aws

Guida per l'utente

Application Cost Profiler

Application Cost Profiler: Guida per l'utente

Table of Contents

AWSApplication Cost Profiler verrà interrotto entro il 30 settembre 2024 e non accetta più nuovi clienti.

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'èAWSApplication Cost Profiler?

AWSApplication Cost Profiler ti aiuta a separare ilAWSfatturazione e costi da parte degli inquilini del tuo servizio. UNinquilinopuò essere un utente, un gruppo di utenti o un progetto.

UNrisorsaè un'entità con cui gli utenti possono lavorareAWS, ad esempio un'istanza Amazon Elastic Compute Cloud (Amazon EC2). Assicurati di poter identificare l'utilizzo delle risorse in base al tenant scelto.

TipicoAWSl'utilizzo delle risorse include servizi condivisi che supportano più tenant all'interno dell'organizzazione. Alcune risorse utilizzano dimensioni basate sul tempo. Per ottenere informazioni sui costi e sulla fatturazione per tenant anziché per uso orario della risorsa, è possibile integrare le risorse con Application Cost Profiler. Con questo approccio granulare, puoi capire comeAWSle risorse vengono utilizzate in una soluzione software condivisa.

Le seguenti risorse che possono utilizzare dimensioni basate sul tempo o l'uso orario sono abilitate per Application Cost Profiler:

- istanze Amazon EC2 (solo istanze on demand e spot)
- Code di Amazon Simple Queue Service (Amazon SQS)
- Argomenti su Amazon Simple Notification Service (Amazon SNS)
- Amazon DynamoDB legge e scrive

> **Note**
>
> L'utilizzo di Amazon SQS, Amazon SNS e DynamoDB non viene addebitato in base al tempo, a differenza della maggior parte delle risorse. Nel loro caso, l'utilizzo durante un'ora (ad esempio, un certo numero di letture e scritture in DynamoDB), è classificato in base alla percentuale dell'ora che si allocano a tenant diversi, indipendentemente dal momento in cui le letture o le scritture sono avvenute durante l'ora.

Integra i tuoi servizi con Application Cost Profiler in tre passaggi:

1. Attivazione e configurazione di un report— Questo passaggio definisce l'aspetto del tuo output finale.

2. Invia i dati di utilizzo del tenant a Application Cost Profiler— Questo passaggio richiede il codice nel servizio per creare dati di utilizzo che associa i tenant al tempo in cui utilizzano le risorse e quindi inviare tali dati di utilizzo a Application Cost Profiler.
3. Recupera report— Application Cost Profiler fornisce report con la cadenza specificata nella configurazione del report. I report mostrano il costo associato all'utilizzo di ciascun inquilino, offrendoti una visione granulare della fatturazione.

Per ulteriori informazioni su queste fasi, consultaNozioni di base.

Guida introduttiva a Application Cost Profiler

AWSApplication Cost Profiler ti aiuta a ottenere informazioni sui costi AWS delle tue risorse segnalando l'utilizzo delle risorse per tenant, anziché per la risorsa nel suo insieme. Un tenant può essere un utente, un gruppo di utenti o un progetto. Assicurati di poter identificare l'utilizzo delle risorse da parte del tenant che scegli. Per ottenere report sui costi relativi all'utilizzo dei tenant, configurate un rapporto e inviate i dati di utilizzo ad Application Cost Profiler. Questa sezione descrive i prerequisiti che è necessario completare prima di utilizzare Application Cost Profiler.

Argomenti

Registrarsi per creare un Account AWS

Se non disponi di un Account AWS, completa la procedura seguente per crearne uno.

Per registrarsi a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

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

   Durante la registrazione di un Account AWS, viene creato un Utente root dell'account AWS. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWSnell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

Al termine del processo di registrazione, riceverai un'e-mail di conferma da AWS. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Creazione di un utente amministratore

Dopo aver effettuato l'accesso a un Account AWS, crea un utente amministratore in modo da non utilizzare l'utente root per le attività quotidiane.

Protezione dell'Utente root dell'account AWS

1. Accedi alla AWS Management Console come proprietario dell'account scegliendo Utente root e immettendo l'indirizzo email del Account AWS. Nella pagina successiva, inserisci la password.

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

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

Creazione di un utente amministratore

- Per le tue attività amministrative quotidiane, assegna l'accesso amministrativo a un utente amministratore in AWS IAM Identity Center.

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

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 Accedere al portale di accesso AWS nella Guida per l'utente Accedi ad AWS.

Concessione dell'accesso programmatico

Gli utenti hanno bisogno di un accesso programmatico se desiderano interagire con AWS esternamente a AWS Management Console. La modalità con cui concedere l'accesso programmatico dipende dal tipo di utente che accede ad AWS.

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

Quale utente necessita dell'accesso programmatico?	Per	Come
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Utilizza credenziali temporane e per firmare richieste programmatiche alla AWS CLI, agli SDK AWS o alle API AWS.	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per la AWS CLI, consulta la pagina Configurazione della AWS CLI per l'uso di AWS IAM Identity Center nella Guida per l'utente dell'AWS Command Line Interface. • Per gli SDK AWS, gli strumenti e le API AWS, consulta la pagina Autentica zione Centro identità IAM nella Guida di riferimento per SDK e strumenti AWS.
IAM	Utilizza credenziali temporane e per firmare richieste programmatiche alla AWS CLI, agli SDK AWS o alle API AWS.	Segui le istruzioni in Utilizzo di credenziali temporanee con le risorse AWS nella Guida per l'utente IAM.
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare richieste programmatiche alla AWS	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per la AWS CLI, consulta la pagina Autenticazione

Quale utente necessita dell'accesso programmatico?	Per	Come
	CLI, agli SDK AWS o alle API AWS.	tramite credenziali utente IAM nella Guida per l'utente dell'AWS Command Line Interface. • Per gli SDK e gli strumenti AWS, consulta la pagina Autenticazione con credenziali a lungo termine nella Guida di riferimento per SDK e strumenti AWS. • Per le API AWS, consulta la pagina Gestione delle chiavi di accesso per utenti IAM nella Guida per l'utente IAM.

Prerequisiti specifici di Application Cost Profiler

Prima di iniziare a utilizzare Application Cost Profiler, è necessario completare i seguenti prerequisiti:

- Abilita Cost Explorer

  Abilita AWS Cost Explorer per il tuo AWS account. La configurazione di un account con Cost Explorer può richiedere fino a 24 ore. È necessario completare la configurazione di Cost Explorer prima che Application Cost Profiler possa generare i report giornalieri e mensili.

  Per ulteriori informazioni, vedere Enabling Cost Explorer nella Guida AWS Billing and Cost Management per l'utente.

- Crea bucket S3

  Crea almeno due bucket Amazon Simple Storage Service (Amazon S3). Application Cost Profiler utilizza un bucket S3 per fornirti report. L'altro bucket S3 viene utilizzato per caricare i dati di utilizzo su Application Cost Profiler. In genere, è necessario un solo bucket S3 per caricare i dati di utilizzo. Tuttavia, potresti voler disporre di più di un bucket S3 in modo da poter continuare l'utilizzo per

diversi servizi in bucket S3 separati con autorizzazioni diverse, se necessario per la tua sicurezza. È necessario concedere le autorizzazioni di Application Cost Profiler a questi bucket S3.

