasmissioni tra utenti di Resource Groups e AWS. Resource Groups utilizza transport layer security (TLS) 1.2, ma supporta anche TLS 1.0 e 1.1.

Gestione delle identità e degli accessi per AWS Resource Groups

AWS Identity and Access Management (IAM) è un Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso a AWS risorse. IAMgli amministratori controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Resource Groups. IAMè un Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Come si usa AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Resource Groups.

Utente del servizio: se utilizzi il servizio Resource Groups per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Resource Groups per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non è possibile accedere a una funzionalità in Resource Groups, vedereRisoluzione dei problemi di AWS Resource Groups identità e accesso.

Amministratore del servizio: se sei responsabile delle risorse Resource Groups presso la tua azienda, probabilmente hai pieno accesso a Resource Groups. È tuo compito determinare a quali funzionalità e risorse di Resource Groups devono accedere gli utenti del servizio. È quindi necessario inviare richieste all'IAMamministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base diIAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM Resource Groups, consultaCome funziona Resource Groups con IAM.

IAMamministratore: se sei un IAM amministratore, potresti voler saperne di più su come scrivere politiche per gestire l'accesso ai Resource Groups. Per visualizzare esempi di policy basate sull'identità di Resource Groups in IAM cui è possibile utilizzare, vedere. Esempi di policy di AWS Resource Groups basate su identità

Autenticazione con identità

L'autenticazione è la modalità di accesso a AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l'accesso a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un IAM ruolo.

Puoi accedere a AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAMIdentity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali Google o Facebook sono esempi di identità federate. Quando accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente che sei, puoi accedere a AWS Management Console o il AWS portale di accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Accedi ad AWS Guida per l'utente.

Se accedi AWS programmaticamente, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le richieste utilizzando le credenziali dell'utente. Se non usi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, vedi Firma AWS APIrichieste nella Guida IAM per l'utente.

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

Account AWS utente root

Quando crei un Account AWS, inizi con un'unica identità di accesso con accesso completo a tutti Servizi AWS e le risorse presenti nell'account. Questa identità è chiamata Account AWS utente root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per l'elenco completo delle attività che richiedono l'accesso come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'IAMutente.

IAM users and groups

Un IAMutente è un'identità all'interno di Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente. IAM

Un IAMgruppo è un'identità che specifica un insieme di utenti. IAM Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per IAM amministrare le risorse.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un IAM utente (anziché un ruolo) nella Guida per l'IAMutente.

IAMruoli

Un IAMruolo è un'identità all'interno del tuo Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. È possibile assumere temporaneamente un IAM ruolo nel AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un AWS CLI oppure AWS APIoperazione o utilizzando un comando personalizzatoURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere Utilizzo IAM dei ruoli nella Guida per l'IAMutente.

IAMi ruoli con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per informazioni sui ruoli per la federazione, vedere Creazione di un ruolo per un provider di identità di terze parti nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla

il set di autorizzazioni a un ruolo in. IAM Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nel AWS IAM Identity Center Guida per l'utente.

- Autorizzazioni IAM utente temporanee: un IAM utente o un ruolo può assumere un IAM ruolo per assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso su più account: puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse su più account IAM nella Guida per l'utente. IAM
- Accesso a più servizi: alcuni Servizi AWS usa le funzionalità in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un IAM utente o un ruolo per eseguire azioni in AWS, sei considerato un preside. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama un Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi a valle. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse da completare. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo di eseguire un'azione per conto dell'utente. I ruoli collegati ai servizi vengono visualizzati nel tuo Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2istanza e in fase di creazione AWS CLI oppure AWS APIrichieste. Ciò è preferibile alla memorizzazione delle chiavi di accesso all'interno

dell'EC2istanza. Per assegnare un AWS assegnate un ruolo a un'EC2istanza e renderlo disponibile a tutte le relative applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Usare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAMutente.

Per sapere se utilizzare IAM ruoli o IAM utenti, consulta Quando creare un IAM ruolo (anziché un utente) nella Guida per l'IAMutente.

Gestione dell'accesso con policy

Puoi controllare l'accesso in AWS creando politiche e allegandole a AWS identità o risorse. Una politica è un oggetto in AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata in AWS come JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere Panoramica delle JSON politiche nella Guida per l'IAMutente.

Gli amministratori possono utilizzare AWS JSONpolitiche per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti il permesso di eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

IAMle politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, il AWS CLI, o il AWS API.

Policy basate su identità

I criteri basati sull'identità sono documenti relativi ai criteri di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono AWS politiche gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una politica gestita o una politica in linea, consulta Scelta tra politiche gestite e politiche in linea nella Guida per l'IAMutente.

Policy basate su risorse

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

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi usare AWS politiche gestite da IAM una politica basata sulle risorse.

Liste di controllo degli accessi () ACLs

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

Amazon S3, AWS WAF e Amazon VPC sono esempi di servizi che supportanoACLs. Per ulteriori informazioniACLs, consulta la panoramica di Access control list (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (utente o ruolo). IAM IAM È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo

`Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità nella Guida per l'utente. IAM IAM

- Politiche di controllo del servizio (SCPs): SCPs sono JSON politiche che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in AWS Organizations. AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà della tua azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. I SCP limiti e le autorizzazioni per le entità presenti negli account dei membri, inclusi tutti Utente root dell'account AWS. Per ulteriori informazioni su Organizations andSCPs, vedere Service control policies nel AWS Organizations Guida per l'utente.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta le politiche di sessione nella Guida IAM per l'utente.

Più tipi di policy

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

Come funziona Resource Groups con IAM

Prima di utilizzare IAM per gestire l'accesso a Resource Groups, è necessario comprendere quali IAM funzionalità sono disponibili per l'uso con Resource Groups. Per una panoramica generale del funzionamento dei Resource Groups e di altri AWS serviziIAM, consulta AWS Services That Work with IAM nella IAMUser Guide.

