Guida per l'utente

AWS Risorse per l'etichettatura e editor di tag

Version 1.0

AWS Risorse per l'etichettatura e editor di tag: Guida per l'utente

Table of Contents

AWS ha spostato la funzionalità di gestione dei tag di Tag Editor dalla AWS Resource Groups console alla console. Esploratore di risorse AWS Con Resource Explorer, puoi cercare e filtrare le risorse e quindi gestire i tag delle risorse da un'unica console. Per ulteriori informazioni sulla gestione dei tag delle risorse in Resource Explorer, consulta la sezione Gestione delle risorse nella guida per l'utente di Resource Explorer.

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.

Che cos'è Tag Editor?

Tag Editor ti consente di gestire efficacemente i tag. 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. Esempi di risorse includono un'istanza Amazon Elastic Compute Cloud (Amazon EC2), un bucket Amazon Simple Storage Service (Amazon S3) o un secret in. AWS Secrets Manager

> **Important**
>
> Non memorizzare informazioni personali identificabili 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.

Con i tag è possibile a gestire, identificare, organizzare, cercare e filtrare le risorse. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri.

Ogni tag è costituito da due parti:

- Una chiave del tag (ad esempio, `CostCenter`, `Environment` o `Project`). Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.
- Un valore di tag (ad esempio, `111122223333` oppure `Production`). Analogamente alle chiavi dei tag, i valori dei tag prevedono una distinzione tra lettere maiuscole e minuscole.

> **Note**
>
> Sebbene le chiavi dei tag facciano distinzione tra maiuscole e minuscole, IAM dispone di convalide aggiuntive per le risorse IAM per impedire l'applicazione di chiavi di tag che differiscono solo nella classificazione delle maiuscole e minuscole. Consigliamo di non utilizzare chiavi che differiscono solo nella custodia. Puoi invece utilizzare Service Control Policies (SCPs), che forniscono il controllo centralizzato sulle autorizzazioni massime disponibili per gli utenti IAM e i ruoli IAM nell'organizzazione.

Metodi di etichettatura delle risorse

Esistono tre modi per aggiungere tag alle AWS risorse:

- Servizio AWS Funzionamento dell'API: le operazioni dell'API di tagging supportavano direttamente un Servizio AWS. Per scoprire le funzionalità di tagging Servizio AWS fornite da ciascuna di esse, consulta la documentazione del servizio nell'indice della AWS documentazione.
- Console Tag Editor: alcuni servizi supportano l'etichettatura con la console Tag Editor.
- API Resource Groups Tagging: la maggior parte dei servizi supporta anche l'etichettatura utilizzando. AWS Resource Groups Tagging API

> **Note**
>
> Puoi anche utilizzare AWS Service Catalog TagOptions Library per gestire facilmente i tag sui prodotti forniti. A TagOptionè una coppia chiave-valore gestita in Service Catalog. Non è un AWS tag, ma funge da modello per la creazione di un AWS tag basato su. TagOption

Puoi assegnare un tag alle risorse per tutti i servizi di maturazione dei costi in AWS. Per i seguenti servizi, AWS consiglia un'alternativa più recente Servizi AWS che supporti l'etichettatura per soddisfare meglio i casi d'uso dei clienti.

Directory del cloud Amazon	Amazon CloudSearch	Amazon Cognito Sync
AWS Data Pipeline	Amazon Elastic Transcoder	Amazon Machine Learning
AWS OpsWorks Stacks	Amazon S3 Glacier Direct	Amazon SimpleDB
Gestore di WorkSpaces applicazioni Amazon	AWS DeepLens	

Ulteriori informazioni

Questa pagina fornisce informazioni generali sull'etichettatura AWS delle risorse. Per ulteriori informazioni sull'etichettatura delle risorse in un particolare AWS servizio, consulta la relativa documentazione. Di seguito sono riportate valide fonti di informazioni sul tagging:

- Per informazioni su AWS Resource Groups Tagging API, consulta la Resource Groups Tagging API Reference Guide.
- Per informazioni sulle funzionalità di tagging Servizio AWS fornite da ciascuna di esse, consulta la documentazione del servizio nell'indice della AWS documentazione.
- Per informazioni sull'utilizzo dei tag nelle policy IAM per controllare chi può visualizzare e interagire con AWS le tue risorse, consulta Controlling access to e for IAM users and roles using tags nella IAM User Guide.

Migliori pratiche e strategie

Queste sezioni forniscono informazioni sulle migliori pratiche e strategie per etichettare le AWS risorse e utilizzare Tag Editor.

Le migliori pratiche di etichettatura

Quando crei una strategia di etichettatura per AWS le risorse, segui le migliori pratiche:

- Non aggiungere Informazioni personali di identificazione (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti AWS servizi, inclusa la fatturazione. I tag non sono destinati ad essere utilizzati per dati privati o sensibili.
- Utilizza un formato standardizzato con distinzione tra maiuscole e minuscole per i tag e applicalo in modo coerente a tutti i tipi di risorse.
- Prendi in considerazione le linee guida per i tag che supportano più scopi, ad esempio la gestione del controllo dell'accesso alle risorse, il monitoraggio dei costi, l'automazione e l'organizzazione.
- Utilizza strumenti automatizzati per gestire i tag delle risorse. Tag Editor e l'API Resource Groups Tagging consentono il controllo programmatico dei tag, semplificando la gestione, la ricerca e il filtraggio automatici di tag e risorse.
- Utilizza molti tag piuttosto che pochi tag.
- Ricorda che è facile cambiare i tag per soddisfare le mutevoli esigenze aziendali, ma considera le conseguenze delle modifiche future. Ad esempio, modificando i tag di controllo di accesso, è necessario aggiornare anche le policy che fanno riferimento a tali tag e controllare l'accesso alle risorse.
- È possibile applicare automaticamente gli standard di assegnazione di tag che l'organizzazione sceglie di adottare creando e distribuendo policy di tag tramite AWS Organizations. Le policy di

tag consentono di specificare regole di assegnazione di tag che definiscono nomi di chiavi validi e valori validi per ogni chiave. È possibile decidere di monitorare soltanto, con la possibilità di valutare e ripulire i tag esistenti. Una volta che i tag sono conformi agli standard scelti, è possibile attivare l'applicazione nelle policy di tag in modo da impedire la creazione di tag non conformi. Per ulteriori informazioni, consultare Policy di tag nella Guida per l'utente di AWS Organizations .

Le migliori pratiche per la denominazione dei tag

Queste sono alcune best practice e convenzioni di denominazione che consigliamo di utilizzare con i tag.

I nomi chiave dei AWS tag fanno distinzione tra maiuscole e minuscole, quindi assicurati che vengano utilizzati in modo coerente. Ad esempio, i tag keys `CostCenter` e `costcenter` sono diversi. Una chiave di tag potrebbe essere configurata come tag di allocazione dei costi per l'analisi e la rendicontazione finanziaria e l'altra chiave potrebbe non essere configurata per lo stesso uso.

Alcuni tag sono predefiniti AWS o creati automaticamente da vari. Servizi AWS Molti tag AWS generati utilizzano nomi chiave tutti minuscoli, con trattini che separano le parole nel nome e prefissi seguiti da due punti per identificare il servizio di origine del tag. Ad esempio, consulta quanto segue:

- `aws:ec2spot:fleet-request-id`è un tag che identifica l'Amazon EC2 Spot Instance Request che ha avviato l'istanza.
- `aws:cloudformation:stack-name`è un tag che identifica lo AWS CloudFormation stack che ha creato la risorsa.
- `elasticbeanstalk:environment-name`è un tag che identifica l'applicazione che ha creato la risorsa.

Valuta la possibilità di assegnare un nome ai tag utilizzando le seguenti regole:

- Usa tutte le lettere minuscole per le parole.
- Usa i trattini per separare le parole.
- Utilizza un prefisso seguito da due punti per identificare il nome dell'organizzazione o il nome abbreviato.

Ad esempio, per una società fittizia denominata AnyCompany, è possibile definire tag come:

- `anycompany:cost-center`per identificare il codice interno del centro di costo.

- `anycompany:environment-type`per identificare se l'ambiente è di sviluppo, test o produzione.
- `anycompany:application-id`per identificare l'applicazione per cui è stata creata la risorsa.

Il prefisso garantisce che i tag siano chiaramente riconoscibili in base alla definizione dell'organizzazione e non a uno strumento di AWS terze parti che l'utente potrebbe utilizzare. L'uso di tutte le lettere minuscole con i trattini per i separatori evita confusione su come scrivere il nome di un tag. Ad esempio, `anycompany:project-id` è più semplice da ricordare rispetto `ANYCOMPANY:ProjectID`, `anycompany:projectID` oppure `Anycompany:ProjectId`.

Limiti e requisiti per la denominazione dei tag

I seguenti requisiti di denominazione e utilizzo di base si applicano ai tag:

- Ogni risorsa può avere un massimo di 50 tag creati dall'utente.
- I tag creati dal sistema che iniziano con `aws:` sono riservati all'uso AWS e non vengono conteggiati per questo limite. Non è possibile modificare o eliminare un tag che inizia con il prefisso `aws:`.
- Per ciascuna risorsa, ogni chiave del tag deve essere univoca e ogni chiave del tag può avere un solo valore.
- Il tag della chiave deve essere composto da un minimo di 1 e un massimo di 128 caratteri Unicode in UTF-8.
- Il valore del tag deve essere composto da un minimo di 0 e un massimo di 256 caratteri Unicode in UTF-8.
- I caratteri consentiti possono variare in base al servizio AWS . Per informazioni sui caratteri che è possibile utilizzare per etichettare le risorse in un particolare AWS servizio, consulta la relativa documentazione. In generale, i caratteri consentiti sono lettere, numeri, spazi rappresentabili in formato UTF-8, oltre ai seguenti caratteri: _ . : / = + - @.
- I valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole. Come best practice, è consigliabile definire una strategia per l'uso delle lettere maiuscole e minuscole nei tag e implementarla costantemente in tutti i tipi di risorse. Ad esempio, puoi decidere se utilizzare `Costcenter`, `costcenter` o `CostCenter` e utilizzare la stessa convenzione per tutti i tag. Non utilizzare tag simili con lettere maiuscole o minuscole incoerenti.

Strategie comuni di tagging

Utilizza le seguenti strategie di assegnazione tag per individuare e gestire le risorse AWS .

Indice

Tag per l'organizzazione delle risorse

I tag sono un buon modo per organizzare AWS le risorse in AWS Management Console. È possibile configurare i tag da visualizzare con le risorse e cercare e filtrare per tag. Con il AWS Resource Groups servizio, è possibile creare gruppi di AWS risorse basati su uno o più tag o porzioni di tag. Puoi anche creare gruppi in base alla loro presenza in uno AWS CloudFormation stack. Utilizzando Resource Groups e Tag Editor, è possibile consolidare e visualizzare i dati per applicazioni che consistono in più servizi, risorse e regioni in un'unica posizione.

Tag per l'allocazione dei costi

AWS Cost Explorer e report di fatturazione dettagliati consentono di suddividere AWS i costi per tag. In genere, si utilizzano tag aziendali come centro di costo/unità aziendale, cliente o progetto per associare AWS i costi alle dimensioni tradizionali di allocazione dei costi. Un report di allocazione dei costi può includere qualsiasi tag. Questa possibilità permette di associare i costi secondo parametri tecnici o di sicurezza, ad esempio in relazione ad applicazioni, ambienti o programmi di conformità specifici.

Per alcuni servizi, è possibile utilizzare un `createdBy` tag AWS generato per l'allocazione dei costi, per tenere conto delle risorse che altrimenti potrebbero non essere categorizzate. Il tag `createdBy` è disponibile solo per i servizi e le risorse AWS supportati. Il suo valore contiene dati associati a specifici eventi API o console. Per ulteriori informazioni, consultare la pagina AWS Tag di allocazione dei costi generati da nella Guida per l'utente di AWS Billing and Cost Management .

Tag per automazione

I tag specifici delle risorse o dei servizi vengono spesso utilizzati per filtrare le risorse durante le attività di automazione. I tag di automazione vengono utilizzati per attivare o disattivare le attività automatiche o per identificare versioni specifiche delle risorse da archiviare, aggiornare o eliminare. Ad esempio, è possibile eseguire script `start` o `stop` automatizzati che disattivano gli ambienti

di sviluppo durante le ore non lavorative per ridurre i costi. In questo scenario, i tag delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sono un modo semplice per identificare le istanze a cui rinunciare a questa azione. Per gli script che trovano ed eliminano istantanee di Amazon EBS obsolete o non funzionanti, i tag snapshot possono aggiungere una dimensione aggiuntiva ai criteri di ricerca. out-of-date

Tag per il controllo degli accessi

Le policy IAM supportano condizioni basate su tag, consentendo di vincolare le autorizzazioni IAM in base a tag o valori di tag specifici. Ad esempio, le autorizzazioni di utente o ruolo IAM possono includere condizioni per limitare le chiamate EC2 API a ambienti specifici (come sviluppo, test o produzione) in base ai relativi tag. La stessa strategia può essere utilizzata per limitare le chiamate API a reti Amazon Virtual Private Cloud (Amazon VPC) specifiche. Il supporto per le autorizzazioni IAM a livello di risorse basate su tag è specifico del servizio. Quando si utilizzano condizioni basate su tag per il controllo di accesso, assicurarsi di definire e limitare chi può modificare i tag. Per ulteriori informazioni sull'utilizzo dei tag per controllare l'accesso API alle risorse AWS , consultare Servizi AWS che funzionano con IAM in Guida per l'utente di IAM.

Governance di tagging

Una strategia di tagging efficace utilizza tag standardizzati e li applica in modo coerente e programmatico su tutte le risorse. AWS È possibile utilizzare approcci sia reattivi che proattivi per gestire i tag nel proprio ambiente. AWS

- La governance reattiva serve a trovare risorse che non sono etichettate correttamente utilizzando strumenti come l'API Resource Groups Tagging e Regole di AWS Config script personalizzati. Per trovare le risorse manualmente, è possibile utilizzare il Tag editor e i report di fatturazione dettagliati.
- La governance proattiva utilizza strumenti come Service Catalog AWS CloudFormation, tag policy in AWS Organizations o autorizzazioni a livello di risorsa IAM per garantire che i tag standardizzati vengano applicati in modo coerente alla creazione delle risorse.