Per ulteriori informazioni sulla configurazione dei bucket Amazon S3 per Application Cost Profiler, consulta. Configurazione dei bucket Amazon S3 per Application Cost Profiler

- Abilita i tag

  Per segnalare l'utilizzo per tag, anziché per risorsa, devi abilitare tali tag nella AWS Billing and Cost Management console.

  Per ulteriori informazioni sull'attivazione dei tag AWS generati, consulta Attivazione dei tag di allocazione dei AWS costi generati nella Guida per l'utente. AWS Billing and Cost Management Per ulteriori informazioni sull'attivazione dei tag definiti dall'utente, vedere Attivazione dei tag di allocazione dei costi definiti dall'utente nella Guida per l'utente. AWS Billing and Cost Management

Passaggi successivi

Dopo aver completato questi prerequisiti, puoi:

- Configura il rapporto e invia i dati di utilizzo ad Application Cost Profiler. Per ulteriori informazioni, consulta Creazione di report.
- Ottieni e analizza i report generati. Per ulteriori informazioni, consulta Utilizzo dei report di profiler costo applicazione.

Configurazione dei bucket Amazon S3 per Application Cost Profiler

Per inviare dati di utilizzo e ricevere report daAWSApplication Cost Profiler, devi avere almeno un bucket Amazon Simple Storage Service (Amazon S3) nel tuoAccount AWSper archiviare i dati e un bucket S3 per ricevere i tuoi report.

> **Note**
>
> Per utenti diAWS Organizations, i bucket Amazon S3 possono trovarsi nell'account di gestione o in singoli account membri. I dati nei bucket S3 di proprietà dell'account di gestione possono essere utilizzati per generare report per l'intera organizzazione. Nei singoli

account membri, i dati nei bucket S3 possono essere utilizzati solo per generare report per quell'account membro.

I bucket S3 creati sono di proprietà delAccount AWSin cui li crei. I bucket S3 vengono fatturati alle tariffe standard Amazon S3. Per ulteriori informazioni su come creare un bucket Amazon S3, consultaCreazione di un bucketnellaGuida dell'utente Amazon Simple Storage Service.

Affinché Application Cost Profiler utilizzi i bucket S3, ai bucket devi collegare una policy che consenta a Profiler dei costi dell'applicazione di leggere e/o scrivere nel bucket. Se si modifica il criterio dopo la configurazione dei report, è possibile impedire a Application Cost Profiler di leggere i dati di utilizzo o di consegnare i report.

Negli argomenti seguenti viene illustrato come configurare le autorizzazioni per i bucket Amazon S3 dopo averli creati. Oltre alla possibilità di leggere e scrivere oggetti, se sono stati crittografati i bucket, Application Cost Profiler deve avere accesso alAWS Key Management Service(AWS KMS) chiave per ogni secchio.

Argomenti

Fornire ad Application Cost Profiler l'accesso al bucket S3 di consegna del report

Il bucket S3 configurato per Application Cost Profiler per la consegna dei report deve avere un criterio che consenta a Application Cost Profiler di creare gli oggetti del report. Inoltre, il bucket S3 deve essere configurato per abilitare la crittografia.

> **Note**
>
> Quando crei il bucket, devi scegliere di crittografarlo. Puoi scegliere di crittografare il bucket con le chiavi gestite da Amazon S3 (SSE-S3) o con la tua chiave gestita daAWS KMS(SSE-KMS). Se hai già creato il bucket senza crittografia, devi modificare il bucket per aggiungere la crittografia.

Per dare all'Application Cost Profiler l'accesso al bucket S3 di consegna del report

1. Accedi aConsole Amazon S3e effettua l'accesso.
2. SelezionaBucketdalla navigazione a sinistra, quindi scegli il bucket dall'elenco.
3. SelezionaAutorizzazionitab, quindi, accanto aPolicy del bucket, scegliModificare.
4. NellaPolicynella sezione, inserire la policy seguente. Replace (Sostituisci)*<bucket_name>*con il nome del tuo bucket*<Account AWS>*con l'ID del tuoAccount AWS.

```
{
      "Version":"2008-10-17",
      "Statement":[
        {
          "Effect":"Allow",
          "Principal":{
            "Service":"application-cost-profiler.amazonaws.com"
          },
          "Action":[
            "s3:PutObject*",
            "s3:GetEncryptionConfiguration"
          ],
          "Resource": [
            "arn:aws:s3:::<bucket-name>",
            "arn:aws:s3:::<bucket-name>/*"
          ],
          "Condition": {
            "StringEquals": {
              "aws:SourceAccount": "<Account AWS>"
            },
            "ArnEquals": {
              "aws:SourceArn": "arn:aws:application-cost-profiler:us-
east-1:<Account AWS>:*"
            }
          }
        }
      ]
    }
```

In questa politica si sta fornendo l'entità del servizio Application Cost Profiler (`application-cost-profiler.amazonaws.com`) l'accesso a report nel bucket specificato. Lo fa a tuo nome, e include un'intestazione con il tuoAccount AWSe un ARN specifico per il periodo fisso

di consegna del report. Per garantire che Application Cost Profiler acceda al tuo bucket solo quando agisce per tuo conto, il`Condition`controlla le intestazioni.

5. ScegliereSalva le modificheper salvare la tua polizza, allegata al tuo bucket.

   Se hai creato il tuo bucket utilizzando la crittografia SSE-S3, hai finito. Se hai utilizzato la crittografia SSE-KMS, sono necessari i seguenti passaggi per consentire all'Application Cost Profiler l'accesso al tuo bucket.

6. (Facoltativo) SelezionareProprietàper il bucket, e sottocrittografia di default, seleziona l'Amazon Resource Name (ARN) perAWS KMSchiave. Questa azione visualizza ilAWS Key Management Serviceconsole e mostra la tua chiave.
7. (Facoltativo) Aggiungere il criterio per consentire a Application Cost Profiler l'accesso alAWS KMSchiave. Per istruzioni sull'aggiunta di questa policy, consultaFornire l'accesso a Application Cost Profiler ai bucket S3 crittografati SSE-KMS.

Fornire a Application Cost Profiler l'accesso al bucket S3 dei dati di utilizzo

Il bucket S3 configurato per la lettura dei dati di utilizzo di Application Cost Profiler deve avere un criterio per consentire a Application Cost Profiler di leggere gli oggetti dati di utilizzo.

> **Note**
>
> Concedendo a Application Cost Profiler l'accesso ai dati di utilizzo dell'utente, accetti che possiamo copiare temporaneamente tali oggetti dati di utilizzo negli Stati Uniti orientali (Virginia settentrionale)Regione AWSdurante l'elaborazione dei report. Questi oggetti di dati saranno conservati nella regione Stati Uniti orientali (Virginia settentrionale) fino al completamento della generazione dei report mensili.