Argomenti

- Politiche basate sull'identità di Resource Groups
- Policy basate su risorse
- Autorizzazione basata sui tag Resource Groups

- IAMRuoli Resource Groups

Politiche basate sull'identità di Resource Groups

Con le politiche IAM basate sull'identità, è possibile specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. Resource Groups supporta azioni, risorse e chiavi di condizione specifiche. Per informazioni su tutti gli elementi utilizzati in una JSON policy, consulta IAMJSONPolicy Elements Reference nella Guida per l'IAMutente.

Azioni

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'`Action`elemento di una JSON policy descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell' AWS APIoperazione associata. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni che non hanno un'operazione corrispondente. API Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

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

Le azioni politiche in Resource Groups utilizzano il seguente prefisso prima dell'azione:`resource-groups:`. Le azioni di Tag Editor vengono eseguite interamente nella console, ma hanno il prefisso `resource-explorer` nelle voci di registro.

Ad esempio, per concedere a qualcuno l'autorizzazione a creare un gruppo Resource Groups con l'`CreateGroup`APIoperazione Resource Groups, includi l'`resource-groups:CreateGroup`azione nella sua politica. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. Resource Groups definisce il proprio set di azioni che descrivono le attività che è possibile eseguire con questo servizio.

Per specificare più azioni Resource Groups e Tag Editor in un'unica istruzione, separale con virgole come segue:

```
"Action": [
      "resource-groups:action1",
      "resource-groups:action2",
      "resource-explorer:action3"
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `List`, includi la seguente azione:

```
"Action": "resource-groups:List*"
```

Per visualizzare un elenco delle azioni di Resource Groups, consulta Actions, Resources and Condition Keys AWS Resource Groups nella Guida per l'IAMutente.

Risorse

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Resource` JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il relativo Amazon Resource Name (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

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

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

L'unica risorsa Resource Groups è un gruppo. La risorsa di gruppo ha ARN il seguente formato:

```
arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}
```

Per ulteriori informazioni sul formato diARNs, consulta Amazon Resource Names (ARNs) e AWS Service Namespaces.

Ad esempio, per specificare il gruppo di `my-test-group` risorse nella tua dichiarazione, usa quanto segue: ARN

```
"Resource": "arn:aws:resource-groups:us-east-1:123456789012:group/my-test-group"
```

Per specificare tutti i gruppi che appartengono a un account specifico, usa il carattere jolly (*):

```
"Resource": "arn:aws:resource-groups:us-east-1:123456789012:group/*"
```

Alcune azioni di Resource Groups, come quelle per la creazione di risorse, non possono essere eseguite su una risorsa specifica. In questi casi, è necessario utilizzare il carattere jolly (*).

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

Alcune API azioni di Resource Groups possono coinvolgere più risorse. Ad esempio, `DeleteGroup` elimina i gruppi, quindi un principale chiamante deve disporre delle autorizzazioni per eliminare un gruppo specifico o tutti i gruppi. Per specificare più risorse in un'unica istruzione, separale ARNs con virgole.