  Ad esempio, è possibile utilizzare la AWS CloudFormation `Resource Tags` proprietà per applicare tag ai tipi di risorse. In Catalogo dei servizi, è possibile aggiungere tag di portfolio e prodotti combinati e applicati automaticamente a un prodotto quando viene avviato. Le forme più rigorose di governance proattiva includono operazioni automatizzate. Ad esempio, è possibile utilizzare l'API per il tagging di gruppi di risorse per cercare i tag di un ambiente AWS oppure eseguire script per mettere in quarantena o eliminare risorse contrassegnate in modo non corretto.

Categorie di tagging

Le aziende che sono più efficaci nell'uso dei tag in genere creano raggruppamenti di tag rilevanti per l'attività per organizzare le proprie risorse in base alle dimensioni tecniche, aziendali e di sicurezza. Le aziende che utilizzano processi automatizzati per gestire la propria infrastruttura includono anche tag aggiuntivi specifici per l'automazione.

Tag tecnici	Tag per automazione	Tag aziendali	Tag di sicurezza
• Nome – Identifica le singole risorse • ID applicazione – Identifica le risorse correlate a un'applicazione specifica • Ruolo applicazione – Descrive la funzione di una determinata risorsa (ad esempio server web, broker messaggi, database) • Cluster – Identifica le farm di risorse che condividono una configurazione comune ed eseguono una funzione specifica per un'applicazione • Ambiente – Distingue tra sviluppo, test e risorse di produzione	• Data/ora – Indica la data o l'ora in cui una risorsa deve essere avviata, arrestata, eliminata o ruotata • Opt-in/opt out – Indica se una risorsa deve essere inclusa in un'attività automatizzata come avvio, arresto o ridimensionamento di istanze • Sicurezza: determina i requisiti, ad esempio la crittografia o l'abilitazione dei log di flusso di Amazon VPC, identifica le tabelle di instradamento o i gruppi di sicurezza che necessitano di ulteriori controlli	• Progetto – Identifica i progetti supportati dalla risorsa • Proprietario – Identifica chi è responsabile della risorsa • Centro di costo/Business Unit – Identifica il centro di costo o la business unit associata a una risorsa, in genere per l'allocazione e il monitoraggio dei costi • Cliente – Identifica un client specifico che serve un particolare gruppo di risorse	• Riservatezza – Un identificativo per il livello di riservatezza dei dati specifico supportato da una risorsa. • Compliance – Un identificativo per i carichi di lavoro che devono rispettare requisiti di conformità specifici

Tag tecnici	Tag per automazione	Tag aziendali	Tag di sicurezza
• Versione – Consente di distinguere tra le versioni di risorse o applicazioni			

Guida introduttiva a Tag Editor

> **Important**
>
> Non memorizzare informazioni personali identificabili 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 aggiungere tag o modificare o eliminare i tag di più risorse contemporaneamente, usa Tag Editor. Con questa funzionalità, è possibile cercare le risorse a cui applicare tag e quindi gestirli per quelle risorse dei tuoi risultati di ricerca.

Per avviare l'editor di tag

1. Accedi alla AWS Management Console.
2. Esegui una delle seguenti operazioni:
   - Scegli Servizi. Quindi, in Management & Governance, scegli Resource Groups & Tag Editor. Nel riquadro di navigazione a sinistra, scegli Tag Editor.
   - Usa il link diretto: console AWS Tag Editor.

Non a tutte le risorse è possibile applicare tag. Per informazioni sulle risorse supportate da Tag Editor, consulta la colonna di etichettatura di Tag Editor in Tipi di risorse supportati nella Guida per l'AWS Resource Groups utente. Se un tipo di risorsa che desideri taggare non è supportato, faccelo AWS sapere scegliendo Feedback nell'angolo inferiore sinistro della finestra della console.

Per informazioni su autorizzazioni e ruoli necessari per applicare tag alle risorse, vedi Impostazione delle autorizzazioni.

Argomenti

Prerequisiti per lavorare con Tag Editor

Prima di iniziare a etichettare le tue risorse, assicurati di disporre di un account attivo Account AWS con le risorse esistenti e dei diritti appropriati per etichettare le risorse e creare gruppi.

Argomenti

Registrati per un Account AWS

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

Per iscriverti a un Account AWS

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

   Parte della procedura di registrazione prevede la ricezione di una telefonata o di un messaggio di testo e l'immissione di un codice di verifica sulla tastiera del telefono.

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

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

Crea un utente con accesso amministrativo

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

Proteggi i tuoi Utente root dell'account AWS

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

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

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

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, assegna l'accesso amministrativo a un utente.

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

Accesso come utente amministratore

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

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

Assegna l'accesso a ulteriori utenti

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

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

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

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

Creare risorse

È necessario disporre di risorse Account AWS per taggare. Per ulteriori informazioni sui tipi di risorse supportati, consulta la colonna Tag Editor Tagging in Tipi di risorse supportati nella Guida per l'AWS Resource Groups utente.

Impostazione delle autorizzazioni

Per sfruttare appieno Tag Editor, potresti aver bisogno di autorizzazioni aggiuntive per etichettare le risorse o per visualizzare le chiavi e i valori dei tag di una risorsa. Queste autorizzazioni rientrano 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.

Se sei un amministratore, puoi fornire le autorizzazioni ai tuoi utenti creando policy tramite il servizio AWS Identity and Access Management (IAM). Per prima cosa crei ruoli, utenti o gruppi IAM e poi applichi le policy con le autorizzazioni di cui hanno bisogno. Per informazioni sulla creazione e l'associazione delle policy IAM, consulta Lavorare con le policy.

Autorizzazioni per singoli servizi

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

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 operazioni di tagging nell'API di quel servizio, come l'operazione Amazon. EC2 CreateTags

Autorizzazioni necessarie per utilizzare la console Tag Editor

Per utilizzare la console Tag Editor per elencare e contrassegnare le risorse, è necessario aggiungere le seguenti autorizzazioni alla dichiarazione politica di un utente in IAM. Puoi aggiungere politiche AWS gestite che vengono gestite e mantenute aggiornate da AWS, oppure puoi creare e mantenere una politica personalizzata.

Utilizzo di politiche AWS gestite per le autorizzazioni di Tag Editor

Tag Editor supporta le seguenti politiche AWS gestite che puoi utilizzare per fornire un set predefinito di autorizzazioni agli utenti. Puoi allegare queste politiche gestite a qualsiasi ruolo, utente o gruppo proprio come faresti con qualsiasi altra politica che crei.

ResourceGroupsandTagEditorReadOnlyAccess

Questa policy concede al ruolo IAM o all'utente associato l'autorizzazione a richiamare le operazioni di sola lettura sia per Tag Editor che per Tag AWS Resource Groups Editor. Per leggere i tag di una risorsa, devi inoltre disporre delle autorizzazioni per quella risorsa tramite una politica separata. Scopri di più nella seguente Nota importante.

ResourceGroupsandTagEditorFullAccess

Questa policy concede al ruolo IAM o all'utente associato 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. Scopri di più nella seguente Nota importante.

Important

Le due politiche precedenti concedono l'autorizzazione a richiamare le operazioni di Tag Editor e utilizzare la console Tag Editor. Tuttavia, è necessario disporre anche 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:

- La policy AWS gestita ReadOnlyAccessconcede le autorizzazioni per le operazioni di sola lettura per le risorse di ogni servizio. AWS mantiene automaticamente questa politica aggiornata con le nuove non Servizi AWS appena diventano disponibili.
- Molti servizi forniscono policy AWS gestite di sola lettura specifiche del servizio che è possibile utilizzare per limitare l'accesso solo alle risorse fornite da tale servizio. Ad esempio, Amazon EC2 fornisce AmazonEC2ReadOnlyAccess.
- Puoi creare una politica personalizzata che conceda l'accesso solo a specifiche operazioni di sola lettura per i pochi servizi e risorse a cui desideri che i tuoi utenti accedano. Questa politica utilizza una strategia allowlist o una strategia di denylist.

  Una strategia di lista consentita 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 nell'esempio seguente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [ "tag:*" ],
            "Resource": "<ARNs of resources to allow tagging>"
        }
    ]
}
```

  In alternativa, puoi utilizzare una strategia di denylist che consenta l'accesso a tutte le risorse tranne quelle che blocchi esplicitamente. Ciò richiede una politica separata che si applica agli utenti pertinenti che consente l'accesso. La seguente politica di esempio nega quindi l'accesso alle risorse specifiche elencate dall'Amazon Resource Name (ARN).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
             "Action": [ "tag:*" ],
            "Resource": "<ARNs of resources to disallow tagging>"
        }
    ]
```

```
}
```

Aggiungere manualmente le autorizzazioni di Tag Editor

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

> **Note**
>
> L'`resource-groups:SearchResources`autorizzazione consente a Tag Editor di elencare le risorse quando filtri 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.

Concessione delle autorizzazioni per l'utilizzo di Tag Editor

Per aggiungere una politica per l'utilizzo AWS Resource Groups di Tag Editor a un ruolo, procedi come segue.

1. Apri la console IAM alla pagina Ruoli.
2. Trova il ruolo a cui vuoi concedere le autorizzazioni di Tag Editor. Scegli il nome del ruolo per aprire la pagina di riepilogo del ruolo.
3. Nella scheda Permissions (Autorizzazioni), scegliere Add permissions (Aggiungi autorizzazioni).

4. Scegli Attach existing policies directly (Collega direttamente le policy esistenti).
5. Scegliere Create Policy (Crea policy).
6. Nella scheda JSON incollare l'istruzione della policy seguente.

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

> **Note**
>
> Questa dichiarazione politica di esempio concede le autorizzazioni per eseguire solo azioni di Tag Editor.

7. Scegli Next: Tags (Successivo: Tag), quindi Next: Review (Successivo: Verifica).
8. Immettere un nome e una descrizione per la nuova politica. Ad esempio, **`AWSTaggingAccess`**.
9. Scegliere Create Policy (Crea policy).

Ora che la policy è stata salvata in IAM, puoi collegarla ad altri principi, come ruoli, gruppi o utenti. Per ulteriori informazioni su come aggiungere una policy a un principal, consulta Aggiungere e rimuovere i permessi di identità IAM nella Guida per l'utente IAM.

Autorizzazione e controllo degli accessi basati sui tag

Servizi AWS supporta quanto segue:

- Criteri basati sulle azioni: ad esempio, è possibile creare una politica che consenta agli utenti di eseguire `GetTagKeys` le nostre `GetTagValues` operazioni, ma non altre.
- Autorizzazioni a livello di risorsa nelle politiche: molti servizi supportano l'utilizzo ARNsper specificare singole risorse nella politica.
- Autorizzazione basata sui tag: molti servizi supportano l'utilizzo di tag di risorse in base a una politica. Ad esempio, è possibile creare una politica che consenta agli utenti l'accesso completo a un gruppo con lo stesso tag degli utenti. Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'AWS Identity and Access Management utente.
- Credenziali temporanee: gli utenti possono assumere un ruolo con una politica che consente le operazioni di Tag Editor.

Tag Editor non utilizza ruoli collegati ai servizi.

Per ulteriori informazioni su come Tag Editor si integra 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 Tag Editor
- Controllo dell'accesso alle AWS risorse mediante politiche

Trovare risorse da taggare

Con Tag Editor, crei una query per trovare risorse disponibili per l'etichettatura in una o più Regioni AWS risorse. È possibile scegliere fino a 20 singoli tipi di risorse, oppure creare una query su tutti i tipi di risorse. La tua query può includere risorse che dispongono già di tag o risorse in cui non sono presenti tag. Per maggiori informazioni, consulta la colonna Tag Editor Tagging in Tipi di risorse supportati nella Guida per l'AWS Resource Groups utente.

Dopo aver trovato risorse per i tag, è possibile utilizzare Tag Editor per aggiungere i tag oppure visualizzare, modificare o eliminare i tag.

Per cercare risorse per i tag

1. Apri la console Tag Editor.
2. (Facoltativo) Scegliete Regioni AWS in che modo cercare le risorse da taggare. Per impostazione predefinita, viene utilizzata la regione corrente. Per questa procedura, scegli us-east-1 e us-west-2.
3. Scegli almeno un tipo di risorsa dall'elenco a discesa Tipi di risorse. È possibile aggiungere o modificare i tag per un massimo di 20 singoli tipi di risorse alla volta, oppure scegliere tutti i tipi di risorse. Per questa procedura, scegliete AWS::EC2::Instancee AWS::S3::Bucket.
4. (Facoltativo) Nei campi Tag, inserite una chiave di tag o una coppia chiave-valore del tag, per limitare le risorse della corrente solo Regione AWS a quelle contrassegnate con i valori specificati. Quando inserite una chiave di tag, le chiavi di tag corrispondenti nella regione corrente vengono visualizzate in un elenco. Puoi scegliere una chiave di tag dall'elenco. Tag Editor auto completa la chiave tag mentre vengono digitati caratteri sufficienti per creare la corrispondenza con una chiave esistente. 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 del tag è facoltativo ma restringe ulteriormente i risultati della query. Per aggiungere ulteriori tag, scegliere Add (Aggiungi). Le query assegnano un `AND` operatore ai tag, quindi la query restituisce solo le risorse che corrispondono sia al tipo di risorsa specificato che a tutti i tag specificati.

> **Note**
>
> La console Tag Editor attualmente non supporta i caratteri jolly.

Per cercare le risorse con più valori per una chiave tag, aggiungere un altro tag con la stessa chiave alla query, ma specificando un valore diverso. I risultati includono tutte le risorse che vengono contrassegnate con la stessa chiave tag e che dispongono di uno qualsiasi dei valori selezionati. La ricerca fa distinzione tra maiuscole e minuscole.

Lascia vuote le caselle Tag per trovare tutte le risorse del tipo specificato tra quelle selezionate Regioni AWS. Questa query restituisce risorse con qualsiasi tag e include quelle che non dispongono di tag. Per rimuovere un tag dalla query, scegliere X sull'etichetta del tag.