Per dare ad Application Cost Profiler l'accesso al bucket S3 dei dati di utilizzo

1. Accedi aConsole Amazon S3e effettua l'accesso.
2. SelezionaBucketdalla navigazione a sinistra, quindi scegli il bucket dall'elenco.
3. SelezionaAutorizzazionitab, quindi, accanto aPolicy del bucket, scegliModificare.
4. NellaPolicynella sezione, inserire la policy seguente. Replace (Sostituisci)*<bucket-name>*con il nome del tuo bucket*<Account AWS>*con l'ID del tuoAccount AWS.

```
{
      "Version":"2008-10-17",
      "Statement":[
        {
          "Effect":"Allow",
          "Principal":{
            "Service":"application-cost-profiler.amazonaws.com"
          },
          "Action":[
            "s3:GetObject*"
          ],
          "Resource": [
            "arn:aws:s3:::<bucket-name>",
            "arn:aws:s3:::<bucket-name>/*"
          ],
          "Condition": {
            "StringEquals": {
              "aws:SourceAccount": "<Account AWS>"
            },
            "ArnEquals": {
              "aws:SourceArn": "arn:aws:application-cost-profiler:us-
east-1:<Account AWS>:*"
            }
          }
        }
      ]
    }
```

In questa politica si sta fornendo l'entità del servizio Application Cost Profiler (`application-cost-profiler.amazonaws.com`) per estrarre i dati dal bucket specificato. Lo fa a tuo nome, e include un'intestazione con il tuoAccount AWSe un ARN specifico per il tuo secchio d'uso. Per garantire che Application Cost Profiler acceda al tuo bucket solo quando agisce per tuo conto, il`Condition`controlla le intestazioni.

5. ScegliereSalva le modificheper salvare la tua polizza, allegata al tuo bucket.

Se il bucket è crittografato conAWS KMSchiavi gestite, quindi è necessario concedere ad Application Cost Profiler l'accesso al bucket seguendo la procedura nella sezione successiva.

Fornire l'accesso a Application Cost Profiler ai bucket S3 crittografati SSE-KMS

Se si crittografano i bucket S3 configurati per Application Cost Profiler (necessari per i bucket di report) con le chiavi memorizzate inAWS KMS(SSE-KMS), è inoltre necessario concedere le autorizzazioni a Application Cost Profiler per decrittografarli. Lo fai dando accesso alAWS KMSchiavi utilizzate per crittografare i dati.

> **Note**
>
> Se il bucket è crittografato con le chiavi gestite di Amazon S3, non è necessario completare questa procedura.

Per dare accesso a Application Cost ProfilerAWS KMSper bucket S3 crittografati SSE-KMS

1. Accedi aAWS KMSplanciae effettua l'accesso.
2. SelezionaChiavi gestite dal clientedalla navigazione a sinistra, quindi scegliere la chiave utilizzata per crittografare il bucket dall'elenco.
3. SelezionaPassa alla visualizzazione policy, quindi scegliModificare.
4. NellaPolicy, inserire la seguente dichiarazione policy.

```
  {
    "Effect": "Allow",
    "Principal": {
        "Service": "application-cost-profiler.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
          "Condition": {
            "StringEquals": {
              "aws:SourceAccount": "<Account AWS>"
            },
            "ArnEquals": {
              "aws:SourceArn": "arn:aws:application-cost-profiler:us-
east-1:<Account AWS>:*"
```

```
            }
    }
```

5. ScegliereSalva le modificheper salvare la tua politica, allegata alla tua chiave.
6. Ripetere per ogni chiave che crittografa un bucket S3 a cui Application Cost Profiler deve accedere.

> **Note**
>
> I dati vengono copiati dal bucket S3 durante l'importazione nei bucket gestiti di Application Cost Profiler (crittografati). Se si revoca l'accesso alle chiavi, Application Cost Profiler non è in grado di recuperare nuovi oggetti dal bucket. Tuttavia, tutti i dati già importati possono ancora essere utilizzati per generare report.

Creazione di report

Dopo aver soddisfatto i prerequisiti, sei pronto per configurare il report per teAccount AWS e inviare i dati di utilizzo adAWS Application Cost Profiler. Questa sezione descrive come configurare il report e come inviare i dati di utilizzo ad Application Cost Profiler.

Configura il report

La procedura seguente mostra come configurare il rapporto che desideri generare in base alla data di utilizzo. È possibile configurare dettagli come la frequenza con cui viene generato il rapporto.

> **Note**
>
> Se faiAccount AWS parte di un'AWSorganizzazione, puoi configurare il rapporto utilizzando l'account di gestione o un account di membro individuale. I report configurati per i singoli account contengono solo dati per quell'account. I report configurati utilizzando l'account di gestione possono includere dati per l'intera organizzazione.
> Il bucket Amazon S3 utilizzato per l'output del report deve appartenere all'account che crea la configurazione del report.

Per configurare il rapporto Application Cost Profiler

1. Apri un browser Web e accedi alla console Application Cost Profiler.
2. Scegli Inizia ora per configurare o modificare un report.
3. Inserisci il nome e la descrizione del rapporto.
4. Inserisci il nome del tuo bucket S3 nel campo Inserisci il nome del bucket S3 e inserisci il prefisso S3 nel campo Inserisci prefisso S3. Per ulteriori informazioni sulla creazione di bucket S3 e sulla concessione delle autorizzazioni di Application Cost Profiler, vedereConfigurazione dei bucket Amazon S3 per Application Cost Profiler.
5. Seleziona le opzioni che desideri assegnare al rapporto:

   - Frequenza temporale: scegli se il rapporto viene generato con una cadenza giornaliera o mensile o entrambe.
   - Formato di output del report: scegli il tipo di file da creare nel bucket Amazon S3. Se si sceglie CSV, Application Cost Profiler crea un file di testo con valori separati da virgole con

compressione gzip per i report. Se si sceglie Parquet, viene generato un file Parquet per i report.

6. Scegli Configura per salvare la configurazione del report.

> **Note**
>
> È inoltre possibile utilizzare l'APIAWS Application Cost Profiler per configurare i report.

Verifica le impostazioni del report scegliendo Inizia ora per visualizzare la configurazione corrente del report.

> **Note**
>
> È possibile configurare un solo report. Tornando alla pagina di configurazione, il rapporto esistente verrà modificato.

Dopo aver configurato il report, l'inserimento dei dati è abilitato. Puoi integrare i tuoi servizi con Application Cost Profiler per fornire dati sull'utilizzo delle tue risorse.

Segnalazione dei dati di utilizzo degli inquilini provenienti dai tuoi servizi

Dopo aver configurato il rapporto, sei pronto per inviare i dati di utilizzo del tenant dalle risorse o dai servizi del tuo account. È necessario informare Application Cost Profiler quando la risorsa viene utilizzata per un tenant specifico. Ad esempio, se il servizio accetta chiamate API da diversi tenant, registri un'ora di inizio e di fine per ogni tenant quando inizi e termini una chiamata API da quel tenant. Application Cost Profiler utilizza questi dati per generare report sul costo del servizio, in base alla quantità di tempo impiegato per il lavoro di ciascun inquilino.