```
"Resource": [
  "resource1",
  "resource2"
]
```

Per visualizzare un elenco dei tipi di risorse Resource Groups e i relativi ARNs tipi ARN di risorse e scoprire con quali azioni è possibile specificare ciascuna risorsa, vedere Actions, Resources, and Condition Keys AWS Resource Groups nella Guida per l'IAMutente.

Chiavi di condizione

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

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

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

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile concedere a un IAM utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il

suo nome IAM utente. Per ulteriori informazioni, consulta gli elementi IAM della politica: variabili e tag nella Guida IAM per l'utente.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'IAMutente.

Resource Groups definisce il proprio set di chiavi di condizione e supporta anche l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione AWS globali, consulta AWS Global Condition Context Keys nella Guida IAM per l'utente.

Per visualizzare un elenco delle chiavi di condizione di Resource Groups e scoprire con quali azioni e risorse è possibile utilizzare una chiave di condizione, consulta Actions, Resources and Condition Keys AWS Resource Groups nella Guida per l'IAMutente.

Esempi

Per visualizzare esempi di politiche basate sull'identità di Resource Groups, vedere. Esempi di policy di AWS Resource Groups basate su identità

Policy basate su risorse

Resource Groups non supporta le politiche basate sulle risorse.

Autorizzazione basata sui tag Resource Groups

È possibile allegare tag ai gruppi in Resource Groups o passare i tag in una richiesta a Resource Groups. Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* o `aws:TagKeys`. È possibile applicare tag a un gruppo durante la creazione o l'aggiornamento del gruppo. Per ulteriori informazioni sull'assegnazione di tag a un gruppo in Resource Groups, consulta Creazione di gruppi basati su query in AWS Resource Groups e Aggiornamento dei gruppi in AWS Resource Groups in questa guida.

Per visualizzare una policy basata sulle identità di esempio per limitare l'accesso a una risorsa basata su tag su tale risorsa, consulta Visualizzazione di gruppi in tag.

IAMRuoli Resource Groups

Un IAMruolo è un'entità all'interno del tuo AWS account che dispone di autorizzazioni specifiche. Resource Groups non dispone né utilizza ruoli di servizio.

Utilizzo di credenziali temporanee con Resource Groups

In Resource Groups, puoi utilizzare credenziali temporanee per accedere con la federazione, assumere un IAM ruolo o assumere un ruolo tra account. È possibile ottenere credenziali di sicurezza temporanee chiamando AWS STS API operazioni come o. AssumeRoleGetFederationToken

Ruoli collegati ai servizi

I ruoli collegati ai AWS servizi consentono ai servizi di accedere alle risorse di altri servizi per completare un'azione per conto dell'utente.

Resource Groups non dispone né utilizza ruoli collegati ai servizi.

Ruoli dei servizi

Questa caratteristica consente a un servizio di assumere un ruolo di servizio per conto dell'utente.

Resource Groups non dispone né utilizza ruoli di servizio.

AWS Policy gestite da per AWS Resource Groups

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

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

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

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

AWS-politiche gestite per i gruppi di risorse

- ResourceGroupsServiceRolePolicy

AWSPolicy gestita: ResourceGroupsServiceRolePolicy

Non puoi allegare`ResourceGroupsServiceRolePolicy`a qualsiasi entità IAM tu stesso. Questa politica può essere associata solo a un ruolo collegato al servizio che consente ai gruppi di risorse di eseguire azioni per conto dell'utente. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per i Resource Groups.

Questa politica concede le autorizzazioni necessarie ai gruppi di risorse per recuperare informazioni sulle risorse nei tuoi gruppi di risorse e in qualsiasi altroAWS CloudFormationpile a cui appartengono quelle risorse. Ciò consente ai gruppi di risorse di generareCloudWatchEventi per la funzionalità degli eventi del ciclo di vita del gruppo.

Per vedere l'ultima versione di questoAWSpolicy gestita, vedere`ResourceGroupsServiceRolePolicy`nella console IAM.

AWSpolitica gestita: ResourceGroupsandTagEditorFullAccess

Quando si associa una politica a un'entità principale, si assegnano all'entità le autorizzazioni definite nella politica.AWSle policy gestite semplificano l'assegnazione delle autorizzazioni appropriate a utenti, gruppi e ruoli rispetto a quando doveste scrivere le policy da soli.

Questa politica concede le autorizzazioni necessarie per l'accesso completo alle funzionalità Resource Groups e Tag Editor.

Per vedere l'ultima versione di questoAWSpolicy gestita, vedere`ResourceGroupsandTagEditorFullAccess`nella console IAM.

Per ulteriori informazioni su questa politica, vedere ResourceGroupsandTagEditorFullAccessnelAWSGuida di riferimento alle politiche gestite.

AWSpolitica gestita: ResourceGroupsandTagEditorReadOnlyAccesso

Quando si associa una politica a un'entità principale, si assegnano all'entità le autorizzazioni definite nella politica.AWSle policy gestite semplificano l'assegnazione delle autorizzazioni appropriate a utenti, gruppi e ruoli rispetto a quando doveste scrivere le policy da soli.

Questa politica concede le autorizzazioni necessarie per l'accesso in sola lettura alle funzionalità Resource Groups e Tag Editor.

Per vedere l'ultima versione di questoAWSpolicy gestita, vedere`ResourceGroupsandTagEditorReadOnlyAccess`nella console IAM.

Per ulteriori informazioni su questa politica, vedere ResourceGroupsandTagEditorReadOnlyAccessonelAWSGuida di riferimento alle politiche gestite.

Aggiornamenti di Resource Groups aAWSpolitiche gestite

Visualizza i dettagli sugli aggiornamenti diAWSpolitiche gestite per i gruppi di risorse 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 sulGruppi di risorse Cronologia dei documentipagina.

Modifica	Descrizione	Data
Aggiornamento della politica —ResourceGroupsandTagEditorFullAccess	Resource Groups ha aggiornato una politica per includere di ulterioriAWS CloudFormationautorizzazioni.	10 agosto 2023
Aggiornamento della politica —ResourceGroupsandTagEditorReadOnlyAccess	Resource Groups ha aggiornato una politica per includere di ulterioriAWS CloudFormationautorizzazioni.	10 agosto 2023
Nuova politica —ResourceGroupsServiceRolePolicy	Resource Groups ha aggiunto una nuova politica per supportare il suo ruolo legato ai servizi.	17 novembre 2022
I gruppi di risorse hanno iniziato a tenere traccia delle modifiche	Resource Groups ha iniziato a tenere traccia delle modifiche relative aAWSpolitiche gestite.	17 novembre 2022

Utilizzo di ruoli collegati ai servizi per i Resource Groups

AWS Resource Groups utilizza ruoli collegati al servizio AWS Identity and Access Management (IAM). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente ai gruppi di risorse. I ruoli collegati ai servizi sono predefiniti dai Resource Groups e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri per tuoServizi AWS conto.

Un ruolo collegato al servizio semplifica la configurazione dei Resource Groups perché ti permette di evitare l'aggiunta manuale delle autorizzazioni necessarie. Resource Groups definisce le autorizzazioni dei relativi ruoli associati ai servizi e su ciascuno di essi, in modo da garantire che solo il servizio Resource Groups potrà assumere i propri ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consultare Servizi AWS che funzionano con IAM e cercare i servizi che riportano Yes (Sì) nella colonna Service-linked roles (Ruoli collegati ai servizi). Scegli Yes (Sì) in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni del ruolo collegato ai servizi per i Resource Groups

Resource Groups utilizza il seguente ruolo collegato ai servizi per supportare gli eventi del ciclo di vita del gruppo. Scegli il link sul nome del ruolo per visualizzare il ruolo nella console IAM dopo averlo creato.

- `AWSServiceRoleForResourceGroups`

Resource Groups utilizza le autorizzazioni di questo ruolo per interrogare iServizi AWS proprietari delle risorse per risolvere il problema dell'appartenenza al gruppo e mantenere il gruppo up-to-date. Consente ai gruppi di risorse di inviare eventi relativi ai servizi al EventBridge servizio Amazon.

Il ruolo`AWSServiceRoleForResourceGroups` collegato al servizio considera attendibile solo il seguente servizio per assumere il ruolo collegato al servizio:

- `resourcegroups.amazonaws.com`

Le autorizzazioni associate al ruolo provengono dalla seguente politicaAWS gestita. Scegli il link sul nome della policy per visualizzare la policy nella console IAM.

- `AWS Policy gestite da per AWS Resource Groups`

Creazione del ruolo collegato al servizio per i Resource Groups

> **Important**
>
> Questo ruolo collegato al servizio può apparire nell'account, se si completa un'operazione in un altro servizio che richiede le caratteristiche supportate da questo ruolo. Per ulteriori informazioni, consulta Comparsa di un nuovo ruolo nella miaAccount AWS.

Per creare il ruolo collegato al servizio, attiva la funzionalità degli eventi del ciclo di vita del gruppo.

Modifica di un ruolo collegato al servizio per i Resource Groups

Resource Groups non consente di modificare il ruolo AWSServiceRoleForResourceGroups collegato al servizio. Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Puoi tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per i Resource Groups

Puoi eliminare il ruolo collegato al servizio solo dopo aver disattivato la funzionalità degli eventi del ciclo di vita del gruppo.

> **Important**
>
> - AWSimpedisce di rimuovere il ruolo collegato al servizio finché non disattivi per la prima volta la funzionalità degli eventi del ciclo di vita del gruppo che lo ha creato.
> - Ti consigliamo di non eliminare il ruolo collegato al servizio fintanto che nel tuo sono presenti gruppi di risorseAccount AWS. Il servizio Resource Groups non può interagire con altri utentiServizi AWS per gestire i tuoi gruppi se elimini questo ruolo.

Eliminazione manuale del ruolo collegato ai servizi

Utilizzare la console IAM, AWS CLI, la AWS o l'API per eliminare i ruoli collegati ai servizi AWSServiceRoleForResourceGroups. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Console

Per eliminare il ruolo collegato al servizio Resource Groups

1. Apri la console IAM nella pagina Ruoli.
2. Trova il ruolo denominato AWSServiceRoleForResourceGroups e seleziona la casella di controllo accanto ad esso.
3. Scegli Delete (Elimina).
4. Conferma l'intenzione di eliminare il ruolo inserendo il nome del ruolo nella casella, quindi scegli Elimina.

Il ruolo scompare dall'elenco di ruoli nella console IAM.

AWS CLI

Per eliminare il ruolo collegato al servizio Resource Groups

Per eliminare il ruolo, immetti il seguente comando con i parametri esattamente come mostrato. Non sostituire nessuno dei valori.