Per trovare risorse che hanno un tag, ma con un valore vuoto, scegli (valore vuoto).

> **Note**
>
> Prima di poter trovare risorse con i tag specificati, è necessario che siano stati applicati ad almeno una risorsa del tipo specificato nell'elenco corrente Regione AWS.

5. Quando la query è pronta, scegliere Search resources (Cerca risorse). I risultati vengono visualizzati sotto forma di tabella nell'area dei risultati della ricerca delle risorse.

   Per filtrare un numero elevato di risorse, immettere un filtro di testo, come parte del nome di una risorsa, in Filter resources (Filtra risorse).

   > **Note**
   >
   > È possibile utilizzare sottostringhe per filtrare i risultati.

6. (Facoltativo) Per configurare le colonne visualizzate da Tag Editor nei risultati della ricerca delle risorse, scegli l'icona a forma di ingranaggio Preferenze nei risultati della ricerca delle risorse.

   Nella pagina Preferences (Preferenze), scegliere il numero di righe che si desidera visualizzare nei risultati della ricerca. Se vuoi vedere tutto il testo nella tabella, seleziona la casella di controllo Avvolgi le righe.

   Attivare le colonne che si desidera il Tag Editor visualizzi nei risultati. Puoi mostrare una colonna per ogni tag presente nei risultati di ricerca o un sottoinsieme selezionato dei risultati della ricerca. Puoi farlo in qualsiasi momento dopo aver trovato le risorse da taggare. Per abilitare una colonna, scegli l'icona dell'interruttore accanto al tag e modificala da disattivata a attiva.

Terminata la configurazione delle colonne visibili e il numero di righe visualizzate, scegliere Confirm (Conferma).

Visualizza e modifica i tag esistenti per una risorsa selezionata

Tag Editor mostra i tag esistenti sulle risorse selezionate presenti nei risultati della ricerca Trova risorse da etichettare.

Se hai abilitato una colonna Tag come descritto nella sezione precedente, puoi vedere il valore corrente di quel tag per ogni risorsa nei risultati della ricerca.

> **Note**
>
> Questo argomento spiega come modificare il tag per una singola risorsa. Puoi anche modificare in blocco i tag per più risorse selezionate contemporaneamente. Per ulteriori informazioni, consulta Gestione dei tag con Tag Editor.

Per modificare i tag in linea nella tabella dei risultati della ricerca

1. Scegli il valore per il tag sulla risorsa che desideri modificare.

   > **Note**
   >
   > - Se la risorsa scelta attualmente non ha un tag con la chiave scelta, il valore viene visualizzato come (senza tag).
   > - Se la risorsa scelta ha un tag con la chiave scelta ma senza un valore, il valore viene visualizzato come '—'.

2. Puoi inserire un nuovo valore o scegliere uno dei valori già presenti su altre risorse con questo tag. Puoi anche eliminare il tag da questa risorsa scegliendo Rimuovi tag.

Per visualizzare tutti i tag di una singola risorsa

1. Nei risultati della ricerca Trova risorse da contrassegnare, scegliete il numero nella colonna Tag per ogni risorsa per la quale desiderate visualizzare i tag esistenti. Le risorse con un trattino nella colonna Tag non dispongono di tag esistenti.

2. Visualizza i tag esistenti in Resource tags (Tag risorse). Puoi anche aprire questa finestra scegliendo Gestisci i tag delle risorse selezionate, quando modifichi o rimuovi i tag dalla pagina Gestisci tag.

> **Note**
>
> Se un tag appena applicato su una risorsa non viene visualizzato, provare ad aggiornare la finestra del browser.

Esporta i risultati in un file.csv

È possibile esportare i risultati di una query Find resources to tag in un file con valori separati da virgole (.csv). Il file.csv include i nomi delle risorse, i servizi, la regione, la risorsa IDs, il numero totale di tag e una colonna per ogni chiave di tag univoca della raccolta. Il file.csv può aiutarvi a sviluppare una strategia di etichettatura per le risorse dell'organizzazione o a determinare dove vi siano sovrapposizioni o incongruenze nell'assegnazione dei tag tra le risorse.

1. Nei risultati della query Find resources to tag (Trova risorse per tag), selezionare Export resources to CSV (Esporta le risorse in un CSV).
2. Quando ti viene richiesto dal browser, scegli di aprire il file.csv o di salvarlo in una posizione comoda.

Gestione dei tag con Tag Editor

Dopo aver trovato le risorse che desideri taggare, puoi aggiungere, rimuovere e modificare i tag per alcuni o tutti i risultati di ricerca. Tag Editor mostra tutti i tag associati alle risorse. Mostra anche se quei tag sono stati aggiunti in Tag Editor, dalla console di servizio della risorsa o utilizzando l'API.

Important

Non memorizzare informazioni personali identificabili 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.

Altri modi per gestire i tag

In questo argomento viene illustrato come etichettare le risorse utilizzando Tag Editor in. AWS Management Console Tuttavia, puoi anche gestire i tag sulle tue AWS risorse utilizzando i seguenti strumenti:

- È possibile digitare o eseguire script di comandi al prompt della shell utilizzando i `resourcegroupstaggingapi`comandi contenuti in AWS Command Line Interface (AWS CLI).
- È possibile creare ed eseguire PowerShell script utilizzando l'API di AWS Resource Groups tagging in. AWS Tools for PowerShell Core
- È possibile creare ed eseguire programmi con uno qualsiasi dei tag disponibili AWS SDKsutilizzando i tag dei gruppi di risorse APIs, come i tag per APIs Python o i tag per Java. APIs

Quando aggiungi, rimuovi o modifichi tag esistenti, stai modificando i tag solo per le risorse selezionate nei risultati della tua query Trova risorse per taggare. È possibile selezionare fino a 500 risorse su cui gestire i tag.

Aggiungi tag alle risorse selezionate

È possibile utilizzare Tag Editor per aggiungere tag alle risorse selezionate che sono i risultati delle query Find resources to tag (Trova risorse per tag).

> **Note**
>
> Questo argomento descrive come modificare in blocco i tag per più risorse. Puoi anche modificare i valori dei tag per una singola risorsa. Per ulteriori informazioni, consulta Visualizza e modifica i tag esistenti per una risorsa selezionata.

1. Apri la console Tag Editor e invia una query che restituisca più risorse a cui desideri taggare.
2. Nella tabella dei risultati della query Trova risorse a cui etichettare, seleziona le caselle di controllo accanto alle risorse a cui desideri aggiungere i tag. Inserisci una stringa di testo in Filtra risorse nella parte superiore della tabella per filtrare parte del nome, dell'ID, delle chiavi dei tag o dei valori dei tag di una risorsa. Nella colonna Tag, notare se le risorse nei risultati hanno già i tag applicati.
3. Seleziona la casella di controllo per una o più risorse, quindi scegli Gestisci i tag delle risorse selezionate.
4. Nella pagina Manage tags (Gestisci i tag), visualizzare i tag per le risorse selezionate. Sebbene la query originale abbia restituito più risorse, stai aggiungendo tag solo alle risorse selezionate nel passaggio 1. Seleziona Aggiungi tag.
5. Inserire una chiave tag e un valore di tag opzionale. Per questa procedura, aggiungerai la chiave del tag **`Team`** e il valore del tag**`Development`**.

   > **Note**
   >
   > Una risorsa può avere un massimo di 50 tag applicati dall'utente. Potresti non essere in grado di aggiungere nuovi tag a una risorsa se ti avvicini a 50 tag applicati dall'utente. AWS i tag generati non si applicano al limite di 50 tag. Le chiavi dei tag devono essere univoche all'interno delle risorse selezionate. Non puoi aggiungere un nuovo tag con una chiave che corrisponde a una chiave di tag già esistente nelle risorse selezionate.

6. Quando hai finito di aggiungere i tag, scegli Rivedi e applica le modifiche.
7. Se si accettano le modifiche, scegliere Apply changes to all selected (Applica le modifiche a tutte le risorse selezionate).
8. A seconda del numero di risorse selezionate, l'applicazione di nuovi tag può richiedere alcuni minuti. Non uscite dalla pagina e non aprite una pagina diversa nella stessa scheda del browser. Se le modifiche hanno esito positivo, viene visualizzato un banner verde nella parte superiore

della pagina. Attendere l'apparizione del banner per esito positivo o negativo sulla pagina prima di continuare.

Se le modifiche ai tag apportate ad alcune o a tutte le risorse non hanno avuto esito positivo, consulta Risoluzione dei problemi relativi alle modifiche ai tag. Dopo aver risolto le modifiche ai tag non riuscite (ad esempio autorizzazioni insufficienti), puoi riprovare a modificare i tag sulle risorse per le quali le modifiche ai tag non sono riuscite. Per ulteriori informazioni, consulta the section called "Riprova le modifiche ai tag non riuscite".

Modifica i tag delle risorse selezionate

È possibile utilizzare Tag Editor per modificare i valori di tag esistenti sulle risorse selezionate che sono i risultati della query Find resources to tag (Trova risorse per tag). La modifica di un tag cambia il valore del tag su tutte le risorse selezionate con la stessa chiave tag. Non puoi rinominare una chiave di tag, ma puoi eliminare un tag e creare un tag con un nuovo nome per sostituire la chiave di tag originale. Ciò elimina tutti i tag con tale chiave sulle risorse selezionate.

> **Important**
>
> Non memorizzare informazioni personali identificabili 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.

1. Nei risultati della query Find resources to tag Trova risorse per tag, selezionare le caselle di controllo accanto alle risorse per cui si desidera modificare i tag esistenti. Inserire una stringa di testo in Filter resources (Filtra risorse) per filtrare parte di un nome o di un ID della risorsa. Nella colonna Tag, notare se le risorse nei risultati hanno già i tag applicati.
2. Scegli Gestisci i tag delle risorse selezionate.
3. Nella pagina Manage tags (Gestisci tag), in Edit tags of selected resources (Modifica tag delle risorse selezionate), visualizzare i tag sulla risorsa selezionata. Sebbene la tua query originale possa aver restituito più risorse, stai modificando i tag solo per le risorse selezionate nel passaggio 1.
4. Modificare, aggiungere o eliminare valori di tag. I tag esistenti devono avere una chiave tag, ma i valori dei tag sono facoltativi.

   In questa procedura, modifichiamo il valore del **`Team`** tag in**`QA`**.

Se le risorse della selezione hanno valori diversi per la stessa chiave, nel campo Valore tag viene visualizzato il messaggio Risorse selezionate con valori di tag diversi. In questo caso, posizionando il cursore nella casella si apre un elenco a discesa di tutti i valori disponibili per questa chiave di tag nelle risorse selezionate.

Se le risorse nella selezione hanno il valore di tag desiderato, il valore di tag viene evidenziato durante la digitazione. Ad esempio, se le risorse nella tua selezione hanno già il valore del tag **QA**, il valore viene evidenziato mentre si digita **Q**. I valori nell'elenco a discesa aiutano a mantenere coerenti i valori dei tag tra le risorse. Il valore del tag viene modificato su tutte le risorse selezionate. In questo esempio, il valore de tag viene modificato in **QA** per tutte le risorse selezionate che avevano una chiave tag **Team**. Per le risorse selezionate che non hanno il **Team** tag, **QA** viene aggiunto il **Team** tag con il valore.

5. Quando hai finito di modificare i tag, scegli Rivedi e applica le modifiche.
6. Se si accettano le modifiche, scegliere Apply changes to all selected (Applica le modifiche a tutte le risorse selezionate).
7. A seconda del numero di risorse selezionate, modificare i tag può richiedere alcuni minuti. Non uscite dalla pagina e non aprite una pagina diversa nella stessa scheda del browser. Se le modifiche hanno esito positivo, viene visualizzato un banner verde nella parte superiore della pagina. Attendere l'apparizione del banner per esito positivo o negativo sulla pagina prima di continuare.

   Se le modifiche ai tag apportate ad alcune o a tutte le risorse non hanno avuto esito positivo, consulta Risoluzione dei problemi relativi alle modifiche ai tag. Dopo aver risolto le cause principali delle modifiche ai tag non riuscite (ad esempio autorizzazioni insufficienti), puoi riprovare a modificare i tag sulle risorse per le quali le modifiche ai tag non sono riuscite. Per ulteriori informazioni, consulta the section called "Riprova le modifiche ai tag non riuscite".

Rimuovi i tag dalle risorse selezionate

È possibile utilizzare Tag Editor per rimuovere i tag dalle risorse selezionate che sono nei risultati della query Find resources to tag (Trova risorse per tag). La rimozione di un tag elimina il tag da tutte le risorse selezionate con il tag. Poiché non puoi modificare le chiavi dei tag, puoi rimuovere i tag e sostituirli con nuovi tag se devi modificare una chiave di tag. Ciò elimina tutti i tag con tale chiave sulle risorse selezionate.

1. Nei risultati della query Find resources to tag (Trova risorse per tag), selezionare le caselle di controllo accanto alle risorse da cui si desidera rimuovere i tag. Inserire una stringa di testo in Filter resources (Filtra risorse) per filtrare parte di un nome o di un ID della risorsa.
2. Scegli Gestisci i tag delle risorse selezionate.
3. Nella pagina Manage tags (Gestisci tag), in Edit tags of selected resources (Modifica tag delle risorse selezionate), visualizzare i tag per le risorse selezionate. Anche se la query originale potrebbe aver restituito più risorse, stai modificando i tag solo per le risorse selezionate nel passaggio 1.
4. Scegliere Remove tag (Rimuovi tag) per visualizzare tutti i tag che si desidera eliminare. In questa procedura, rimuoviamo il **`Team`** tag.

   > **Note**
   >
   > Scegliendo Remove tag (Rimuovi tag) si rimuove un tag da tutte le risorse selezionate che hanno tale tag.

5. Sceglieree Review and apply changes (Rivedi e applica modifiche).
6. Nella pagina di conferma, scegliere Apply changes to all selected (Applica le modifiche a tutte le risorse selezionate).
7. A seconda del numero di risorse selezionate, la rimozione di tag può richiedere alcuni minuti. Non uscite dalla pagina e non aprite una pagina diversa nella stessa scheda del browser. Se le modifiche hanno esito positivo, viene visualizzato un banner verde nella parte superiore della pagina. Attendere l'apparizione del banner per esito positivo o negativo sulla pagina prima di continuare.