Per fornire ad Application

- Prepara i dati sull'utilizzo delle risorse: crea tabelle che descrivono quando una risorsa viene utilizzata per un tenant specifico.
- Carica dati di utilizzo: carica le tabelle su un bucket Amazon S3 a cui hai concesso l'autorizzazione ad accedere ad Application Cost Profiler.

- Importa dati di utilizzo: richiama l'operazione`ImportApplicationUsage` API per far sapere ad Application Cost Profiler che i dati sono pronti per essere elaborati.

Nelle sezioni seguenti vengono descritte ciascuna di queste fasi in modo più dettagliato.

Argomenti

Fase 1: Preparazione dei dati sull'utilizzo delle risorse

Quando una risorsa viene utilizzata nel tuo servizio, tieni traccia del tenant che la sta utilizzando. Registra questi dati in una tabella che puoi caricare in seguito per l'importazione di Application Cost Profiler. Ogni riga della tabella descrive una risorsa, il tenant che utilizza la risorsa e gli orari di inizio e fine di tale utilizzo. Un esempio di risorsa è un'istanza Amazon Elastic Compute Cloud (Amazon EC2) in uso.

Questo passaggio richiede l'integrazione del codice nel servizio per fornire le informazioni corrette sull'utilizzo.

I campi presenti in una tabella di utilizzo delle risorse sono elencati nella tabella seguente.

Campo	Descrizione
ApplicationId	Identifica l'applicazione o il prodotto del sistema che viene utilizzato. Definisce l'ambito dei metadati del tenant.
TenantId	Un identificatore nel sistema per l'inquilino che sta consumando la risorsa specificata. Applicati on Cost Profiler si aggrega a questo livello all'interno di ApplicationId.
TenantDesc	(Facoltativo) Dati aggiuntivi sull'inquilino per la tua segnalazione aggiuntiva.

Campo	Descrizione
UsageAccountId	L'account in cui viene eseguita la risorsa (importante per gli account che fanno parte di un'organizzazione).
StartTime	Timestamp (in millisecondi e microsecondi) da Epoch, in UTC. Indica l'ora di inizio del periodo di utilizzo da parte del tenant specificato.
EndTime	Timestamp (in millisecondi e microsecondi) da Epoch, in UTC. Indica l'ora di fine del periodo di utilizzo da parte del tenant specificato.
ResourceId	Amazon Resource (ARN) per la risorsa in uso.
Nome	(Facoltativo) In alternativa a specificare un ResourceId, è possibile specificare un tag di risorsa Name per attribuire i costi a un set di risorse (il campo deve includere il valore che si desidera utilizzare per il tag Nome). I tag delle risorse sono abilitati come parte del report di costi e utilizzo. Per ulteriori informazioni sui tag delle risorse, consulta i dettagli dei tag delle risorse nella Guida per l'utente del rapporto sui costi e sull'utilizzo.

L'output deve essere in un file di valori separati da virgola (.csv) che include una riga di titolo, come illustrato nell'esempio seguente.

```
ApplicationId,TenantId,TenantDesc,UsageAccountId,StartTime,EndTime,ResourceId
MyApp,Tenant1,,123456789012,1613681437032.9001,1613681437041.5312,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant2,,123456789012,1613681245531.4426,1613681245551.1323,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant1,,123456789012,1613681904815.3381,1613681904930.0972,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
```

```
MyApp,Tenant2,,123456789012,1613681904765.1956,1613681904946.574,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
```

Salva i dati come file, con l'estensione.csv (o .csv.gzip se compresso con gzip). Quando carichi questi dati su Application Cost Profiler, ogni porzione di volta viene assegnata al tenant associato. In questo esempio, il rapporto include l'intervallo di tempo del costo dell'istanza Amazon EC2 per quel tenant. Solo per le istanze Amazon EC2, le sezioni non associate a un tenant specifico vengono aggiunte a un tenant non attribuito. Gli intervalli di tempo sovrapposti vengono contati più volte. È tua responsabilità assicurarti che i dati nella tabella di utilizzo siano accurati.

> **Note**
>
> Il file deve rappresentare un'ora di tempo. Se una risorsa viene utilizzata per più ore, termina l'utilizzo ogni ora e inserisci un nuovo record nel file successivo che inizi alla stessa ora. È necessario inviare un singolo file contenente i dati di un'ora intera. Se vengono inviati più file per i dati della stessa ora, Application Cost Profiler considera solo i dati nel file più recente.

Ad esempio, la tabella seguente mostra come Application Cost Profiler calcola l'utilizzo per tre tenant, nell'arco di un'ora (3.600.000 millisecondi), in base agli intervalli di tempo forniti.

Inquilino	Intervalli di tempo forniti	Percentuale calcolata del costo orario
Inquilino 1	1.200.000 ms	33,34%
Inquilino 2	600.000 ms	16,66%
<unattributed>		50,00%

In questo esempio, a Tenant1 viene assegnato un terzo dell'ora e a Tenant2 viene assegnato un sesto dell'ora. La restante mezz'ora (1.800.000 ms) non è attribuita a nessuno dei client, ovvero il 50% dell'ora.

Attualmente, le seguenti risorse sono abilitate per Application Cost Profiler:

- Istanze Amazon EC2 (solo istanze on demand e spot)

- Funzioni lambda (se si inviano dati per una funzione Lambda, è necessario inviare l'ARN della risorsa non qualificata come`ResourceId`.)
- Istanza Elastic Container Service (Amazon ECS) Containt
- Code di Amazon Simple Queue Service (Amazon SQS)
- Argomenti su Amazon Simple Notification Service (Amazon SNS)
- Amazon DynamoDB legge e scrive

> **Note**
>
> L'utilizzo di Amazon SQS, Amazon SNS e DynamoDB non viene addebitato in base al tempo, a differenza della maggior parte delle risorse. Nel loro caso, l'utilizzo durante un'ora (ad esempio, un numero di letture e scritture in DynamoDB) è classificato in base alla percentuale dell'ora assegnata a diversi tenant, indipendentemente da quando le letture o le scritture sono avvenute durante l'ora.

Fase 2: Caricamento dell'utilizzo delle risorse

Dopo aver ottenuto un file di utilizzo per tenant, carica il file di dati su Amazon S3 e assicurati che Application Cost Profiler disponga dell'autorizzazione per accedervi.

Per ulteriori informazioni sulla creazione di un bucket S3, consultaPrerequisiti specifici di Application Cost Profiler.

Devi assicurarti che Application Cost Profiler abbia accesso al tuo bucket S3. Questa operazione deve essere eseguita solo una volta per bucket S3 (è possibile riutilizzare lo stesso bucket per caricare più file di utilizzo). Per informazioni su come concedere l'accesso al bucket, vedereFornire a Application Cost Profiler l'accesso al bucket S3 dei dati di utilizzo. Se il bucket è crittografato, vediFornire l'accesso a Application Cost Profiler ai bucket S3 crittografati SSE-KMS.

> **Note**
>
> Non è necessario crittografare i bucket S3 utilizzati per i dati di utilizzo.