```
$ aws iam delete-service-linked-role \
    --role-name AWSServiceRoleForResourceGroups
{
    "DeletionTaskId": "task/aws-service-role/resource-groups.amazonaws.com/
AWSServiceRoleForResourceGroups/34e58943-e9a5-4220-9856-fc565EXAMPLE"
}
```

Il comando restituisce un ID attività. L'eliminazione effettiva del ruolo avviene in modo asincrono. Puoi verificare lo stato dell'eliminazione del ruolo fornendo l'identificatore di attività fornito alAWS CLI comando seguente.

```
$ aws iam get-service-linked-role-deletion-status \
    --deletion-task-id "task/aws-service-role/resource-groups.amazonaws.com/
AWSServiceRoleForResourceGroups/34e58943-e9a5-4220-9856-fc565EXAMPLE"
{
    "Status": "SUCCEEDED"
}
```

Regioni supportate per i ruoli collegati ai servizi

Resource Groups supporta l'utilizzo di ruoli collegati ai servizi in tutti iRegioni AWS luoghi in cui il servizio è disponibile. Per ulteriori informazioni, consulta Regioni ed endpoint di AWS.

Esempi di policy di AWS Resource Groups basate su identità

Per impostazione predefinita, i responsabili IAM, ad esempio ruoli e utenti, non dispongono dell'autorizzazione per creare o modificare Resource Groups di risorse. Inoltre, non sono in grado di eseguire attività utilizzando l'API AWS Management Console, AWS CLI, o AWS. Un amministratore IAM deve creare policy IAM che concedono ai responsabili l'autorizzazione per eseguire operazioni API specifiche sulle risorse specifiche di cui hanno bisogno. L'amministratore deve quindi collegare queste policy ai responsabili che richiedono tali autorizzazioni.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy nella scheda JSON nella Guida per l'utente IAM.

Argomenti

- Best practice delle policy
- Utilizzo della console e dell'API Resource Groups
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Visualizzazione di gruppi in tag

Best practice delle policy

Le policy basate su identità determinano se qualcuno può creare, accedere o eliminare risorse di Resource Groups nell'account. Queste operazioni possono comportare costi aggiuntivi per il proprio Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e suggerimenti:

- Nozioni di base sulle policy gestite da AWS e passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite da AWS che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWS specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni di processo nella Guida per l'utente di IAM.

- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di servizio, ma solo se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer fornisce oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente rootAccount AWS, attiva MFA per una maggiore sicurezza. Per richiedere l'AMF quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

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

Utilizzo della console e dell'API Resource Groups

Per accedere alla consoleAWS Resource Groups e all'API tag Editor, è necessario disporre di un set di autorizzazioni minimo. Queste autorizzazioni devono consentire di elencare e visualizzare i dettagli relativi alle risorse dei gruppi di risorse disponibili nell'AWSaccount. Se crei una policy basata su identità più restrittiva rispetto alle autorizzazioni minime richieste, la console e i comandi API non funzioneranno nel modo previsto per i responsabili (ruoli e utenti IAM) associate a tale policy.

Per garantire che tali entità possano ancora utilizzare Resource Groups, collega la seguente policy (o una policy che contiene le autorizzazioni elencate nella policy seguente) alle entità. Per ulteriori informazioni, consultare Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

Per ulteriori informazioni sulla concessione dell'accesso ai gruppi di risorse, consultaConcessione delle autorizzazioni per l'utilizzo AWS Resource Groups e Tag Editor in questa guida.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono allegate alla relativa identità utente. La policy include le autorizzazioni per completare questa operazione sulla console o a livello di programmazione utilizzando la AWS CLI o l'API AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
```

```
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Visualizzazione di gruppi in tag

Puoi utilizzare condizioni nella policy basata su identità per controllare l'accesso alle risorse dei Resource Groups di risorse in base ai tag. Questo esempio mostra come creare una policy che consente di visualizzare una risorsa, in questo esempio, un gruppo di risorse. Tuttavia, l'autorizzazione viene concessa solo se il tag di gruppo`project` ha lo stesso valore del`project` tag collegato al committente chiamante.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name"
        },
        {
```

```
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/
project}"}
            }
        }
    ]
}
```

Puoi collegare questa policy ai responsabili nel tuo account. Se un titolare con la chiave del tag`project` e il valore del tag`alpha` tenta di visualizzare un gruppo di risorse, anche il gruppo deve essere taggato`project=alpha`. Altrimenti all'utente viene negato l'accesso. La chiave di tag di condizione `project` corrisponde a `Project` e `project` perché i nomi delle chiavi di condizione non effettuano la distinzione tra maiuscole e minuscole. Per ulteriori informazioni, consulta Elementi delle policy JSON IAM: Condition nella Guida per l'utente IAM.