   Se le modifiche dei tag per alcune o tutte le risorse non hanno esito positivo, consulta la sezione Risoluzione dei problemi relativi alle modifiche dei tag. Dopo aver risolto le cause principali delle modifiche ai tag non riuscite (ad esempio autorizzazioni insufficienti), puoi riprovare a modificare i tag sulle risorse per le quali la modifica dei tag non è riuscita. Per ulteriori informazioni, consulta the section called "Riprova le modifiche ai tag non riuscite".

Utilizzo dei tag nelle politiche di autorizzazione IAM

AWS Identity and Access Management (IAM) è Servizio AWS quello che usi per creare e gestire le politiche di autorizzazione che determinano chi può accedere alle tue AWS risorse. Ogni tentativo di accedere a un AWS servizio o di leggere o scrivere una AWS risorsa è un accesso controllato da una policy IAM.

Queste politiche ti consentono di fornire un accesso granulare alle tue risorse. Una delle funzionalità che puoi utilizzare per ottimizzare questo accesso è l'`Condition`elemento della politica. Questo elemento consente di specificare le condizioni che devono soddisfare la richiesta per determinare se la richiesta può procedere. Tra le cose che puoi verificare con l'`Condition`elemento ci sono le seguenti:

- Tag allegati all'utente o al ruolo che effettua la richiesta.
- Tag allegati alla risorsa oggetto della richiesta.

Tag e controllo degli accessi basato sugli attributi

I tag possono essere una parte importante della strategia di controllo degli AWS accessi. Per informazioni sull'utilizzo dei tag come attributi in una strategia di controllo degli accessi basata sugli attributi (ABAC), consulta Controlling access to AWS resources using tags e Controlling access to e for IAM users and roles using tags, entrambi nella IAM User Guide.

Un tutorial completo che mostra come concedere l'accesso a diversi progetti e gruppi utilizzando i tag è disponibile su IAM tutorial: Definisci le autorizzazioni per accedere alle AWS risorse in base ai tag nella Guida per l'utente.AWS Identity and Access Management

Se utilizzi un provider di identità (IdP) basato su SAML per l'accesso singolo, puoi allegare tag ai ruoli presunti che forniscono l'accesso ai tuoi utenti. Per ulteriori informazioni, consulta il tutorial IAM: Usa i tag di sessione SAML per ABAC nella Guida per l'utente.AWS Identity and Access Management

Chiavi di condizione relative ai tag

La tabella seguente descrive le chiavi di condizione che è possibile utilizzare in una politica di autorizzazioni IAM per controllare l'accesso in base ai tag. Queste chiavi condizionali consentono di eseguire le seguenti operazioni:

- Confrontate i tag sul principale che chiama l'operazione.
- Confrontate i tag forniti all'operazione come parametro.
- Confronta i tag allegati alla risorsa a cui l'operazione accederebbe.

Per i dettagli completi su una chiave di condizione e su come utilizzarla, consulta la pagina collegata nella colonna Nome chiave di condizione.

Nome della chiave di condizione	Descrizione
aws:PrincipalTag	Confronta il tag allegato al principale (ruolo o utente IAM) che effettua la richiesta con il tag specificato nella policy.
aws:RequestTag	Confronta la coppia chiave-valore del tag che è stata passata alla richiesta come parametro con la coppia chiave-valore del tag specificata nella policy.
aws:ResourceTag	Confronta la coppia chiave-valore associata alla risorsa con la coppia chiave-valore del tag specificata nella politica.
aws:TagKeys	Confronta solo le chiavi dei tag nella richiesta con le chiavi specificate nella politica.

Esempi di politiche IAM che utilizzano tag

Example Esempio 1: obbliga gli utenti ad allegare un tag specifico quando creano una risorsa

L'esempio seguente di policy di autorizzazione IAM mostra come forzare l'utente che crea o modifica i tag di una policy IAM a includere un tag nella chiave. `Owner` Inoltre, la policy richiede che il valore del tag sia impostato sullo stesso valore del `Owner` tag attualmente associato al principale chiamante. Affinché questa strategia funzioni, è necessario che a tutti i principali sia associato un `Owner` tag e che agli utenti sia impedito di modificare tale tag. Se si tenta di creare o modificare una policy senza includere il `Owner` tag, la policy non corrisponde e l'operazione non è consentita.

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

```
        {
            "Sid": "TagCustomerManagedPolicies",
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy",
                "iam:TagPolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:policy/*",
            "Condition": {
                "StringEquals": {"aws:RequestTag/Owner": "${aws:PrincipalTag/Owner}"}
            }
        }
    ]
}
```

Example Esempio 2: utilizza i tag per limitare l'accesso a una risorsa al suo «proprietario»

Il seguente esempio di policy di autorizzazione IAM consente all'utente di interrompere un' EC2istanza Amazon in esecuzione solo se il principale chiamante è etichettato con lo stesso valore di `project` tag dell'istanza.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances"
      ],
      "Resource": [
        "arn:aws:iam::123456789012:instance/*"
      ],
      "Condition": {
        "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/project}"}
      }
    }
  ]
}
```

Questo esempio è un esempio di controllo degli accessi basato sugli attributi (ABAC). Per ulteriori informazioni ed esempi aggiuntivi sull'utilizzo delle policy IAM per implementare una strategia di

controllo degli accessi basata su tag, consulta i seguenti argomenti nella Guida per l'utente:AWS Identity and Access Management

- Controllo dell'accesso alle AWS risorse tramite tag
- Controllo dell'accesso a e per utenti e ruoli IAM tramite tag
- Tutorial IAM: Definisci le autorizzazioni per accedere alle AWS risorse in base ai tag: mostra come concedere l'accesso a diversi progetti e gruppi utilizzando più tag.

AWS Organizations politiche di tag

Una politica sui tag è un tipo di politica che crei in AWS Organizations. Puoi utilizzare le politiche sui tag per standardizzare i tag tra le risorse degli account della tua organizzazione. Per utilizzare le politiche sui tag, ti consigliamo di seguire i flussi di lavoro descritti in Guida introduttiva alle politiche sui tag nella Guida per l'AWS Organizations utente. Come indicato in quella pagina, i flussi di lavoro consigliati includono la ricerca e la correzione di tag non conformi. Per eseguire queste attività, si utilizza la console Tag Editor.

Prerequisiti e autorizzazioni

Prima di poter valutare la conformità alle politiche sui tag in Tag Editor, è necessario soddisfare i requisiti e impostare le autorizzazioni necessarie.

Argomenti

Prerequisiti per valutare la conformità alle politiche sui tag

La valutazione della conformità alle politiche sui tag richiede quanto segue:

- È innanzitutto necessario abilitare la funzionalità e creare e allegare politiche sui tag. AWS Organizations Per ulteriori informazioni, consulta le seguenti pagine della Guida AWS Organizations per l'utente:
  - Prerequisiti e autorizzazioni per la gestione delle politiche relative ai tag
  - Abilitazione delle politiche relative ai tag
  - Guida introduttiva alle politiche sui tag
- Per trovare tag non conformi nelle risorse di un account, sono necessarie le credenziali di accesso per quell'account e le autorizzazioni elencate in. Autorizzazioni per la valutazione della conformità di un account
- Per valutare la conformità a livello di organizzazione, sono necessarie le credenziali di accesso per l'account di gestione dell'organizzazione e le autorizzazioni elencate in. Autorizzazioni per la

valutazione della conformità a livello di organizzazione Puoi richiedere il rapporto di conformità solo dagli Regione AWS Stati Uniti orientali (Virginia settentrionale).

Autorizzazioni per la valutazione della conformità di un account

La ricerca di tag non conformi nelle risorse di un account richiede le seguenti autorizzazioni:

- `organizations:DescribeEffectivePolicy`— Per ottenere i contenuti della politica di tag efficace per l'account.
- `tag:GetResources`— Per ottenere un elenco di risorse che non rispettano la politica sui tag allegata.
- `tag:TagResources`— Per aggiungere o aggiornare i tag. Sono inoltre necessarie autorizzazioni specifiche del servizio per creare tag. Ad esempio, per etichettare le risorse in Amazon Elastic Compute Cloud (Amazon EC2), sono necessarie le autorizzazioni per. `ec2:CreateTags`
- `tag:UnTagResources`— Per rimuovere un tag. Sono inoltre necessarie le autorizzazioni specifiche del servizio per rimuovere i tag. Ad esempio, per rimuovere i tag dalle risorse in Amazon EC2, sono necessarie le autorizzazioni per. `ec2:DeleteTags`

La seguente policy di esempio AWS Identity and Access Management (IAM) fornisce le autorizzazioni per valutare la conformità dei tag per un account.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EvaluateAccountCompliance",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeEffectivePolicy",
                "tag:GetResources",
                "tag:TagResources",
                "tag:UnTagResources"
            ],
            "Resource": "*"
        }
    ]
}
```

Per ulteriori informazioni su policy e autorizzazioni IAM, consulta la Guida per l'utente di IAM.

Autorizzazioni per la valutazione della conformità a livello di organizzazione

La valutazione della conformità a livello di organizzazione alle politiche di tag richiede le seguenti autorizzazioni:

- `organizations:DescribeEffectivePolicy`— Per ottenere il contenuto della politica sui tag allegata all'organizzazione, all'unità organizzativa (OU) o all'account.
- `tag:GetComplianceSummary`— Per ottenere un riepilogo delle risorse non conformi in tutti gli account dell'organizzazione.
- `tag:StartReportCreation`— Per esportare i risultati della valutazione di conformità più recente in un file. La conformità a livello di organizzazione viene valutata ogni 48 ore.
- `tag:DescribeReportCreation`— Per verificare lo stato della creazione del report.
- `s3:ListAllMyBuckets`— Per facilitare l'accesso al rapporto di conformità a livello di organizzazione.
- `s3:GetBucketAcl`— Ispezionare l'Access Control List (ACL) del bucket Amazon S3 che riceve il rapporto di conformità.
- `s3:GetObject`— Per recuperare il rapporto di conformità dal bucket Amazon S3 di proprietà del servizio.
- `s3:PutObject`— Inserire il rapporto di conformità nel bucket Amazon S3 specificato.

Se il bucket Amazon S3 a cui viene consegnato il report è crittografato tramite SSE-KMS, devi disporre anche dell'autorizzazione per quel bucket. `kms:GenerateDataKey`

Il seguente esempio di policy IAM fornisce le autorizzazioni per valutare la conformità a livello di organizzazione. Sostituisci *`placeholder`* ognuna con le tue informazioni:

- *`bucket_name`*— Il nome del tuo bucket Amazon S3
- *`organization_id`*— L'ID della tua organizzazione

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

```
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeEffectivePolicy",
                "tag:StartReportCreation",
                "tag:DescribeReportCreation",
                "tag:GetComplianceSummary",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GetBucketAclForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                }
            }
        },
        {
            "Sid": "GetObjectForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::*/tag-policy-compliance-reports/*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                }
            }
        },
        {
            "Sid": "PutObjectForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/AwsTagPolicies/organization_id/*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                },
                "StringLike": {
                    "s3:x-amz-copy-source": "*/tag-policy-compliance-reports/*"
                }
```

```
            }
        }
    ]
}
```

Per ulteriori informazioni su policy e autorizzazioni IAM, consulta la Guida per l'utente di IAM.

Policy sui bucket Amazon S3 per l'archiviazione dei report

Per creare un report di conformità a livello di organizzazione, l'identità che usi per chiamare l'`StartReportCreation`API deve avere accesso a un bucket Amazon Simple Storage Service (Amazon S3) nella regione Stati Uniti orientali (Virginia settentrionale) per archiviare il rapporto. Tag Policies utilizza le credenziali dell'identità chiamante per inviare il report di conformità al bucket specificato.

Se il bucket e l'identità utilizzati per chiamare l'`StartReportCreation`API appartengono allo stesso account, non sono necessarie policy di bucket Amazon S3 aggiuntive per questo caso d'uso.