Carica i tuoi dati nel bucket S3 come file, con estensione.csv (o .csv.gzip se compresso con gzip), a intervalli di un'ora. Dopo aver caricato un nuovo file, è necessario informare Application Cost Profiler di averlo caricato in modo che il file possa essere importato nel rapporto.

> **Note**
>
> Concedendo ad Application Cost Profiler l'accesso ai dati di utilizzo, l'utente accetta che possiamo copiare temporaneamente tali oggetti di dati di utilizzo negli Stati Uniti orientali (Virginia settentrionale)Regione AWS durante l'elaborazione dei report. Questi oggetti di dati verranno conservati nella regione US East (N.) fino al completamento del report mensile.

Fase 3: Importazione dei dati di utilizzo in Application Cost Profiler

Dopo aver caricato i dati di utilizzo in un bucket Amazon S3 a cui Application Cost Profiler ha accesso, informa Application Cost Profiler che i dati esistono e importali nel rapporto finale. A tale scopo, è necessario utilizzare l'`ImportApplicationUsage`operazione nell'API Application Cost Profiler.

Per informazioni sull'APIAWS Application Cost Profiler, inclusa l'`ImportApplicationUsage`operazione, consulta l'AWSApplication Cost Profiler API Reference.

Gli esempi seguenti mostrano come chiamare`ImportApplicationUsage`. Sostituisci il *`testo di input tra parentesi`* con i valori del bucket S3 e dell'oggetto caricato.

```
POST /ImportApplicationUsage HTTP/1.1
Content-type: application/json

{
    "sourceS3Location" : {
        "bucket": "<bucket-name>",
        "key": "<object-key>",
        "region": "<region-id>"
    }
}
```

> **Note**
>
> Il`region` parametro è obbligatorio solo se il bucket si trova in unRegione AWS bucket disabilitato per impostazione predefinita. Per ulteriori informazioni, consulta la sezione relativa alla gestione di Regioni AWS nella Riferimenti generali di AWS.

Application Cost Profiler genera un nuovo rapporto con la frequenza richiesta durante la configurazione del report, utilizzando i dati con cui è stato importato`ImportApplicationUsage`.

Dopo aver configurato il report e aver importato automaticamente i dati di utilizzo in Application Cost Profiler, sei pronto per visualizzare i report generati. Per ulteriori informazioni sui report, consultaUtilizzo dei report di profiler costo applicazione.

Utilizzo dei report di profiler costo applicazione

Dopo aver integrato i dati di utilizzo conAWSApplication Cost Profiler e inviano i dati su base oraria, Application Cost Profiler genera automaticamente il report.

I report vengono generati quotidianamente o mensilmente, in base all'opzione selezionata quandoconfigurazione del report. I report vengono inviati al bucket Amazon Simple Storage Service (Amazon S3) selezionato al momento della configurazione del report.

I report giornalieri generati il primo giorno del mese hanno i dati del mese precedente.

Dati disponibili in un rapporto Application Cost Profiler

Le colonne create in un report di utilizzo sono mostrate nella tabella seguente.

Nome colonna	Descrizione
PayerAccountId	L'ID dell'account di gestione in un'organi zzazione o l'ID account se l'account non fa parte diAWS Organizations.
UsageAccountId	L'ID account per l'account con utilizzo.
LineItemType	Il tipo di record. Sempre `Usage`.
Ora di inizio utilizzo	Timestamp (in millisecondi) da Epoch, in UTC. Indica l'ora di inizio del periodo per l'utilizzo da parte del tenant specificato.
Ora di fine utilizzo	Timestamp (in millisecondi) da Epoch, in UTC. Indica l'ora di fine del periodo per l'utilizzo da parte del tenant specificato.
Identificativo dell'applicazione	LaApplicationIdspecificato nei dati di utilizzo inviati a Application Cost Profiler.
Antiidentificatore TENN	LaTenantiDspecificato nei dati di utilizzo inviati a Application Cost Profiler. I dati senza

Nome colonna	Descrizione
	record nei dati di utilizzo vengono raccolti inunattributed .
Descrizione dell'inquilino	LaTenantDesc specificato nei dati di utilizzo inviati a Application Cost Profiler.
ProductCode	LaAWSprodotto fatturato (ad esempioAmazonEC2).
UsageType	Il tipo di utilizzo da fatturare (ad esempioBoxUsage:c5.large).
Operazioni	L'operazione che viene fatturata (ad esempio,RunInstances).
ResourceId	L'ID della risorsa o Amazon Resource Name (ARN) per la risorsa da fatturare.
fattore di scala	Se una risorsa viene sovraallocata per un'ora, ad esempio, i dati di utilizzo segnalati sono pari a 2 ore anziché 1 ora, viene applicato un fattore di scala per rendere il totale uguale all'importo fatturato effettivo (in questo caso, 0,5). Questa colonna riporta il fattore di scala utilizzato per la risorsa specifica per quell'ora. Il fattore di scala è sempre maggiore di zero (0) e inferiore o uguale a 1.
Percentuale di attribuzione tenant	La percentuale di utilizzo attribuita al tenant specificato (tra zero (0) e 1).
UsageAmount	La quantità di utilizzo attribuita al tenant specificato.
CurrencyCode	La valuta in cui si trovano il tasso e il costo (ad esempio,USD).

Nome colonna	Descrizione
Tariffa	La tariffa di fatturazione per l'utilizzo, per unità.
Costo inquilino	Il costo totale per tale risorsa per il tenant specificato.
Regione	LaAWSRegione della risorsa.
Nome	Se sono stati creati tag delle risorse per le risorse nel report Costo e utilizzo o tramite i dati di utilizzo delle risorse,NomeIl tag viene mostrato qui. Per ulteriori informazioni sui tag delle risorse, consultaDettagli dei tag delle risorsenellaGuida per l'utente del report di costi e utilizzo.

Di seguito è riportato un esempio di report di output per una risorsa per due ore.

```
PayerAccountId,UsageAccountId,LineItemType,UsageStartTime,UsageEndTime,ApplicationIdentifier,Te
123456789012,123456789012,Usage,2021-02-01T00:00:00.000Z,2021-02-01T00:30:00.000Z,Canary,unattr
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T00:30:00.000Z,2021-02-01T01:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
```

In questo esempio, la prima ora viene assegnata a`Tenant1`per metà del tempo. Rimane una mezz'ora`unattributed`. Nella seconda ora, quattro inquilini sono tutti assegnati l'ora intera. In questo caso, il fattore di scala li ridimensiona tutti di 0,25 e vengono tutti assegnati un quarto dell'ora. È possibile vedere il costo finale nella`TenantCost`colonna.

AWSQuote e endpoint di profiler costo applicazione

L'account AWS dispone delle seguenti quote predefinite, precedentemente definite limiti, per ogni servizio AWS. Salvo dove diversamente specificato, ogni quota si applica aAWSSpecifico per la regione. Se per alcune quote è possibile richiedere aumenti, altre quote non possono essere modificate.