Risoluzione dei problemi di AWS Resource Groups identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Resource Groups e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in Resource Groups
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne al mio AWS account di accedere ai miei Resource Groups

Non sono autorizzato a eseguire un'azione in Resource Groups

Se ti AWS Management Console dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è colui che ti ha fornito le credenziali di accesso.

L'errore di esempio seguente si verifica quando l'utente `mateojackson` tenta di utilizzare la console per visualizzare i dettagli su un gruppo ma non dispone `resource-groups:ListGroups` dell'autorizzazione.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: resource-groups:ListGroups on resource: arn:aws:resource-groups::us-
west-2:123456789012:group/my-test-group
```

In questo caso, Mateo richiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa `my-test-group` utilizzando l'azione `resource-groups:ListGroups`.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo a Resource Groups.

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

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Resource Groups. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne al mio AWS account di accedere ai miei Resource Groups

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l’assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizza tali policy per concedere alle persone l’accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Resource Groups supporta queste funzionalità, vedereCome funziona Resource Groups con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per scoprire la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.

Registrazione e monitoraggio in un gruppo di risorse monitoraggio in Resource Groups

TutteAWS Resource Groups le azioni vengono registrateAWS CloudTrail.

Registrazione delle chiamate API AWS Resource Groups con AWS CloudTrail

AWS Resource Groupse Tag Editor sono integrati conAWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o unAWS servizio in Resource Groups o Tag Editor. CloudTrail acquisisce un sottoinsieme di chiamate API per i Resource Groups come eventi, incluse le chiamate dalla console Resource Groups o dall'Editor di tag e dalle chiamate di codice alle API dei Resource Groups. Se si crea un trail, è possibile abilitare la distribuzione continua di CloudTrail eventi in un bucket Amazon S3, inclusi gli eventi per i Resource Groups. Se non configuri un trail, è comunque possibile visualizzare gli eventi più recenti nella CloudTrail console di in Event history (Cronologia eventi). Le informazioni raccolte da permettono CloudTrail di determinare la richiesta effettuata a Resource Groups, l'indirizzo IP da cui è stata effettuata la richiesta, l'autore della richiesta, il momento in cui è stata effettuata e altri dettagli.

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

Informazioni sui Resource Groups in CloudTrail

CloudTrail è abilitato sull'AWSaccount al momento della sua creazione. Quando si verifica un'attività nei Resource Groups o nella console di Tag Editor, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi delAWS servizio nella sezione Event history (Cronologia eventi). È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia CloudTrail eventi di.

Per una registrazione continua degli eventi nell'AWSaccount, inclusi gli eventi per i Resource Groups, crea un trail. Un trail consente di CloudTrail distribuire i file di log in un bucket Amazon S3. Per impostazione di default, quando crei un trail nella console, il trail sarà valido in tutte le regioni. Il trail registra gli eventi di tutte le regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri servizi AWS per analizzare con maggiore dettaglio e usare i dati raccolti nei log CloudTrail. Per ulteriori informazioni, consultare:

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

Tutte le operazioni Resource Groups vengono registrate CloudTrail e sono documentate nella documentazione di riferimento delleAWS Resource Groups API di. Le azioni Resource Groups in CloudTrail vengono visualizzate come eventi con l'endpoint API`resource-groups.amazonaws.com` come origine. Ad esempio, le chiamate alle`UpdateGroupQuery` operazioni`CreateGroup`,`GetGroup`, e generano voci nei file di CloudTrail log. Le azioni dell'editor di tag nella console vengono registrate CloudTrail e vengono visualizzate come eventi con l'endpoint API interno`resource-explorer` come origine.

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

- Se la richiesta è stata effettuata con le credenziali utente IAM o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta l'elemento CloudTrail `userIdentity`.

Informazioni sulle voci dei file di log dei file di log dei gruppi di log

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

L'esempio seguente mostra una voce di CloudTrail log di che illustra l'operazione`CreateGroup`.

```
{"eventVersion":"1.05",
"userIdentity":{
    "type":"AssumedRole",
    "principalId":"ID number:AWSResourceGroupsUser",
    "arn":"arn:aws:sts::831000000000:assumed-role/Admin/AWSResourceGroupsUser",
    "accountId":"831000000000","accessKeyId":"ID number",
    "sessionContext":{
        "attributes":{
            "mfaAuthenticated":"false",
            "creationDate":"2018-06-05T22:03:47Z"
            },
        "sessionIssuer":{
            "type":"Role",
            "principalId":"ID number",
            "arn":"arn:aws:iam::831000000000:role/Admin",
            "accountId":"831000000000",
            "userName":"Admin"
            }
        }
    },
"eventTime":"2018-06-05T22:18:23Z",
"eventSource":"resource-groups.amazonaws.com",
"eventName":"CreateGroup",
"awsRegion":"us-west-2",
"sourceIPAddress":"100.25.190.51",
"userAgent":"console.amazonaws.com",
"requestParameters":{
    "Description": "EC2 instances that we are using for application staging.",
    "Name": "Staging",
    "ResourceQuery": {
      "Query": "string",
      "Type": "TAG_FILTERS_1_0"
```