Se l'account associato all'identità utilizzata per chiamare l'`StartReportCreation`API è diverso dall'account proprietario del bucket Amazon S3, al bucket deve essere allegata la seguente policy relativa al bucket. Sostituisci ciascuno *`placeholder`* con le tue informazioni:

- *`bucket_name`*— Il nome del tuo bucket Amazon S3
- *`organization_id`*— L'ID della tua organizzazione
- *`identity_ARN`*— L'ARN dell'identità IAM utilizzato per chiamare l'API `StartReportCreation`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CrossAccountTagPolicyACL",
            "Effect": "Allow",
            "Principal": {
                "AWS": "identity_ARN"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name"
        },
        {
```

```
            "Sid": "CrossAccountTagPolicyBucketDelivery",
            "Effect": "Allow",
            "Principal": {
                "AWS": "identity_ARN"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/AwsTagPolicies/organization_id/*"
        }
    ]
}
```

Valutazione della conformità di un account

Puoi valutare la conformità di un account della tua organizzazione grazie alla sua efficace politica sui tag.

> **Important**
>
> Le risorse senza tag non appaiono nei risultati come non conformi.
> Per trovare risorse prive di tag nel tuo account, usale Esploratore di risorse AWS con una query che utilizza. **`tag:none`** Per ulteriori informazioni, consulta Cerca risorse senza tag nella Guida per l'utente.Esploratore di risorse AWS

La politica di etichettatura efficace specifica le regole di etichettatura che si applicano a un account. La politica di tag efficace è l'aggregazione di tutte le politiche sui tag ereditate dall'account, più qualsiasi politica di tag collegata direttamente all'account. Quando colleghi una policy di tag alla root dell'organizzazione, questa si applica a tutti gli account dell'organizzazione. Quando si allega una politica sui tag a un'unità organizzativa (OU), questa si applica a tutti gli account OUs che appartengono all'unità organizzativa.

> **Note**
>
> Se non hai ancora creato le politiche sui tag, consulta Guida introduttiva alle politiche sui tag nella Guida per l'AWS Organizations utente.

Per trovare tag non conformi, devi disporre delle seguenti autorizzazioni:

- `organizations:DescribeEffectivePolicy`
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`

Per valutare la conformità di un account alla sua politica di tag effettiva (console)

1. Dopo aver effettuato l'accesso all'account di cui desideri verificare la conformità, apri la console Tag Policies.
2. La sezione Politica di etichettatura effettiva mostra quando la policy è stata aggiornata l'ultima volta e le chiavi dei tag definite. È possibile espandere una chiave di tag per visualizzare informazioni sui suoi valori, sul trattamento dei casi e sull'eventuale applicazione dei valori per tipi di risorse specifici.

   > **Note**
   >
   > Se hai effettuato l'accesso all'account di gestione, devi scegliere un account per visualizzarne la politica efficace e visualizzare le informazioni sulla conformità.

3. Nella sezione Risorse con tag non conformi, specifica quali tag non conformi devono Regione AWS essere cercati. Facoltativamente, puoi anche cercare per tipo di risorsa. Quindi scegli Cerca risorse.

   I risultati in tempo reale vengono visualizzati nella sezione Risultati della ricerca. Per modificare il numero di risultati restituiti per pagina o le colonne da visualizzare, scegli l'icona delle impostazioni.
4. Nei risultati della ricerca, seleziona una risorsa con tag non conformi.
5. Nella finestra di dialogo che elenca i tag della risorsa, scegliete il collegamento ipertestuale per aprire il Servizio AWS luogo in cui è stata creata la risorsa. Da quella console, correggete il tag non conforme.

   > **Tip**
   >
   > Se non sei sicuro di quali tag non siano conformi, vai alla sezione Politica sui tag efficaci per l'account nella console Tag Policies. Puoi espandere una chiave di tag per visualizzarne le regole di etichettatura.

6. Ripeti il processo di ricerca e correzione dei tag finché le risorse dell'account che ti interessano non saranno conformi in ogni regione.

Per trovare tag non conformi (, API)AWS CLIAWS

Utilizza i comandi e le operazioni seguenti per trovare tag non conformi:

- AWS Command Line Interface (AWS CLI):
  - aws resourcegroupstaggingapi get-resources
  - aws resourcegroupstaggingapi tag-resources
  - aws resourcegroupstaggingapi untag-resources

  Per la procedura completa per l'utilizzo delle politiche relative ai tag in AWS CLI, vedere Utilizzo delle politiche relative ai tag nella Guida per l' AWS CLIAWS Organizations utente.
- AWS Resource Groups Tagging API:
  - GetResources
  - TagResources
  - UntagResources

Passaggi successivi

Ti consigliamo di ripetere il processo di individuazione e correzione dei problemi di conformità. Continua fino a quando le risorse dell'account che ti interessano non saranno conformi alla politica in materia di tag in vigore in ciascuna regione.

La ricerca e la correzione di tag non conformi è un processo iterativo per diversi motivi, tra cui i seguenti:

- L'uso delle politiche di tag da parte della tua organizzazione può evolversi nel tempo.
- Quando si creano risorse, è necessario del tempo per apportare cambiamenti all'interno dell'organizzazione.
- La conformità può cambiare ogni volta che viene creata una nuova risorsa o quando vengono assegnati nuovi tag a una risorsa.
- La politica di tag effettiva di un account viene aggiornata ogni volta che una politica sui tag viene allegata o rimossa dalla stessa. La politica sui tag effettiva viene inoltre aggiornata ogni volta che vengono apportate modifiche alle politiche di etichettatura ereditate dall'account.

Se hai effettuato l'accesso come account di gestione dell'organizzazione, puoi anche generare un rapporto. Questo rapporto mostra informazioni su tutte le risorse contrassegnate negli account dell'organizzazione. Per ulteriori informazioni, consulta Valutazione della conformità a livello di organizzazione.

Valutazione della conformità a livello di organizzazione

Puoi valutare la conformità della tua organizzazione con la sua efficace politica sui tag. Puoi generare un rapporto che elenchi tutte le risorse etichettate negli account dell'organizzazione e indichi se ciascuna risorsa è conforme alla politica di tag efficace.

> **Important**
>
> Le risorse senza tag non appaiono nei risultati come non conformi.
> Per trovare risorse senza tag nel tuo account, usale Esploratore di risorse AWS con una query che utilizza. **`tag:none`** Per ulteriori informazioni, consulta Cerca risorse senza tag nella Guida per l'utente.Esploratore di risorse AWS

Puoi generare il rapporto solo dall'account di gestione della tua organizzazione. `us-east-1` Regione AWS L'account che genera il report deve avere accesso a un bucket Amazon S3 nella regione Stati Uniti orientali (Virginia settentrionale). Il bucket deve avere una policy relativa ai bucket allegata, come illustrato nella policy del bucket di Amazon S3 per l'archiviazione dei report.

Per generare un rapporto di conformità a livello di organizzazione, devi disporre delle seguenti autorizzazioni:

- `organizations:DescribeEffectivePolicy`
- `tag:GetComplianceSummary`
- `tag:StartReportCreation`
- `tag:DescribeReportCreation`
- `s3:ListAllMyBuckets`
- `s3:GetBucketAcl`
- `s3:GetObject`
- `s3:PutObject`

Per un esempio di policy IAM che mostra queste autorizzazioni, consulta Autorizzazioni per valutare la conformità a livello di organizzazione.

Per generare un rapporto di conformità a livello di organizzazione (console)

1. Apri la console Tag Policies.
2. Scegli la scheda principale di Questa organizzazione e, nella parte inferiore della pagina, scegli Genera rapporto.
3. Nella schermata Genera rapporto, specifica dove archiviare il rapporto.
4. Scegli Inizia a esportare.

Quando il rapporto è completo, puoi scaricarlo dalla sezione Rapporto di non conformità nella scheda principale dell'organizzazione.

> **Note**
>
> La conformità a livello di organizzazione viene valutata ogni 48 ore. Ciò si traduce in quanto segue:
>
> - Possono essere necessarie fino a 48 ore prima che le modifiche alla politica o alle risorse relative ai tag vengano visualizzate nel rapporto di conformità a livello di organizzazione. Ad esempio, supponi di avere una policy di tag che definisce un nuovo tag standardizzato per un tipo di risorsa. Le risorse di quel tipo che non dispongono di questo tag possono essere visualizzate come conformi nel rapporto per un massimo di 48 ore.
> - Sebbene sia possibile generare il report in qualsiasi momento, i risultati del report non vengono aggiornati fino al completamento della valutazione successiva.
> - La NoncompliantKeyscolonna elenca le chiavi dei tag sulla risorsa che non sono conformi alla politica di tag effettiva.
> - La KeysWithNonCompliantValuescolonna elenca le chiavi definite nella politica effettiva che si trovano sulla risorsa con un trattamento dei casi errato o valori non conformi.
> - Se chiudi un account Account AWS che era membro dell'organizzazione, questo può continuare a comparire nel rapporto sulla conformità dei tag per un massimo di 90 giorni.

Per generare un rapporto di conformità a livello di organizzazione (API)AWS CLIAWS

Utilizza i seguenti comandi e operazioni per generare un rapporto di conformità a livello di organizzazione, verificarne lo stato e visualizzare il rapporto:

- AWS Command Line Interface AWS CLI):
  - aws resourcegroupstaggingapi start-report-creation
  - aws resourcegroupstaggingapi describe-report-creation
  - aws resourcegroupstaggingapi get-compliance-summary

  Per la procedura completa per l'utilizzo delle politiche relative ai tag in AWS CLI, vedere Utilizzo delle politiche relative ai tag nella Guida per l' AWS CLIAWS Organizations utente.
- AWS API:
  - StartReportCreation
  - DescribeReportCreation
  - GetComplianceSummary

Monitora le modifiche ai tag con flussi di lavoro serverless e Amazon EventBridge

Amazon EventBridge supporta la modifica dei tag sulle AWS risorse. Usando questo EventBridge tipo, puoi creare EventBridge regole per abbinare le modifiche ai tag e indirizzare gli eventi verso uno o più obiettivi. Ad esempio, un target potrebbe essere una AWS Lambda funzione per richiamare flussi di lavoro automatizzati. Questo argomento fornisce un tutorial sull'utilizzo di Lambda per creare una soluzione serverless economica per elaborare in modo sicuro le modifiche ai tag sulle risorse. AWS

Le modifiche ai tag generano eventi EventBridge

EventBridge offre un flusso quasi in tempo reale di eventi di sistema che descrivono i cambiamenti nelle AWS risorse. Molte AWS risorse supportano i tag, che sono attributi personalizzati e definiti dall'utente per organizzare e classificare AWS facilmente le risorse. I casi d'uso più comuni dei tag sono l'allocazione dei costi, la categorizzazione, il controllo degli accessi, la sicurezza e l'automazione.

Con EventBridge, puoi monitorare le modifiche ai tag e tenere traccia dello stato dei tag sulle risorse. AWS In precedenza, per ottenere funzionalità simili, era possibile eseguire continuamente il polling APIs e l'orchestrazione di più chiamate. Ora, qualsiasi modifica a un tag, inclusi il servizio individuale APIs, il Tag Editor e l'API di tagging, avvierà la modifica del tag sull'evento di risorsa. L'esempio seguente mostra un EventBridge evento tipico richiesto da una modifica del tag. Mostra le chiavi dei tag nuove, aggiornate o eliminate e i valori associati.

```
{
  "version": "0",
  "id": "bddcf1d6-0251-35a1-aab0-adc1fb47c11c",
  "detail-type": "Tag Change on Resource",
  "source": "aws.tag",
  "account": "123456789012",
  "time": "2018-09-18T20:41:38Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
```

```
    "changed-tag-keys": [
      "a-new-key",
      "an-updated-key",
      "a-deleted-key"
    ],
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added",
      "an-updated-key": "tag-value-was-just-changed",
      "an-unchanged-key": "tag-value-still-the-same"
    },
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
  }
}
```

Tutti EventBridge gli eventi hanno gli stessi campi di primo livello:

- versione: per impostazione predefinita, questo valore è impostato su `0` (zero) in tutti gli eventi.
- id — Viene generato un valore univoco per ogni evento. Questo può essere utile per tracciare gli eventi man mano che passano dalle regole alle destinazioni e vengono elaborati.
- detail-type: identifica, in combinazione con il `source` campo, i campi e i valori che appaiono nel campo di dettaglio.
- source: identifica il servizio che è stato l'origine dell'evento. La fonte per le modifiche ai tag è`aws.tag`.
- time: il timestamp dell'evento.
- regione: identifica il Regione AWS luogo in cui ha avuto origine l'evento.
- risorse: questo array JSON contiene Amazon Resource Names (ARNs) che identificano le risorse coinvolte nell'evento. Questa è la risorsa in cui i tag sono stati modificati.
- dettaglio — Un oggetto JSON, il cui contenuto è diverso a seconda del tipo di evento. Per la modifica dei tag sulla risorsa, sono inclusi i seguenti campi dettagliati:
  - changed-tag-keys— Le chiavi dei tag che sono state modificate da questo evento.
  - servizio: il servizio a cui appartiene la risorsa. In questo esempio, il servizio è `ec2` Amazon EC2.
  - resource-type: il tipo di risorsa del servizio. In questo esempio, si tratta di un' EC2istanza Amazon.
  - version: la versione del set di tag. La versione inizia da 1 e aumenta quando i tag vengono modificati. È possibile utilizzare la versione per verificare l'ordine degli eventi di modifica dei tag.

- tags: i tag allegati alla risorsa dopo la modifica.

Per ulteriori informazioni, consulta i modelli di EventBridge eventi di Amazon nella Amazon EventBridge User Guide.

Utilizzando EventBridge, puoi creare regole che corrispondono a modelli di eventi specifici in base ai diversi campi. Dimostriamo come farlo nel tutorial. Inoltre, mostriamo come un' EC2 istanza Amazon può essere interrotta automaticamente se un tag specificato non è associato all'istanza. Utilizziamo i EventBridge campi per creare un pattern che corrisponda agli eventi dei tag per l'istanza che avvia una funzione Lambda.

Lambda e serverless

AWS Lambda segue il paradigma serverless per eseguire codice nel cloud. Esegui il codice solo quando è necessario, senza pensare ai server. Paghi solo per il tempo di elaborazione esatto che utilizzi. Anche se si chiama serverless, ciò non significa che non ci siano server. In questo contesto, la modalità serverless significa che non è necessario fornire, configurare o gestire i server utilizzati per eseguire il codice. AWS fa tutto questo per te, così puoi concentrarti sul codice. Per ulteriori informazioni su Lambda, consulta la panoramica del AWS Lambda prodotto.

Tutorial: arresto automatico delle EC2 istanze Amazon prive dei tag obbligatori

Man mano che il tuo pool di AWS risorse e Account AWS quello che gestisci cresce, puoi utilizzare i tag per semplificare la categorizzazione delle tue risorse. I tag vengono comunemente utilizzati per casi d'uso critici come l'allocazione dei costi e la sicurezza. Per gestire efficacemente AWS le risorse, è necessario etichettarle in modo coerente. Spesso, quando una risorsa viene fornita, riceve tutti i tag appropriati. Tuttavia, un processo successivo può comportare una modifica dei tag che comporta un allontanamento dalla politica aziendale in materia di tag. Monitorando le modifiche ai tag, puoi individuare eventuali variazioni dei tag e rispondere immediatamente. In questo modo avrete maggiore fiducia nel fatto che i processi che dipendono dalla corretta categorizzazione delle risorse produrranno i risultati desiderati.

L'esempio seguente mostra come monitorare le modifiche ai tag sulle EC2 istanze Amazon per verificare che un'istanza specificata continui ad avere i tag richiesti. Se i tag dell'istanza cambiano e l'istanza non ha più i tag richiesti, viene richiamata una funzione Lambda per chiudere automaticamente l'istanza. Perché vorresti farlo? Garantisce che tutte le risorse siano etichettate in

base alla politica aziendale in materia di tag, per un'efficace allocazione dei costi o per poter contare su una sicurezza basata sul controllo degli accessi basato sugli attributi (ABAC).

> **Important**
>
> Ti consigliamo vivamente di eseguire questo tutorial in un account non di produzione in cui non sia possibile chiudere inavvertitamente istanze importanti.
> Il codice di esempio in questo tutorial limita intenzionalmente l'impatto di questo scenario solo alle istanze di un elenco di istanze. IDs È necessario aggiornare l'elenco con l'istanza IDs che si desidera chiudere per il test. Questo aiuta a evitare che tu possa chiudere accidentalmente tutte le istanze in una regione del tuo Account AWS.
> Dopo il test, assicurati che tutte le istanze siano etichettate in base alla strategia di tagging della tua azienda. Quindi, puoi rimuovere il codice che limita la funzione solo all'istanza nell' IDs elenco.

Questo esempio utilizza JavaScript e la versione 16.x di Node.js. L'esempio utilizza l' Account AWS ID di esempio 123456789012 e gli Regione AWS Stati Uniti orientali (Virginia settentrionale) (). `us-east-1` Sostituiscili con l'ID e la regione del tuo account di prova.

> **Note**
>
> Se la tua console utilizza una regione diversa come impostazione predefinita, assicurati di cambiare la regione che stai usando in questo tutorial ogni volta che cambi console. Una causa comune del fallimento di questo tutorial è che l'istanza e la funzione si trovano in due regioni diverse.

Se utilizzi una regione diversa da quella`us-east-1`, assicurati di modificare tutti i riferimenti nei seguenti esempi di codice nella regione scelta.

Argomenti

- Fase 1: Creazione della funzione Lambda
- Fase 2: Configura le autorizzazioni IAM richieste
- Fase 3. Esegui un test preliminare della tua funzione Lambda
- Fase 4. Crea la EventBridge regola che avvia la funzione
- Fase 5. Prova la soluzione completa

- Riepilogo del tutorial

Fase 1: Creazione della funzione Lambda

Creazione della funzione Lambda

1. Apri la console di gestione di AWS Lambda.
2. Scegli Crea funzione, quindi scegli Autore da zero.
3. Per Function name (Nome funzione), immettere **`AutoEC2Termination`**.
4. Per Runtime scegli Node.js 16.x.
5. Mantieni tutti gli altri campi ai valori predefiniti e scegli Crea funzione.
6. Nella scheda Codice della pagina dei `AutoEC2Termination` dettagli, apri il file index.js per visualizzarne il codice.
   - Se è aperta una scheda con index.js, puoi scegliere la casella di modifica in quella scheda per modificarne il codice.
   - Se una scheda con index.js non è aperta, fai un secondo clic sul file index.js nella cartella Auto EC2 Terminator nel pannello di navigazione. Quindi scegli Apri.
7. Nella scheda index.js, incolla il codice seguente nella casella dell'editor, sostituendo tutto ciò che è già presente.

   Sostituisci il valore `RegionToMonitor` con la regione in cui desideri eseguire questa funzione.