Nelle seguenti tabelle sono elencate le quote di servizio per account e ilAWSEndpoint regione per Application Cost Profiler.

Service Quotas

Risorsa	Valore predefinito	Descrizione
Percentuale di`PutReportDefinition` richieste	5	Il numero massimo di`PutReportDefinition` richieste al secondo per account.
Percentuale di`UpdateReportDefinition` richieste	5	Il numero massimo di`UpdateReportDefinition` richieste al secondo per account.
Percentuale di`GetReportDefinition` richieste	5	Il numero massimo di`GetReportDefinition` richieste al secondo per account.
Percentuale di`DeleteReportDefinition` richieste	5	Il numero massimo di`DeleteReportDefinition` richieste al secondo per account.
Percentuale di`ListReportDefinitions` richieste	5	Il numero massimo di`ListReportDefiniti`

Risorsa	Valore predefinito	Descrizione
		ons richieste al secondo per account.
Percentuale diImportApplicationUsage richieste	5	Il numero massimo diImportApplicationUsage richieste al secondo per account.
Dimensione massima del file di dati di utilizzo	10 MB	La dimensione massima di un file di dati di utilizzo orario.

Endpoint del servizio

Application Cost Profiler è un servizio globale. Tutte le chiamate API devono essere effettuate all'endpoint Stati Uniti orientali (Virginia settentrionale).

- Stati Uniti orientali (Virginia settentrionale) – `application-cost-profiler.us-east-1.amazonaws.com`

Sicurezza inAWSApplication Cost Profiler

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

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

- La sicurezza del cloud:AWS è responsabile della protezione dell'infrastruttura che esegue i servizi AWS nel AWS Cloud. AWS fornisce, inoltre, servizi utilizzabili in modo sicuro. I revisori di terze parti testano regolarmente e verificano l'efficacia della nostra sicurezza nell'ambito dei Programmi di conformità AWS. Per ulteriori informazioni sui programmi di conformità che si applicano a Application Cost Profiler, consultaServizi AWS coperti dal programma di compliance.
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che viene utilizzato. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Questa documentazione aiuta a comprendere come applicare il modello di responsabilità condivisa quando si usaAWSApplication Cost Profiler. Viene illustrato come configurare Application Cost Profiler per soddisfare gli obiettivi di sicurezza e conformità. Viene anche illustrato come utilizzare gli altriAWSservizi che possono aiutarti a monitorare e proteggere le risorse di Application Cost Profiler.

Indice

Protezione dei dati in AWS Application Cost Profiler

Il modello di responsabilità AWS condivisa modello di si applica alla protezione dei dati in AWS Application Cost Profiler. Come descritto in questo modello, AWS è responsabile della protezione

dell'infrastruttura globale che esegue tutto l'Cloud AWS. L'utente è responsabile nel mantenere il controllo sui contenuti ospitati in questa infrastruttura. Questi contenuti comprendono la configurazione della protezione e le attività di gestione per i Servizi AWSutilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog AWS Shared Responsibility Model and GDPR nel Blog sulla sicurezza AWS.

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

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse AWS. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura la registrazione di log sulle attività di API e utenti con AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza predefiniti in 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 necessiti di moduli crittografici convalidati FIPS 140-2 quando accedi ad AWSattraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando si lavora con Application Cost Profiler o altro Servizi AWS utilizzando la console, l'API o AWS gli AWS CLI SDK. 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 a riposo

AWSApplication Cost Profiler crittografa sempre tutti i dati archiviati nel servizio a riposo senza richiedere alcuna configurazione aggiuntiva. Questa crittografia è automatica quando si utilizza Application Cost Profiler.

Per i bucket Amazon S3 che fornisci, devi crittografare il bucket di report e puoi crittografare il bucket di dati di utilizzo e consentire l'accesso ad Application Cost Profiler. Per ulteriori informazioni, consulta Configurazione dei bucket Amazon S3 per Application Cost Profiler.

Crittografia dei dati in transito

AWSApplication Cost Profiler utilizza Transport Layer Security (TLS) e la crittografia lato client per la crittografia in transito. La comunicazione con Application Cost Profiler avviene sempre tramite HTTPS, quindi i dati sono sempre crittografati in transito. Questa crittografia è configurata per impostazione predefinita quando si utilizza Application Cost Profiler.

Gestione delle identità e degli accessi per AWS Application Cost Profiler

AWS Identity and Access Management (IAM) è un Servizio AWSche consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse di Application Cost Profiler. IAM è un Servizio AWS il cui uso non comporta costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Application Cost Profiler.

Utente del servizio: se si utilizza il servizio Application Cost Profiler per svolgere il proprio lavoro, l'amministratore fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzate più funzionalità di Application Cost Profiler per svolgere il vostro lavoro, potreste 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 di Application Cost Profiler, consulta. Risoluzione dei problemi relativi AWS all'identità e all'accesso di Application Cost Profiler

Amministratore del servizio: se sei responsabile delle risorse di Application Cost Profiler presso la tua azienda, probabilmente hai pieno accesso a Application Cost Profiler. Spetta a te determinare a quali funzionalità e risorse di Application Cost Profiler 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 ulteriori informazioni su come la tua azienda può utilizzare IAM con Application Cost Profiler, consulta. Come funziona AWS Application Cost Profiler con IAM

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere policy per gestire l'accesso ad Application Cost Profiler. Per visualizzare esempi di policy basate sull'identità di Application Cost Profiler che puoi utilizzare in IAM, consulta. AWSEsempi di policy basate sull'identità di Application Cost Profiler

Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWS con le credenziali di identità. Devi essere autenticato (connesso a AWS) come utente root Utente root dell'account AWS, come utente IAM o assumere un ruolo IAM.

Puoi accedere ad AWS come identità federata utilizzando le credenziali fornite attraverso un'origine di identità. Gli utenti AWS IAM Identity Center (Centro identità IAM), l'autenticazione Single Sign-On (SSO) dell'azienda e le 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. Se accedi ad AWS tramite la federazione, assumi indirettamente un ruolo.

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

Se accedi ad AWS in modo programmatico, AWS fornisce un Software Development Kit (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le richieste utilizzando le tue credenziali. Se non utilizzi gli strumenti AWS, devi firmare le richieste personalmente. Per ulteriori informazioni sulla firma delle richieste, consulta Firma delle richieste AWS nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. AWS consiglia ad esempio di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza dell'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) in AWS nella Guida per l'utente di IAM.

Utente root di un Account AWS

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWS e le risorse nell'account. Tale identità è detta utente root Account AWS ed è possibile accedervi 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 utilizzarle 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 di IAM.

Utenti e gruppi IAM

Un utente IAM è una identità all'interno del tuo 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, per 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 di 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, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale 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 Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità all'interno di un Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un ruolo IAM nella AWS Management Console mediante lo scambio di ruoli. È possibile assumere un ruolo chiamando un'azione AWS CLI o API AWS oppure utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di 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 Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di 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 ulteriori 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, per alcuni dei Servizi AWS, è possibile collegare 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 Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso multi-servizio: alcuni Servizi AWS utilizzano funzionalità in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale 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.
  - Autorizzazioni principale: quando si utilizza un utente o un ruolo IAM per eseguire azioni in AWS, si viene considerati un principale. Le policy concedono autorizzazioni a un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le

operazioni. Per vedere se un'azione richiede azioni dipendenti aggiuntive in una policy, consulta Azioni, risorse e chiavi di condizione per i AWS servizi nel Service Authorization Reference.