```
      },
    "Tags": {
      "Key":"Phase",
      "Value":"Stage"
      }
    },
"responseElements":{
    "Group": {
      "Description":"EC2 instances that we are using for application staging.",
      "groupArn":"arn:aws:resource-groups:us-west-2:831000000000:group/Staging",
      "Name":"Staging"
     },
    "resourceQuery": {
      "Query":"string",
      "Type":"TAG_FILTERS_1_0"
     }
    },
"requestID":"de7z64z9-d394-12ug-8081-7zz0386fbcb6",
"eventID":"8z7z18dz-6z90-47bz-87cf-e8346428zzz3",
"eventType":"AwsApiCall",
"recipientAccountId":"831000000000"
}
```

Convalida della conformità per Resource Groups

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 .

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

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono i passaggi per l'implementazione di ambienti di base incentrati sulla AWS sicurezza e la conformità.

- Architettura per la HIPAA sicurezza e la conformità su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee. HIPAA

  > **Note**
  >
  > Non tutte sono idonee. Servizi AWS HIPAA Per ulteriori informazioni, consulta la Guida ai servizi HIPAA idonei.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe riguardare il settore e la località in cui operi.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization ()). ISO
- Evaluating Resources with Rules nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, ad esempio PCI DSS soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente AWS l'utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in Resource Groups

AWS Resource Groupsesegue backup automatizzati sulle risorse interne del servizio. Questi backup non sono configurabili dall'utente. I backup vengono crittografati, sia inattivi o in transito. Resource Groups memorizzano i dati dei clienti in Amazon DynamoDB.

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

Anche una perdita completa dei gruppi di risorse utente non comporterebbe la perdita di dati dei clienti, poiché la maggior parte dei dati dei clienti viene replicata inAWSZone di disponibilità (AZ). Se si eliminano i gruppi accidentalmente, contattareAWS Supportcenter.

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

Sicurezza dell'infrastruttura nei Resource Groups

Non esistono altri modi per isolare il traffico di servizio o di rete fornito da Resource Groups. Se applicabile, utilizzare l'isolamento AWS specifico. È possibile utilizzare Resource Groups API e la console per VPC massimizzare la privacy e la sicurezza dell'infrastruttura.

In quanto servizio gestito, AWS Resource Groups è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Si utilizzano API chiamate AWS pubblicate per accedere ai Resource Groups attraverso la rete. I client devono supportare quanto segue:

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

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

Resource Groups non supporta le politiche basate sulle risorse.

Best practice practice practice practice practice practice practice practice practice practice practice practice

Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Dato che queste best practice potrebbero non essere appropriate o sufficienti nel proprio ambiente, si considerino come riflessioni utili più che istruzioni.

- Usa il principio del privilegio minimo per concedere l'accesso ai gruppi. Resource Groups supporta le autorizzazioni a livello di risorsa. Concedi l'accesso a gruppi specifici solo come richiesto per utenti specifici. Evita di utilizzare asterischi nelle dichiarazioni politiche che assegnano le autorizzazioni a tutti gli utenti o a tutti i gruppi. Per ulteriori informazioni sul privilegio minimo, consulta Concedere il privilegio minimo nella Guida per l'utente IAM.
- Tieni le informazioni private fuori dai campi pubblici. Il nome di un gruppo viene considerato come metadati di servizio. I nomi dei gruppi non sono crittografati. Non inserire informazioni sensibili nei nomi dei gruppi. Le descrizioni dei gruppi sono private.

  Non inserire informazioni private o sensibili nelle chiavi o nei valori dei tag.
- Usa l'autorizzazione basata sui tag ogni volta che è opportuno. Resource Groups supporta l'autorizzazione basata sui tag. Puoi etichettare i gruppi, quindi aggiornare le policy associate ai tuoi responsabili IAM, come utenti e ruoli, per impostare il loro livello di accesso in base ai tag applicati a un gruppo. Per ulteriori informazioni su come utilizzare l'autorizzazione basata sui tag, consulta Controllare l'accesso alleAWS risorse utilizzando i tag delle risorse nella Guida per l'utente IAM.

  MoltiAWS servizi supportano l'autorizzazione basata sui tag per le operazioni. Tieni presente che l'autorizzazione basata su tag potrebbe essere configurata per le risorse dei membri di un gruppo. Se l'accesso alle risorse di un gruppo è limitato dai tag, utenti o gruppi non autorizzati potrebbero non essere in grado di eseguire azioni o automazioni su tali risorse. Ad esempio, se un'istanza Amazon EC2 in uno dei tuoi gruppi è contrassegnata con una chiave di tag pari a`Confidentiality` e un valore di tag pari a`High`, e non sei autorizzato a eseguire comandi sulle risorse taggate`Confidentiality:High`, le azioni o le automazioni eseguite sull'istanza EC2 avranno esito negativo, anche se le azioni hanno esito positivo per altre risorse del gruppo di risorse. Per ulteriori informazioni sui servizi che supportano l'autorizzazione basata su tag per le proprie risorse, consulta AWSServizi che funzionano con IAM nella Guida per l'utente di IAM.

  Per ulteriori informazioni sullo sviluppo di una strategia di etichettatura perAWS le tue risorse, consulta StrategieAWS di tagging.

Service quotas per gruppi di risorse

La tabella seguente descrive le quote all'interno di AWS Resource Groups (Resource Groups). Per una quota regolabile, puoi richiedere un aumento della console Service Quotas.