```
// Set the following line to specify which Region's instances you want to monitor
// Only instances in this Region are succesfully stopped on a match

const RegionToMonitor = "us-east-1"

// Specify the instance ARNs to check.
// This limits the function for safety to avoid the tutorial shutting down all
 instances in account
// The first ARN is a "dummy" that matches the test event you create in Step 3.
// Replace the second ARN with one that matches a real instance that you want to
 monitor and that you can
// safely stop

const InstanceList = [
    "i-0000000aaaaaaaaaa",
```

```
    "i-05db4466d02744f07"
];

// The tag key name and value that marks a "valid" instance. Instances in the
 previous list that
// do NOT have the following tag key and value are stopped by this function

const ValidKeyName = "valid-key";
const ValidKeyValue = "valid-value";

// Load and configure the AWS SDK
const AWS = require('aws-sdk');
// Set the AWS Region
AWS.config.update({region: RegionToMonitor});
// Create EC2 service object.
const ec2 = new AWS.EC2({apiVersion: '2016-11-15'});

exports.handler = (event, context, callback) => {

  // Retrieve the details of the reported event.
  var detail = event.detail;
  var tags = detail["tags"];
  var service = detail["service"];
  var resourceType = detail["resource-type"];
  var resource = event.resources[0];
  var resourceSplit = resource.split("/");
  var instanceId = resourceSplit[resourceSplit.length - 1];

  // If this event is not for an EC2 resource, then do nothing.
  if (!(service === "ec2")) {
    console.log("Event not for correct service -- no action (", service, ")" );
    return;
  }

  // If this event is not about an instance, then do nothing.
  if (!(resourceType === "instance")) {
    console.log("Event not for correct resource type -- no action (", resourceType,
 ")" );
    return;
  }

  // CAUTION - Removing the following 'if' statement causes the function to run
 against
```

```
 //           every EC2 instance in the specified Region in the calling Account
AWS.
 //           If you do this and an instance is not tagged with the approved tag
key
 //           and value, this function stops that instance.

 // If this event is not for the ARN of an instance in our include list, then do
nothing.
 if (InstanceList.indexOf(instanceId)<0) {
   console.log("Event not for one of the monitored instances -- no action (",
resource, ")");
   return;
 }

 console.log("Tags changed on monitored EC2 instance (",instanceId,")");

 // Check attached tags for expected tag key and value pair
 if ( tags.hasOwnProperty(ValidKeyName) && tags[ValidKeyName] == "valid-value"){
   // Required tags ARE present
   console.log("The instance has the required tag key and value -- no action");
   callback(null, "no action");
   return;
 }

 // Required tags NOT present
 console.log("This instance is missing the required tag key or value -- attempting
to stop the instance");

 var params = {
   InstanceIds: [instanceId],
   DryRun: true
 };

 // call EC2 to stop the selected instances
 ec2.stopInstances(params, function(err, data) {
   if (err && err.code === 'DryRunOperation') {
     // dryrun succeeded, so proceed with "real" stop operation
     params.DryRun = false;
     ec2.stopInstances(params, function(err, data) {
       if (err) {
         console.log("Failed to stop instance");
         callback(err, "fail");
       } else if (data) {
         console.log("Successfully stopped instance", data.StoppingInstances);
```

```
          callback(null, "Success");
        }
      });
    } else {
      console.log("Dryrun attempt failed");
      callback(err);
    }
  });
};
```

8. Scegli Deploy per salvare le modifiche e rendere attiva la nuova versione della funzione.

Questa funzione Lambda controlla i tag di EC2 un'istanza Amazon, come riportato dall'evento di modifica del tag in. EventBridge In questo esempio, se all'istanza dell'evento manca la chiave di tag richiesta `valid-key` o se il tag non ha il valore`valid-value`, la funzione tenta di fermare l'istanza. È possibile modificare questo controllo logico o i requisiti dei tag per i propri casi d'uso specifici.

Tieni aperta la finestra della console Lambda nel browser.

Fase 2: Configura le autorizzazioni IAM richieste

Prima che la funzione possa essere eseguita correttamente, è necessario concedere alla funzione l'autorizzazione per interrompere un' EC2 istanza. Il ruolo AWS fornito lambda_basic_executionnon dispone di tale autorizzazione. In questo tutorial, modifichi la politica di autorizzazione IAM predefinita allegata al ruolo di esecuzione della funzione denominato`AutoEC2Termination-role-`*`uniqueid`*. L'autorizzazione aggiuntiva minima richiesta per questo tutorial è`ec2:StopInstances`.

Per ulteriori informazioni sulla creazione di policy IAM EC2 specifiche per Amazon, consulta Amazon EC2: consente l'avvio o l'arresto di un' EC2 istanza e la modifica di un gruppo di sicurezza, a livello di codice e nella console nella IAM User Guide.

Per creare una policy di autorizzazione IAM e collegarla al ruolo di esecuzione della funzione Lambda

1. In un'altra scheda o finestra del browser, apri la pagina Ruoli della console IAM.
2. Inizia a digitare il nome del ruolo e**`AutoEC2Termination`**, quando appare nell'elenco, scegli il nome del ruolo.
3. Nella pagina di riepilogo del ruolo, scegli la scheda Autorizzazioni e scegli il nome dell'unica politica già allegata.
4. Nella pagina di riepilogo della politica, scegli Modifica politica.

5. Nella scheda Visual Editor, scegli Aggiungi autorizzazioni aggiuntive.
6. Per Service (Servizio), scegliere EC2.
7. Per Azioni, scegli StopInstances. Puoi digitare **`Stop`** nella barra di ricerca e quindi scegliere `StopInstances` quando visualizzare.
8. Per Risorse, scegli Tutte le risorse, scegli Rivedi politica, quindi scegli Salva modifiche.

   Ciò crea automaticamente una nuova versione della politica e imposta quella versione come predefinita.

   La politica finale dovrebbe essere simile all'esempio seguente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:StopInstances",
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "logs:CreateLogGroup",
            "Resource": "arn:aws:logs:us-east-1:123456789012:*"
        },
        {
            "Sid": "VisualEditor2",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:us-east-1:123456789012:log-group:/aws/lambda/
AutoEC2Termination:*"
        }
    ]
}
```

Fase 3. Esegui un test preliminare della tua funzione Lambda

In questo passaggio, invii un evento di test alla tua funzione. La funzionalità di test Lambda funziona inviando un evento di test fornito manualmente. La funzione elabora l'evento di test come se l'evento provenisse da. EventBridge È possibile definire più eventi di test con valori diversi per esercitare tutte le diverse parti del codice. In questo passaggio, invii un evento di test che indica che i tag di un' EC2istanza Amazon sono cambiati e che i nuovi tag non includono la chiave e il valore del tag richiesti.

Per testare la tua funzione Lambda

1. Torna alla finestra o alla scheda con la console Lambda e apri la scheda Test per la tua funzione di EC2 terminazione automatica.
2. Scegli Crea nuovo evento.
3. Per Event name (Nome evento) immettere **`SampleBadTagChangeEvent`**.
4. Nell'Event JSON, sostituisci il testo con l'evento di esempio mostrato nel seguente testo di esempio. Non è necessario modificare gli account, la regione o l'ID dell'istanza affinché questo evento di test funzioni correttamente.

```
{
  "version": "0",
  "id": "bddcf1d6-0251-35a1-aab0-adc1fb47c11c",
  "detail-type": "Tag Change on Resource",
  "source": "aws.tag",
  "account": "123456789012",
  "time": "2018-09-18T20:41:38Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "valid-key"
    ],
    "tags": {
      "valid-key": "NOT-valid-value"
    },
    "service": "ec2",
    "resource-type": "instance",
    "version": 3
```

```
  }
}
```

5. Scegli Save (Salva), quindi Test .

   Il test sembra fallire, ma va bene.

   Dovresti vedere il seguente errore nella scheda Risultati dell'esecuzione in Risposta.

```
{
  "errorType": "InvalidInstanceID.NotFound",
  "errorMessage": "The instance ID 'i-0000000aaaaaaaaaa' does not exist",
  ...
}
```

   L'errore si verifica perché l'istanza specificata nell'evento di test non esiste.

   Le informazioni nella scheda Risultati di esecuzione, nella sezione Registri delle funzioni, dimostrano che la funzione Lambda ha tentato con successo di arrestare un'istanza. EC2 Tuttavia, non è riuscita perché inizialmente il codice tenta un'DryRunoperazione per arrestare l'istanza, il che indica che l'ID dell'istanza non era valido.

```
START RequestId: 390c1f8d-0d9b-4b44-b087-8de64479ab44 Version: $LATEST
2022-11-30T20:17:30.427Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    Tags
 changed on monitored EC2 instance ( i-0000000aaaaaaaaaa )
2022-11-30T20:17:30.427Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    This
 instance is missing the required tag key or value -- attempting to stop the
 instance
2022-11-30T20:17:31.206Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    Dryrun
 attempt failed
2022-11-30T20:17:31.207Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    ERROR   Invoke
 Error     {"errorType":"InvalidInstanceID.NotFound","errorMessage":"The instance
 ID 'i-0000000aaaaaaaaaa' does not
 exist","code":"InvalidInstanceID.NotFound","message":"The instance ID
 'i-0000000aaaaaaaaaa' does not
 exist","time":"2022-11-30T20:17:31.205Z","requestId":"a5192c3b-142d-4cec-
bdbc-685a9b7c7abf","statusCode":400,"retryable":false,"retryDelay":36.87870631147607,"stack
["InvalidInstanceID.NotFound: The instance ID 'i-0000000aaaaaaaaaa' does
 not exist","    at Request.extractError (/var/runtime/node_modules/aws-sdk/
lib/services/ec2.js:50:35)","    at Request.callListeners (/var/runtime/
node_modules/aws-sdk/lib/sequential_executor.js:106:20)","    at Request.emit
 (/var/runtime/node_modules/aws-sdk/lib/sequential_executor.js:78:10)","    at
```

```
 Request.emit (/var/runtime/node_modules/aws-sdk/lib/request.js:686:14)","    at
 Request.transition (/var/runtime/node_modules/aws-sdk/lib/request.js:22:10)","
    at AcceptorStateMachine.runTo (/var/runtime/node_modules/aws-sdk/lib/
state_machine.js:14:12)","    at /var/runtime/node_modules/aws-sdk/lib/
state_machine.js:26:10","    at Request.<anonymous> (/var/runtime/node_modules/aws-
sdk/lib/request.js:38:9)","    at Request.<anonymous> (/var/runtime/node_modules/
aws-sdk/lib/request.js:688:12)","    at Request.callListeners (/var/runtime/
node_modules/aws-sdk/lib/sequential_executor.js:116:18)"]}
END RequestId: 390c1f8d-0d9b-4b44-b087-8de64479ab44
```

6. Per dimostrare che il codice non tenta di interrompere l'istanza quando viene utilizzato il tag corretto, puoi creare e inviare un altro evento di test.

   Scegli la scheda Test sopra Code source. La console mostra l'evento SampleBadTagChangeEventdi test esistente.

7. Scegli Crea nuovo evento.
8. In Event Name (Nome evento), digitare **`SampleGoodTagChangeEvent`**.
9. Nella riga 17, elimina **`NOT-`** per modificare il valore in**`valid-value`**.
10. Nella parte superiore della finestra dell'evento Test, scegli Salva, quindi scegli Test.