- Ruolo di servizio: un ruolo di servizio è un ruolo IAM assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'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: è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste di AWS CLIo dell'API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWS a un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo dell'istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Per controllare l'accesso a AWS è possibile creare policy e collegarle a identità o risorse AWS. Una policy è un oggetto in AWS che, quando associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste policy quando un principale IAM (utente, utente root o sessione ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene archiviata in AWSsotto forma di 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 di IAM.

Gli amministratori possono utilizzare le policy AWSJSON per specificare l'accesso ai diversi elementi. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può 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'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dalla AWS Management Console, la AWS CLI o l'API AWS.

Policy basate su 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 azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le policy gestite sono policy autonome che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le policy gestite includono le policy gestite da AWS e le policy gestite dal cliente. 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 di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su 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 utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy gestite da AWS da IAM in una policy basata su risorse.

Liste di controllo degli accessi (ACL)

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

Amazon S3, AWS WAF e Amazon VPC sono esempi di servizi che supportano le ACL. Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta altri tipi di policy 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 funzione 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 di IAM.
- Policy di controllo dei servizi (SCP): le SCP sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o unità organizzativa (OU) in AWS Organizations. AWS Organizationsè un servizio per il raggruppamento e la gestione centralizzata degli Account AWSmultipli di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. La SCP limita le autorizzazioni per le entità negli account membri, compreso ogni Utente root dell'account AWS. Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations.
- 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 di IAM.

Più tipi di policy

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

Come funziona AWS Application Cost Profiler con IAM

Prima di utilizzare IAM per gestire l'accesso ad Application Cost Profiler, è necessario comprendere quali funzionalità IAM sono disponibili per l'uso con Application Cost Profiler. Per avere una visione di alto livello di come Application Cost Profiler e altri AWS servizi funzionano con IAM, consulta AWSServices That Work with IAM nella IAM User Guide.

Argomenti

- Politiche basate sull'identità di Application Cost Profiler
- Politiche basate sulle risorse di Application Cost Profiler
- Autorizzazione basata sui tag di Application Cost Profiler
- Ruoli IAM di Application Cost Profiler

Politiche basate sull'identità di Application Cost Profiler

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. Application Cost Profiler supporta azioni 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.

Azioni

Gli amministratori possono utilizzare le policy AWS JSON per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni di policy hanno spesso lo stesso nome dell'operazione API AWS. Ci sono alcune eccezioni, ad esempio le azioni 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 Application Cost Profiler utilizzano il seguente prefisso prima dell'azione:. `application-cost-profiler:` Ad esempio, per concedere a qualcuno il permesso di visualizzare i dettagli della definizione del rapporto Application Cost Profiler, includi l'`application-cost-profiler:GetReportDefinition`azione nella sua politica. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. Application Cost Profiler definisce il proprio set di azioni che descrivono le attività che è possibile eseguire con questo servizio.

Per specificare più operazioni in una singola istruzione, separarle con una virgola come mostrato di seguito.

```
"Action": [
      "application-cost-profiler:ListReportDefinitions",
      "application-cost-profiler:GetReportDefinition"
```

Di seguito sono riportate le azioni disponibili in Application Cost Profiler. Ciascuna consente l'azione dell'API con lo stesso nome. Per ulteriori informazioni sull'API Application Cost Profiler, consulta AWSApplication Cost Profiler API Reference.

- `application-cost-profiler:ListReportDefinitions`— Consente di elencare l'eventuale definizione del rapporto per l'AWSaccount.
- `application-cost-profiler:GetReportDefinition`— Consente di ottenere i dettagli della definizione del rapporto per il rapporto Application Cost Profiler.
- `application-cost-profiler:PutReportDefinition`— Consente di creare una nuova definizione di report.
- `application-cost-profiler:UpdateReportDefinition`— Consente l'aggiornamento di una definizione di report.
- `application-cost-profiler:DeleteReportDefinition`— Consente l'eliminazione di un report (disponibile solo tramite l'API Application Cost Profiler).
- `application-cost-profiler:ImportApplicationUsage`— Consente di richiedere l'importazione dei dati di utilizzo di Application Cost Profiler da un bucket Amazon S3 specificato.

Risorse

Application Cost Profiler non supporta la specificazione della risorsa Amazon Resource Names (ARNs) in una policy.

Chiavi di condizione

Application Cost Profiler non fornisce chiavi di condizione specifiche del servizio, ma supporta l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente IAM.

Esempi

Per visualizzare esempi di politiche basate sull'identità di Application Cost Profiler, vedere. AWSEsempi di policy basate sull'identità di Application Cost Profiler

Politiche basate sulle risorse di Application Cost Profiler

Application Cost Profiler non supporta politiche basate sulle risorse.

Autorizzazione basata sui tag di Application Cost Profiler

Application Cost Profiler non supporta l'etichettatura delle risorse o il controllo degli accessi in base ai tag.

Ruoli IAM di Application Cost Profiler

Un ruolo IAM è un'entità all'interno dell'account AWS che dispone di autorizzazioni specifiche.

Utilizzo di credenziali temporanee con Application Cost Profiler

È possibile utilizzare credenziali temporanee per effettuare l'accesso con la federazione, assumere un ruolo IAM o un ruolo multi-account. È possibile ottenere credenziali di sicurezza temporanee chiamando operazioni AWS STS API come o. AssumeRoleGetFederationToken

Application Cost Profiler supporta l'utilizzo di credenziali temporanee.

Ruoli collegati ai servizi

Ruoli collegati al servizio consentono ai servizi AWS di accedere a risorse in altri servizi per completare un'operazione a tuo nome. I ruoli collegati ai servizi sono visualizzati nell'account IAM e sono di proprietà del servizio. Un amministratore può visualizzare, ma non modificare le autorizzazioni dei ruoli collegati ai servizi.

Application Cost Profiler non supporta i ruoli collegati ai servizi.

Ruoli dei servizi

Questa caratteristica consente a un servizio di assumere un ruolo di servizio per conto dell'utente. Questo ruolo consente al servizio di accedere alle risorse in altri servizi per completare un'operazione per conto dell'utente. I ruoli dei servizi sono visualizzati nell'account IAM e sono di proprietà dell'account. Ciò significa che un amministratore può modificare le autorizzazioni per questo ruolo. Tuttavia, il farlo potrebbe pregiudicare la funzionalità del servizio.

Application Cost Profiler non supporta i ruoli di servizio.