Nome	Predefinita	Adattabile	Descrizione
Gruppi di risorse per account	Ogni regione supportata: 100	Sì	Il numero massimo di gruppi di risorse che puoi creare in questo account. Un gruppo di risorse è una raccolta di AWS risorse che corrispondono a criteri specifici.

AWS Resource Groups cronologia dei documenti

Modifica	Descrizione	Data
Contenuti aggiornati	Titoli degli argomenti aggiornati e contenuti riorganizzati per migliorare la leggibilità e la reperibilità.	1 agosto 2024
Support per altri tipi di risorse	Altri tipi di risorse sono ora supportati da Resource Groups e Tag Editor.	30 maggio 2024
ResourceGroupsandTagEditorFullAccess Politiche AWS gestite aggiornate e ResourceGroupsandTagEditorReadOnlyAccess	Resource Groups ha aggiornato due policy AWS gestite per aggiungere AWS CloudFormation autorizzazioni aggiuntive.	10 agosto 2023
Quote di servizio Resource Groups	È ora possibile visualizzare i limiti di quota di Resource Groups utilizzando Service Quotas.	29 giugno 2023
IAMaggiornamento delle migliori pratiche	Guida aggiornata per allinearsi alle IAM migliori pratiche. Per ulteriori informazioni, consulta le migliori pratiche di sicurezza in IAM.	3 gennaio 2023
Le informazioni di Tag Editor sono state spostate nella relativa guida	La documentazione per Tag Editor è stata rimossa da questa guida e spostata nella nuova Guida per l'utente di Tag Editor.	13 dicembre 2022
I gruppi di risorse possono ora includere risorse di Amazon	AWS Resource Groups ora supporta l'inclusione di risorse	20 ottobre 2022

Keyspaces (per Apache Cassandra)	per Amazon Keyspaces (per Apache Cassandra) in un gruppo di risorse.	
Obsoletizzazione dei tipi di risorse	I seguenti tipi di risorse non sono più supportati da Tag Editor:`AWS::RoboMaker::Robot` , `AWS::RoboMaker::Fleet` e. `AWS::RoboMaker::DeploymentJob`	17 maggio 2022
Nuova politica AWS gestita - ResourceGroupsServiceRolePolicy	Resource Groups ha aggiunto una nuova policy AWS gestita in AWS Identity and Access Management (IAM) per supportare il ruolo collegato al servizio del servizio.	12 gennaio 2022
Eventi del ciclo di vita del gruppo	I Resource Groups ora possono generare eventi in Amazon CloudWatch Events per avvisarti quando vengono apportate modifiche ai tuoi gruppi di risorse.	12 gennaio 2022
I gruppi di risorse possono ora essere utilizzati da Amazon VPC Network Access Analyzer per monitorare il traffico di rete indesiderato verso AWS le tue risorse.	Puoi utilizzarli AWS Resource Groups per specificare le fonti e le destinazioni per i tuoi requisiti di accesso alla rete.	3 dicembre 2021
È stato aggiunto il supporto per le risorse di AWS Resilience Hub	AWS Resource Groups ora supporta l'inclusione di risorse per AWS Resilience Hub in un gruppo di risorse.	18 novembre 2021

È stato aggiunto il supporto per le risorse di Amazon Pinpoint	AWS Resource Groups ora supporta l'inclusione di risorse per Amazon Pinpoint in un gruppo di risorse.	11 novembre 2021
È stato aggiunto il supporto per i gruppi di risorse configurati e gestiti da AppRegistry	AWS Resource Groups ora supporta gruppi di risorse che contengono configurazioni di servizio per le risorse nelle applicazioni create utilizzando AWS Service Catalog AppRegistry. Per ulteriori informazioni, vedere Configurazioni dei servizi nel AWS Resource Groups API riferimento.	15 settembre 2021
Aggiunto il supporto per le risorse di Amazon OpenSearch Service	AWS Resource Groups ora supporta l'inclusione di risorse per Amazon OpenSearch Service in un gruppo di risorse.	11 agosto 2021
È stato aggiunto il supporto per le risorse di AWS Braket	AWS Resource Groups ora supporta l'inclusione di risorse per AWS Braket in un gruppo di risorse.	30 giugno 2021
Aggiunto supporto per le risorse di Amazon EMR Containers	AWS Resource Groups ora supporta l'inclusione di risorse per EMR i contenitori Amazon in un gruppo di risorse.	27 aprile 2021

È stato aggiunto il supporto per risorse di AWS servizi aggiuntivi	AWS Resource Groups ora supporta l'inclusione di risorse per i seguenti servizi in un gruppo di risorse: Amazon CodeGuru Reviewer, Amazon Elastic Inference, Amazon Forecast, Amazon Fraud Detector e Service Quotas.	25 febbraio 2021
È stato aggiunto un capitolo sulla sicurezza e la conformità.	Descrive in che modo Resource Groups protegge le tue informazioni e rispetta gli standard normativi.	30 luglio 2020

È stato aggiunto il supporto per i gruppi di risorse configurati per i servizi AWS	È ora possibile creare gruppi di risorse associati a un AWS servizio e che configurano il modo in cui il servizio può interagire con le risorse del gruppo. In questa prima versione della funzionalità, puoi creare un gruppo di risorse che contiene le prenotazioni di EC2 capacità Amazon e quindi avviare EC2 le istanze Amazon nel gruppo. Se una o più prenotazioni del gruppo corrispondono alla tua istanza, quell'istanza utilizza la prenotazione. Se l'istanza non corrisponde a nessuna prenotazione disponibile nel gruppo, viene avviata come istanza on-demand. Per ulteriori informazioni, consulta Lavorare con i gruppi di prenotazione di capacità nella Amazon EC2 User Guide.	29 luglio 2020
È stato aggiunto il supporto per AWS IoT Greengrass le risorse.	Altri tipi di risorse sono ora supportati da AWS Resource Groups and Tag Editor.	25 marzo 2020

Visualizza i dati operativi per AWS Resource Groups	Nella AWS Systems Manager console, la AWS Resource Groups pagina mostra i dati operativi per un gruppo selezionato in quattro schede: Dettagli, Config CloudTrai l,,. OpsItems Queste schede non sono disponibili quando si visualizza un gruppo nella console Resource Groups. È possibile utilizzare le informazi oni contenute in queste schede per comprendere quali risorse di un gruppo sono conformi e funzionano correttamente e quali risorse richiedono un'azione. Se è necessario intervenire su una risorsa, è possibile utilizzar e i runbook di automazio ne di Systems Manager per eseguire operazioni comuni di manutenzione e risoluzio ne dei problemi. Per ulteriori informazioni, vedere Visualizz azione dei dati operativi AWS Resource Groups nella Guida per l'AWS Systems Manager utente.	16 marzo 2020