    L'output mostra quanto segue, a dimostrazione del fatto che la funzione riconosce il tag valido e non tenta di chiudere l'istanza.

```
START RequestId: 53631a49-2b54-42fe-bf61-85b9e91e86c4 Version: $LATEST
2022-12-01T23:24:12.244Z    53631a49-2b54-42fe-bf61-85b9e91e86c4    INFO    Tags
 changed on monitored EC2 instance ( i-0000000aaaaaaaaaa )
2022-12-01T23:24:12.244Z    53631a49-2b54-42fe-bf61-85b9e91e86c4    INFO    The
 instance has the required tag key and value -- no action
END RequestId: 53631a49-2b54-42fe-bf61-85b9e91e86c4
```

    Tieni la console Lambda aperta nel browser.

Fase 4. Crea la EventBridge regola che avvia la funzione

Ora puoi creare una EventBridge regola che corrisponda all'evento e punti alla tua funzione Lambda.

Per creare la regola EventBridge

1. In un'altra scheda o finestra del browser, apri la EventBridge console nella pagina Crea regola.

2. Per Nome, immettete**`ec2-instance-rule`**, quindi scegliete Avanti.
3. Scorri verso il basso fino a Metodo di creazione e scegli Modello personalizzato (editor JSON).
4. Nella casella di modifica, incolla il seguente testo del pattern, quindi scegli Avanti.

```
{
  "source": [
    "aws.tag"
  ],
  "detail-type": [
    "Tag Change on Resource"
  ],
  "detail": {
    "service": [
      "ec2"
    ],
    "resource-type": [
      "instance"
    ]
  }
}
```

   Questa regola corrisponde `Tag Change on Resource` agli eventi per EC2 le istanze Amazon e richiama ciò che specifichi come Target nel passaggio successivo.
5. Quindi, aggiungi la tua funzione Lambda come destinazione. Nella casella Target 1, in Seleziona una destinazione, scegli la funzione Lambda.
6. In Funzione, scegliete la funzione di EC2terminazione automatica creata in precedenza, quindi scegliete Avanti.
7. Nella pagina Configura tag, scegli Avanti. Quindi, nella pagina Rivedi e crea, scegli Crea regola. Ciò concede inoltre automaticamente il permesso di EventBridge richiamare la funzione Lambda specificata.

Fase 5. Prova la soluzione completa

Puoi testare il risultato finale creando un' EC2 istanza e osservando cosa succede quando ne modifichi i tag.

Per testare la soluzione di monitoraggio con un'istanza reale

1. Apri la EC2console Amazon alla pagina Istanze.
2. Crea un' EC2 istanza Amazon. Prima di avviarla, allega un tag con la chiave `valid-key` e il valore`valid-value`. Per informazioni su come creare e avviare un'istanza, consulta la Fase 1: Avvio di un'istanza nella Amazon EC2 User Guide. Nella procedura Per avviare un'istanza, nel passaggio 3, in cui inserisci il tag Name, scegli anche Aggiungi tag aggiuntivi, scegli Aggiungi tag e quindi inserisci la chiave **`valid-key`** e il valore di**`valid-value`**. Puoi procedere senza una key pair se questa istanza è destinata esclusivamente agli scopi di questo tutorial e prevedi di eliminarla dopo averla completata. Torna a questo tutorial quando raggiungi la fine del passaggio 1; non è necessario eseguire il passaggio 2: Connect alla tua istanza.
3. Copia il file InstanceIddalla console.
4. Passa dalla EC2 console Amazon alla console Lambda. Scegli la funzione di EC2terminazione automatica, scegli la scheda Codice, quindi scegli la scheda index.js per modificare il codice.
5. Modifica la seconda voce `InstanceList` incollando il valore che hai copiato dalla console Amazon EC2 . Assicurati che il `RegionToMonitor` valore corrisponda alla regione che contiene l'istanza che hai incollato.
6. Scegli Deploy per rendere attive le modifiche. La funzione è ora pronta per essere attivata modificando i tag in quell'istanza nella regione specificata.
7. Passa dalla console Lambda alla console Amazon EC2 .
8. Modifica i tag allegati all'istanza eliminando il tag valid-key o modificando il valore di quella chiave.

   > **Note**
   >
   > Per informazioni su come modificare i tag su un' EC2istanza Amazon in esecuzione, consulta Aggiungere ed eliminare tag su una singola risorsa nella Amazon EC2 User Guide.

9. Attendi qualche secondo, quindi aggiorna la console. L'istanza dovrebbe cambiare lo stato dell'istanza in Arresto e quindi in Arrestato.
10. Passa dalla EC2 console Amazon alla console Lambda con la tua funzione e scegli la scheda Monitor.
11. Scegli la scheda Registri e, nella tabella Richiamazioni recenti, scegli la voce più recente nella colonna. LogStream

La CloudWatch console Amazon si apre sulla pagina Log events per l'ultima chiamata della funzione Lambda. L'ultima voce dovrebbe essere simile all'esempio seguente.

```
2022-11-30T12:03:57.544-08:00    START RequestId: b5befd18-2c41-43c8-
a320-3a4b2317cdac Version: $LATEST
2022-11-30T12:03:57.548-08:00    2022-11-30T20:03:57.548Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO Tags changed on monitored EC2 instance ( arn:aws:ec2:us-
west-2:123456789012:instance/i-1234567890abcdef0 )
2022-11-30T12:03:57.548-08:00    2022-11-30T20:03:57.548Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO This instance is missing the required tag key or value --
 attempting to stop the instance
2022-11-30T12:03:58.488-08:00    2022-11-30T20:03:58.488Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO Successfully stopped instance [ { CurrentState: { Code: 64,
 Name: 'stopping' }, InstanceId: 'i-1234567890abcdef0', PreviousState: { Code: 16,
 Name: 'running' } } ]
2022-11-30T12:03:58.546-08:00    END RequestId: b5befd18-2c41-43c8-
a320-3a4b2317cdac
```

Riepilogo del tutorial

Questo tutorial ha dimostrato come creare una EventBridge regola da abbinare a una modifica di tag su un evento di risorse per EC2 le istanze Amazon. La regola indicava una funzione Lambda che spegne automaticamente l'istanza se non ha il tag richiesto.

Il EventBridge supporto di Amazon per la modifica dei tag sulle AWS risorse offre la possibilità di creare un'automazione basata sugli eventi per molte risorse. Servizi AWS La combinazione di questa funzionalità AWS Lambda offre strumenti per creare soluzioni serverless che accedono alle AWS risorse in modo sicuro, scalabili su richiesta e sono convenienti.

Altri possibili casi d'uso dell' tag-change-on-resource EventBridge evento includono:

- Lancia un avviso se qualcuno accede alla tua risorsa da un indirizzo IP insolito: utilizza un tag per memorizzare l'indirizzo IP di origine di ogni visitatore che accede alla tua risorsa. Le modifiche al tag generano un CloudWatch evento. È possibile utilizzare tale evento per confrontare l'indirizzo IP di origine con un elenco di indirizzi IP validi e attivare un'e-mail di avviso se l'indirizzo IP di origine non è valido.
- Monitora se ci sono modifiche al controllo di accesso basato su tag per una risorsa: se hai impostato l'accesso a una risorsa utilizzando il controllo di accesso basato su attributi (tag)

(ABAC), puoi utilizzare EventBridge gli eventi generati da qualsiasi modifica al tag per richiedere un controllo da parte del team di sicurezza.

Risoluzione dei problemi di modifica dei tag

L'elenco di controllo seguente può essere utile se si verificano errori quando si tenta di applicare o modificare i tag nelle risorse selezionate nei risultati della query Find resources to tag (Trova risorse per tag).

- La risorsa potrebbe aver già attivato il numero massimo di tag. In genere, le risorse possono avere un massimo di 50 tag definiti dall'utente. AWS i tag generati non vengono conteggiati ai fini del conteggio massimo di 50 tag. Gli altri utenti possono anche aggiungere tag alla stessa risorsa nello stesso momento, che potrebbe aumentare i tag della risorsa fino al limite massimo.
- Alcuni servizi consentono un altro set di caratteri (o limitano il set di caratteri consentito) per la creazione di tag. Se hai aggiunto o modificato tag utilizzando caratteri speciali, consulta i requisiti dei tag nella documentazione del servizio della risorsa per verificare che tali caratteri siano consentiti dal servizio.
- Potresti non avere le autorizzazioni per modificare i tag della risorsa. Se non disponi delle autorizzazioni per visualizzare i tag esistenti su una risorsa, non puoi apportare modifiche ai tag della risorsa.
- Potresti non avere le autorizzazioni per modificare la risorsa. Le modifiche apportate ai metadati della risorsa potrebbero essere limitati da un altro amministratore.
- La risorsa potrebbe essere stata modificata o eliminata da un altro utente o processo. Ad esempio, supponiamo che una risorsa sia stata lanciata come parte della creazione di uno AWS CloudFormation stack. Se lo stack è stato eliminato o non è più attivo, la risorsa potrebbe non essere più disponibile.
- Le modifiche ai tag potrebbero non essere possibili se una risorsa è offline o terminata, oppure se sono in corso altri aggiornamenti (ad esempio gli aggiornamenti software) per la risorsa.
- Le modifiche ai tag possono avere esito negativo se si chiude la scheda del browser o si modifica la pagina prima del completamento delle modifiche ai tag. Terminare le modifiche di tag e attendere che l'esito positivo o negativo del banner appaia sulla pagina, prima di lasciare la pagina.
- Sebbene esista un limite di velocità per AWS Resource Groups Tagging API, il servizio che stai taggando potrebbe imporre un limite separato che potresti raggiungere prima del limite dell'API Resource Groups Tagging.

Riprova le modifiche ai tag non riuscite

Se le modifiche dei tag hanno dato esito negativo su almeno una delle risorse selezionate, il Tag Editor visualizza un banner rosso nella parte inferiore della pagina. Il banner mostra un messaggio di errore per ogni tipo di errore che si verifica. Per ogni errore, il banner identifica le risorse specifiche su cui Tag Editor non è stato in grado di apportare modifiche ai tag. Dopo aver esaminato e risolto gli errori, scegli Riprova le modifiche ai tag non riuscite sulle risorse per riprovare a modificare solo le risorse per le quali le modifiche ai tag non sono riuscite.

Sicurezza in Tag Editor

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

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

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gira Servizi AWS su Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per ulteriori informazioni sui programmi di conformità che si applicano a Tag Editor, consulta AWS Services in Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata da Servizio AWS ciò che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Tag Editor. I seguenti argomenti mostrano come configurare Tag Editor per soddisfare i tuoi obiettivi di sicurezza e conformità.

Argomenti

Protezione dei dati in Tag Editor

Il modello di responsabilità AWS condivisa modello si applica alla protezione dei dati in Tag Editor. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale

che gestisce tutto il Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

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

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

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

Crittografia dei dati

Le informazioni di tagging non sono crittografate. Sebbene non siano crittografati, i tag possono contenere informazioni utilizzate nell'ambito della strategia di sicurezza, quindi è importante

controllare chi può accedere ai tag sulle risorse. È particolarmente importante controllare chi può modificare i tag, poiché tale accesso potrebbe essere utilizzato per aumentare le proprie autorizzazioni.

Crittografia a riposo

Non esistono altri modi per isolare il traffico di servizio o di rete specifici di Tag Editor. Se applicabile, utilizza AWS un isolamento specifico. Puoi utilizzare l'API e la console Tag Editor in un cloud privato virtuale (VPC) per massimizzare la privacy e la sicurezza dell'infrastruttura.

Crittografia in transito

I dati di Tag Editor vengono crittografati in transito verso il database interno del servizio per il backup. Questa opzione non è configurabile dall'utente.

Gestione delle chiavi

Tag Editor non è attualmente integrato AWS Key Management Service e non supporta AWS KMS keys.

Riservatezza del traffico Internet

Tag Editor utilizza HTTPS per tutte le trasmissioni tra gli utenti di Tag Editor e AWS. Tag Editor utilizza TLS (Transport Layer Security) 1.3, ma supporta anche TLS 1.2.

Gestione delle identità e degli accessi per Tag Editor

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse di Tag Editor. IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Come funziona Tag Editor con IAM
- Esempi di policy basate sull'identità di Tag Editor
- Risoluzione dei problemi relativi all'identità e all'accesso a Tag Editor

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che svolgi in Tag Editor.

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

Amministratore del servizio: se sei responsabile delle risorse di Tag Editor presso la tua azienda, probabilmente hai pieno accesso a Tag Editor. È tuo compito determinare a quali funzionalità e risorse di Tag Editor devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con Tag Editor, consultaCome funziona Tag Editor con IAM.

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere politiche per gestire l'accesso a Tag Editor. Per visualizzare esempi di policy basate sull'identità di Tag Editor che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità di Tag Editor

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se

accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

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

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sul metodo consigliato per la firma delle richieste, consulta Signature Version 4 AWS per le richieste API nella Guida per l'utente IAM.

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

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Utenti e gruppi

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

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

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

Roles

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Per assumere temporaneamente un ruolo IAM in AWS Management Console, puoi passare da un ruolo utente a un ruolo IAM (console). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Create a role for a third-party identity provider (federation) nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per

informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso inoltrato (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che AWS CLI effettuano richieste AWS API. Questa soluzione è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

Gestione dell'accesso con policy

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

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

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

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

Policy basate sulle risorse

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

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Elenchi di controllo degli accessi () ACLs

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

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la panoramica della lista di controllo degli accessi (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

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

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.
- Politiche di controllo del servizio (SCPs): SCPs sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più di

proprietà dell' Account AWS azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna di esse. Utente root dell'account AWS Per ulteriori informazioni su Organizations and SCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.

- Politiche di controllo delle risorse (RCPs): RCPs sono politiche JSON che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le politiche IAM allegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di Servizi AWS tale supporto RCPs, vedere Resource control policies (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta la logica di valutazione delle policy nella IAM User Guide.

Come funziona Tag Editor con IAM

Prima di utilizzare IAM per gestire l'accesso a Tag Editor, è necessario comprendere quali funzionalità IAM sono disponibili per l'uso con Tag Editor. Per avere una visione di alto livello di come Tag Editor e altri Servizi AWS funzionano con IAM, consulta Servizi AWS la sezione relativa all'utilizzo di IAM nella IAM User Guide.

Argomenti

- Politiche basate sull'identità di Tag Editor
- Policy basate sulle risorse

- Autorizzazione basata su tag
- ruoli IAM di Tag Editor

Politiche basate sull'identità di Tag Editor

Con le policy basate sull'identità IAM, puoi specificare azioni e risorse consentite o negate oltre alle condizioni in base alle quali le azioni sono consentite o negate. Tag Editor supporta azioni, risorse e chiavi di condizione specifiche. Per informazioni su tutti gli elementi utilizzati in una policy JSON, consulta Documentazione di riferimento degli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Operazioni

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

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

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

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

Ad esempio, per concedere a qualcuno il permesso di etichettare una risorsa con l'operazione `tag:TagResources` API, includi l'`tag:TagResources`azione nella sua politica. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. Tag Editor definisce il proprio set di azioni che descrivono le attività che è possibile eseguire con questo servizio.

Per specificare più azioni di etichettatura in una singola istruzione, separale con virgole come segue.

```
"Action": [
      "tag:action1",
      "tag:action2",
      "tag:action3"
```

Puoi specificare più operazioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le operazioni che iniziano con la parola `Get`, includi la seguente operazione.

```
"Action": "tag:Get*"
```

Per visualizzare un elenco delle azioni di Tag Editor, consulta Azioni, risorse e chiavi di condizione per Tag Editor nel Service Authorization Reference.

Risorse

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

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le operazioni 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": "*"
```

Tag Editor non dispone di risorse proprie. Invece, manipola i metadati (tag) allegati alle risorse create da altri. Servizi AWS

Chiavi di condizione

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

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

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano

più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

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

Tag Editor non definisce alcuna chiave di condizione specifica del servizio.

Esempi

Per visualizzare esempi di politiche basate sull'identità di Tag Editor, consulta. Esempi di policy basate sull'identità di Tag Editor

Policy basate sulle risorse

Tag Editor non supporta le politiche basate sulle risorse perché non definisce nessuna delle proprie risorse.

Autorizzazione basata su tag

L'autorizzazione basata sui tag fa parte della strategia di sicurezza denominata controllo degli accessi basato sugli attributi (ABAC).

Per controllare l'accesso a una risorsa in base ai relativi tag, è necessario fornire informazioni sui tag nell'elemento condition di una policy utilizzando i tasti `aws:ResourceTag/key-name` `aws:RequestTag/key-name`, o condition. `aws:TagKeys` È possibile applicare tag a una risorsa durante la creazione o l'aggiornamento della risorsa.

Per visualizzare una policy basata sulle identità di esempio per limitare l'accesso a una risorsa basata su tag su tale risorsa, consulta Visualizzazione dei gruppi in base ai tag. Per ulteriori informazioni sul controllo degli accessi basato sugli attributi (ABAC), vedi A cosa serve ABAC? AWSnella Guida per l'utente di IAM.

ruoli IAM di Tag Editor

Un ruolo IAM è un'entità interna all'utente Account AWS che dispone di autorizzazioni specifiche. Tag Editor non dispone né utilizza ruoli di servizio.

Utilizzo di credenziali temporanee con Tag Editor

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

Ruoli collegati ai servizi

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

Tag Editor 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.

Tag Editor non dispone né utilizza ruoli di servizio.

Esempi di policy basate sull'identità di Tag Editor

Per impostazione predefinita, i responsabili IAM, come i ruoli e gli utenti, non sono autorizzati a creare o modificare i tag. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS APIs. Un amministratore IAM deve creare policy IAM che concedano ai responsabili l'autorizzazione a eseguire operazioni API specifiche sulle risorse specifiche di cui hanno bisogno. L'amministratore deve quindi collegare tali policy ai principali che richiedono tali autorizzazioni.

Per istruzioni sulla creazione di una policy basata sull'identità IAM utilizzando questi esempi di documenti di policy JSON, consulta Creating Policies on the JSON Tab nella IAM User Guide.

Argomenti

- Best practice per le policy
- Utilizzo della console Tag Editor e dell'API Resource Groups Tagging
- Consentire agli utenti di visualizzare le loro autorizzazioni

- Visualizzazione dei gruppi in base ai tag

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse di Tag Editor nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Protezione dell'accesso API con MFA nella Guida per l'utente IAM.

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

Utilizzo della console Tag Editor e dell'API Resource Groups Tagging

Per accedere alla console Tag Editor e all'API Resource Groups Tagging, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sui tag allegati alle risorse del tuo. Account AWS Se crei una policy basata sull'identità che è più restrittiva delle autorizzazioni minime richieste, i comandi della console e dell'API non funzioneranno come previsto per i principali IAM che adottano tale policy.

Per garantire che tali principali possano ancora utilizzare Tag Editor, allega la seguente policy (o una policy che contenga le autorizzazioni elencate nella seguente policy) alle entità. Per ulteriori informazioni, consulta la sezione Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM:

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

Per ulteriori informazioni sulla concessione dell'accesso all'API Tag Editor e Resource Groups Tagging, vedere. Concessione delle autorizzazioni per l'utilizzo di Tag Editor

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica

include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI 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 dei gruppi in base ai tag

Puoi utilizzare le condizioni della tua politica basata sull'identità per controllare l'accesso alle risorse di Tag Editor in base ai tag. Questo esempio mostra come è possibile creare una politica che consenta la visualizzazione di 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 associato al principale 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}"}
            }
        }
    ]
}
```

È possibile collegare questa policy agli utenti nell'account. Se un utente 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 la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.

Risoluzione dei problemi relativi all'identità e all'accesso a Tag Editor

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

Argomenti

- Non sono autorizzato a eseguire un'azione in Tag Editor
- Non sono autorizzato a eseguire iam: PassRole

Non sono autorizzato a eseguire un'azione in Tag Editor

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 tag su una risorsa ma non dispone delle `tag:GetTagKeys` autorizzazioni.

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

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

Non sono autorizzato a eseguire iam: PassRole

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

Alcuni Servizi AWS consentono di passare 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 Tag Editor. 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.

Registrazione e monitoraggio in Tag Editor

Tutte le azioni di Tag Editor vengono registrate. AWS CloudTrail

Registrazione delle chiamate API di Tag Editor con CloudTrail

Tag Editor è integrato con AWS CloudTrail un servizio che fornisce una registrazione delle azioni intraprese da un utente, da un ruolo o da un utente Servizio AWS in Tag Editor. CloudTrail acquisisce tutte le chiamate API per Tag Editor come eventi, incluse le chiamate dalla console Tag Editor e le chiamate di codice all'API Resource Groups Tagging. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Tag Editor. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta che è stata effettuata a Tag Editor, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

Per ulteriori informazioni in merito CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

Informazioni su Tag Editor in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività in Tag Editor o nella console Tag Editor, tale attività viene registrata in un CloudTrail evento insieme ad altri Servizio AWS eventi nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi in tuo Account AWS, compresi gli eventi per Tag Editor, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurarne altri Servizi AWS per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta le seguenti risorse:

- Creare un percorso per il tuo Account AWS
- Servizi e integrazioni CloudTrail supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail

- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le azioni di Tag Editor vengono registrate CloudTrail e sono documentate nel riferimento all'API Tag Editor. Le azioni di Tag Editor nella console vengono registrate da CloudTrail, e vengono mostrate come eventi con `tagging.amazonaws.com` come. `eventSource`

Ogni evento o voce di 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 dell'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, vedete l'CloudTrail`userIdentity`elemento.

Informazioni sulle voci dei file di registro di Tag Editor

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta da qualsiasi sorgente e include informazioni sull'operazione richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. I file di log di CloudTrail non sono uno stack trace ordinato delle chiamate API pubbliche, pertanto queste non vengono visualizzate in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'azione`TagResources`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661372702",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661372702",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
```

```
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-24T20:25:03Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-24T20:27:14Z",
    "eventSource": "tagging.amazonaws.com",
    "eventName": "TagResources",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.65",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resourcegroupstaggingapi.tag-resources",
    "requestParameters": {
        "resourceARNList": [
            "arn:aws:events:us-east-1:123456789012:rule/SecretsManagerMonitorRule"
        ],
        "tags": {
            "owner": "alice"
        }
    },
    "responseElements": {
        "failedResourcesMap": {}
    },
    "requestID": "8f9ea891-4125-460c-802f-26c11EXAMPLE",
    "eventID": "b2c9322a-aad7-424b-8f0b-423daEXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "tagging.us-east-1.amazonaws.com"
    }
}
```

Convalida della conformità per Tag Editor

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

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

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

- Governance e conformità per la sicurezza: queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.
- Riferimenti sui servizi conformi ai requisiti HIPAA: elenca i servizi HIPAA idonei. Non tutti Servizi AWS sono idonei alla normativa HIPAA.
- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty

può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.

- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in Tag Editor

Tag Editor esegue backup automatici su risorse di servizio interne. Questi backup non sono configurabili dall'utente. I backup sono crittografati, sia a riposo che in transito. Tag Editor archivia i dati dei clienti in Amazon DynamoDB.

L'infrastruttura AWS globale è costruita attorno a zone Regioni AWS di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

Se elimini i tag accidentalmente, contatta Center.Supporto AWS

Per ulteriori informazioni sulle Regioni AWS zone di disponibilità, consulta AWS Global Infrastructure.

Sicurezza dell'infrastruttura in Tag Editor

Tag Editor non offre metodi aggiuntivi per isolare il traffico di servizio o di rete. Se applicabile, utilizza AWS un isolamento specifico. Puoi utilizzare l'API e la console Tag Editor in un cloud privato virtuale (VPC) per massimizzare la privacy e la sicurezza dell'infrastruttura.

Utilizzi chiamate API AWS pubblicate per accedere a Tag Editor attraverso la rete. I client devono supportare quanto segue:

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

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale AWS Identity and Access Management (IAM). In

alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per firmare le richieste.

Tag Editor non supporta politiche basate sulle risorse.

È possibile richiamare le operazioni API di Tag Editor da qualsiasi posizione di rete, ma Tag Editor supporta politiche di accesso basate sulle risorse, che possono includere restrizioni basate sull'indirizzo IP di origine. Puoi anche utilizzare le policy di Tag Editor per controllare l'accesso da endpoint Amazon Virtual Private Cloud (Amazon VPC) specifici o specifici. VPCs In effetti, questo approccio isola l'accesso alla rete a una determinata risorsa solo dal VPC specifico all'interno AWS della rete.

Quote del servizio

La tabella seguente fornisce informazioni sulle quote di servizio per Tag Editor.

Queste quote attualmente non sono regolabili tramite la console Service Quotas. Contattare Supporto.

Nome	Predefinita
Tag collegati per risorsa	50 tag definiti dall'utente (i tag AWS generati non rientrano in questo limite).
Nome chiave di tag	Minimo 1, massimo 128 caratteri Unicode in formato UTF-8. I caratteri consentiti includono lettere, numeri, spazi e i seguenti caratteri: `_ . : / = + - @` I nomi delle chiavi non possono iniziare con `aws:` perché quel prefisso è riservato all' AWS uso. **Note** Alcuni Servizi AWS hanno alcune restrizioni aggiuntive relative ai caratteri o alla lunghezza. Per ulteriori informazioni, consulta la documenta

Nome	Predefinita
	zione per il servizio specifico.
Valori Tag	Minimo 0, massimo 256 caratteri Unicode in formato UTF-8. I caratteri consentiti includono lettere, numeri, spazi e i seguenti caratteri: `_ . : / = + - @` **Note** Alcuni Servizi AWS hanno alcune restrizioni aggiuntive relative ai caratteri o alla lunghezza. Per ulteriori informazioni, consulta la documentazione per il servizio specifico.
Frequenza di chiamata di GetResourcesOperazione API	Massimo 15 chiamate al secondo
Frequenza di chiamata delle seguenti operazioni API: • TagResources • UntagResources • GetTagKeys • GetTagValues	Massimo 5 chiamate al secondo

Cronologia dei documenti di Tag Editor

Modifica	Descrizione	Data
La gestione dei tag nella console AWS Resource Groups Tag Editor è stata spostata Esploratore di risorse AWS nella console	AWS ha spostato la funzionalità di gestione dei tag di Tag Editor dalla AWS Resource Groups console alla Esploratore di risorse AWS console. Per ulteriori informazioni sulla gestione dei tag delle risorse in Resource Explorer, consulta la sezione Gestione delle risorse nella guida per l'utente di Resource Explorer.	10 aprile 2025
Autorizzazioni aggiornate per la valutazione della conformità a livello di organizzazione	Sono state aggiornate le autorizzazioni per la valutazione della conformità a livello di organizzazione per includere le autorizzazioni che facilitano l'accesso al rapporto di conformità.	28 agosto 2024
Contenuti aggiornati	Titoli degli argomenti aggiornati e contenuto riorganizzato per migliorare la leggibilità e la reperibilità.	25 luglio 2024
Taggare i contenuti da Riferimenti generali di AWS quelli spostati in questa guida	Gli argomenti relativi all'etichettatura AWS delle risorse sono stati spostati Riferimenti generali di AWS da questa guida.	24 marzo 2023
Aggiornamento delle best practice di IAM	Guida aggiornata per l’allineamento alle best practice IAM.	3 gennaio 2023

	Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.	
Spostamento della documentazione di Tag Editor nella relativa guida	La documentazione di Tag Editor è ora fornita nella relativa guida per l'utente anziché far parte della Guida per l' AWS Resource Groups utente.	13 dicembre 2022
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
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
La console Tag Editor esce dalla AWS Systems Manager console	La console Tag Editor è ora indipendente dalla console Systems Manager. Sebbene sia ancora possibile trovare i puntatori alla console Tag Editor nella barra di navigazione sinistra di Systems Manager, è possibile aprire la console Tag Editor direttamente dal menu a discesa in alto a sinistra di. AWS Management Console	5 giugno 2019

I vecchi strumenti di Tag Editor non sono più disponibili	Le menzioni agli editor di tag più vecchi, classici o precedenti sono state rimosse; questi strumenti non sono più disponibili in AWS. Utilizzate invece 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 file CSV	È possibile esportare i risultati di una query nella pagina Trova Risorse per tag su un file in formato CSV. 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