Verifica la conformità con le politiche sui tag	Dopo aver creato e allegato le politiche relative ai tag agli account utilizzando AWS Organizations, puoi trovare tag non conformi sulle risorse degli account della tua organizzazione.	26 novembre 2019
Support per altri tipi di risorse	Altri tipi di risorse sono ora supportati da AWS Resource Groups and Tag Editor.	4 ottobre 2019
Nuovi tipi di risorse supportati da AWS Resource Groups	Ora sono supportati più tipi di risorse AWS Resource Groups, specialmente per i gruppi basati su uno AWS CloudFormation stack.	5 agosto 2019
Nuovi tipi di risorse supportati da AWS Resource Groups	Amazon API Gateway RESTAPIs, CloudWatch gli eventi Amazon Events e gli SNS argomenti Amazon ora sono tipi di risorse supportati in AWS Resource Groups.	27 giugno 2019
Tag Editor ora supporta la ricerca di risorse senza tag	Ora puoi cercare risorse in Tag Editor a cui non sono stati applicati valori di tag per una chiave di tag specifica.	18 giugno 2019
Nuovi tipi di risorse supportati da AWS Resource Groups Tag Editor	Sono stati aggiunti oltre 50 nuovi tipi di risorse AWS Resource Groups e supporto per Tag Editor.	6 giugno 2019

AWS Resource Groups e la console Tag Editor esce dalla AWS Systems Manager console	La console AWS Resource Groups and Tag Editor è ora indipendente dalla console Systems Manager. Sebbene sia ancora possibile trovare i puntatori alla AWS Resource Groups console nella barra di navigazione sinistra di Systems Manager, è possibile aprire la console Resource Groups and Tag Editor direttamente dal menu a discesa in alto a sinistra di. AWS Management Console	5 giugno 2019
Nuove funzionalità di autorizzazione e controllo degli accessi di Resource Groups	Resource Groups ora supporta politiche basate sulle azioni, autorizzazioni a livello di risorsa e autorizzazioni basate sui tag.	24 maggio 2019
I vecchi strumenti Resource Groups e Tag Editor non sono più disponibili	Le menzioni a Resource Groups e Tag Editor precedenti, classici o precedenti sono state rimosse; questi strumenti non sono più disponibili in AWS. Utilizzate invece AWS Resource Groups and Tag Editor.	14 maggio 2019
Tag Editor ora supporta l'etichettatura delle risorse in più aree	Tag Editor ora ti consente di cercare e gestire i tag di risorse in più regioni, con l'aggiunta della tua attuale regione alle query di risorse per impostazione predefinita.	2 maggio 2019

Tag Editor ora supporta l'esportazione dei risultati delle query in un CSV	È possibile esportare i risultati di una query nella pagina Trova risorse per taggare in un file in CSV formato. Una nuova colonna Regione viene mostrata ni risultati della query di Tag Editor. Tag Editor ora permette di cercare le risorse che hanno valori vuoti per una chiave tag specifica. I valori della chiave tag si completan o automaticamente man mano che si digita un valore univoco tra le chiavi esistenti.	2 Aprile 2019
Tag Editor ora supporta l'aggiunta di tutti i tipi di risorse a una query	È possibile applicare tag a fino a 20 singoli tipi di risorse in un'unica operazione, oppure è possibile scegliere tutti i tipi di risorse per eseguire la query di tutti i tipi di risorse in una regione. Il completamento automatico è stato aggiunto al campo Tag key (Chiave tag) di una query per aiutare a abilitare le chiavi dei tag coerenti tra le risorse. Se le modifiche dei tag non vanno a buon fine in alcune risorse, è possibile riprovare le modifiche dei tag solo sulle risorse per cui le modifiche dei tag non sono riuscite.	19 marzo 2019

Tag Editor ora supporta più tipi di risorse in una ricerca	È possibile applicare tag a fino a 20 tipi di risorse in un'unica operazione. È anche possibile scegliere le colonne che vengono visualizzate nei risultati della ricerca, incluse le colonne per ciascuna chiave tag univoca presente nei risultati di ricerca o nelle risorse selezionate dai risultati.	26 febbraio 2019
Documentazione aggiunta per il nuovo Tag Editor	La sezione «Lavorare con Tag Editor» descrive come utilizzare la nuova esperienza della console AWS Tag Editor.	13 febbraio 2019
Nuovi tipi di risorse supportati per i gruppi in Resource Groups	Sono stati aggiunti nuovi tipi di risorse che ora sono supportati in Resource Groups.	4 febbraio 2019
Esperienza utente migliorata per l'aggiunta di tag alle query Resource Groups basate su tag	Modifiche minori all'esperienza utente della console per l'aggiunta di tag in una query basata su tag.	17 dicembre 2018
AWS CloudFormation supporto di query basato sullo stack aggiunto a Resource Groups	È possibile creare gruppi di risorse in cui la query è basata su uno AWS CloudFormation stack. Dopo aver scelto uno stack, è possibile scegliere quali tipi di risorse dallo stack si desidera visualizzare nella propria query del gruppo.	13 novembre 2018

Resource Groups e CloudTrail	Resource Groups ora offre AWS CloudTrail supporto. È possibile visualizzare e utilizzare i registri di tutte le API chiamate Resource Groups in CloudTrail entrata.	29 giugno 2018

- APIversione: 2017-11-27
- Ultimo aggiornamento della documentazione: 24 settembre 2019

Aggiornamenti precedenti

La tabella seguente descrive le modifiche importanti apportate a ogni versione della Guida per l'utente di AWS Resource Groups prima di giugno 2018.

Modifica	Descrizione	Data
Rilascio iniziale	Versione iniziale della prossima generazione di AWS Resource Groups	29 novembre 2017

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.