AWSEsempi di policy basate sull'identità di Application Cost Profiler

Per impostazione predefinita, gli utenti e i ruoli IAM non dispongono delle autorizzazioni per creare o modificare AWS le risorse di Application Cost Profiler. Inoltre, non possono eseguire attività utilizzandoAWS Management Console, AWS Command Line Interface (AWS CLI) o AWS API. Un amministratore deve creare policy IAM che concedano a utenti e ruoli l'autorizzazione a eseguire le operazioni API specifiche di cui hanno bisogno. L'amministratore deve quindi allegare queste policy a utenti o IAM che richiedono tali autorizzazioni.

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

Argomenti

Best practice delle policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse di Application Cost Profiler 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:

- Nozioni di base sulle policy gestite da AWSe passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le

policy gestite da AWSche concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWSspecifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.

- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di servizio, ma solo se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di 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 IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo Account AWS, attiva 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 Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

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

Utilizzo della console Application Cost Profiler

Per accedere alla console AWS Application Cost Profiler, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentire all'utente di elencare e visualizzare i dettagli sulle risorse di Application Cost Profiler presenti nell'account. AWS Se crei una policy basata su

identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti e ruoli IAM) associate a tale policy.

Per garantire che tali entità possano utilizzare la console di Application Cost Profiler per visualizzare la definizione del rapporto Application Cost Profiler per l'AWSaccount, assegna le seguenti autorizzazioni alle entità.

```
application-cost-profiler:ListReportDefinitions
application-cost-profiler:GetReportDefinition
```

Ad esempio, è possibile creare la seguente politica per gli utenti di sola lettura.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "application-cost-profiler:ListReportDefinitions",
            "application-cost-profiler:GetReportDefinition"
         ],
         "Resource":"*"
      }
   ]
}
```

Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Non sono necessarie le autorizzazioni minime della console per gli utenti che effettuano chiamate solo all'API di AWS CLI o di AWS. Al contrario, puoi accedere solo alle operazioni che soddisfano l'operazione API che stai cercando di eseguire.

Consentire agli utenti di visualizzare le loro autorizzazioni

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

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

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

Accesso a un bucket Amazon S3

In questo esempio, vuoi concedere a un utente IAM del tuo AWS account l'accesso a uno dei tuoi bucket Amazon S3,. `examplebucket` Si vuole anche consentire all'utente di aggiungere, aggiornare ed eliminare oggetti.

Oltre ad assegnare le autorizzazioni `s3:PutObject`, `s3:GetObject` e `s3:DeleteObject` all'utente, la policy assegna anche le autorizzazioni `s3:ListAllMyBuckets`, `s3:GetBucketLocation` e `s3:ListBucket`. Queste sono le autorizzazioni aggiuntive richieste dalla console. Inoltre, le operazioni `s3:PutObjectAcl` e `s3:GetObjectAcl` sono necessarie per essere in grado di copiare, tagliare e incollare gli oggetti nella console. Per una procedura dettagliata

di esempio che concede le autorizzazioni agli utenti e ne esegue il test utilizzando la console, consulta Una procedura guidata di esempio: utilizzo delle policy utente per controllare l'accesso al bucket .

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListBucketsInConsole",
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets"
         ],
         "Resource":"arn:aws:s3:::*"
      },
      {
         "Sid":"ViewSpecificBucketInfo",
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetBucketLocation"
         ],
         "Resource":"arn:aws:s3:::examplebucket"
      },
      {
         "Sid":"ManageBucketContents",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetObject",
            "s3:GetObjectAcl",
            "s3:DeleteObject"
         ],
         "Resource":"arn:aws:s3:::examplebucket/*"
      }
   ]
}
```

Risoluzione dei problemi relativi AWS all'identità e all'accesso di Application Cost Profiler

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con AWS Application Cost Profiler e (IAM). AWS Identity and Access Management

Argomenti

Non sono autorizzato a eseguire un'azione in Application Cost Profiler

Se la AWS Management Console indica che non hai l'autorizzazione a eseguire un'operazione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è colui che ti ha fornito le credenziali di accesso.

Il seguente errore di esempio si verifica quando l'utente `mateojackson` IAM tenta di utilizzare la console per visualizzare i dettagli sul report di Application Cost Profiler ma non dispone `application-cost-profiler:ListReportDefinitions` dell'autorizzazione.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 application-cost-profiler:ListReportDefinitions on resource: Report Definition
```

In questo caso, Mateo chiede al suo amministratore di aggiornare le sue politiche per consentirgli di accedere alla risorsa di definizione del report utilizzando l'`application-cost-profiler:ListReportDefinitions`azione.

Non sono autorizzato a eseguire iam: PassRole

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

Alcuni Servizi AWSconsentono di trasmettere un ruolo esistente a tale servizio, invece di creare un nuovo ruolo di servizio o un ruolo collegato ai servizi. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Application Cost Profiler. 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`.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne al mio AWS account di accedere alle risorse di My Application Cost Profiler

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

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Application Cost Profiler supporta queste funzionalità, consulta. Come funziona AWS Application Cost Profiler con IAM
- Per informazioni su come garantire l'accesso alle risorse negli Account AWSche possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS in tuo possesso nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso alle risorse ad Account AWS di terze parti, consulta Fornire l'accesso agli Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.

- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Convalida della conformità per AWS Application Cost Profiler

Per sapere se il Servizio AWSè coperto da programmi di conformità specifici, consulta i Servizi AWScoperti dal programma di conformità e scegli il programma di conformità desiderato. Per informazioni generali, consulta Programmi per la conformità di AWS.

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

La responsabilità di conformità durante l'utilizzo dei Servizi AWSè determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle normative vigenti. Per semplificare il rispetto della conformità, AWSmette a disposizione le seguenti risorse:

- Guide Quick Start per la sicurezza e conformità: queste guide all'implementazione illustrano considerazioni relative all'architettura e forniscono la procedura per l'implementazione di ambienti di base su AWSincentrati sulla sicurezza e sulla conformità.
- Architetture per la sicurezza e la conformità HIPAA su Amazon Web Services: questo whitepaper descrive come le aziende possono utilizzare AWSper creare applicazioni conformi alla normativa HIPAA.

  > **Note**
  >
  > Non tutti i Servizi AWSsono conformi ai requisiti HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- Risorse per la conformità AWS: una raccolta di cartelle di lavoro e guide suddivise per settore e area geografica.
- Valutazione delle risorse con le regole nella Guida per gli sviluppatori di AWS Config: il servizio AWS Configvaluta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti.
- AWS Security Hub: questo Servizio AWSfornisce una visione completa dello stato di sicurezza all'interno di AWS. La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWSe 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.

- AWS Audit Manager: questo Servizio AWSaiuta a verificare continuamente l'utilizzo di AWSper semplificare la gestione dei rischi e della conformità alle normative e agli standard di settore.

Resilienza inAWSApplication Cost Profiler

L'infrastruttura globale di AWS è basata su regioni AWS e zone di disponibilità. Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, connesse tramite reti altamente ridondanti, a bassa latenza e throughput elevato. 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 a data center singolo o multiplo.

Per ulteriori informazioni sulle regioni AWS e sulle zone di disponibilit, consulta Infrastruttura globale di AWS.

Sicurezza dell'infrastruttura inAWSApplication Cost Profiler

Come servizio gestito,AWSApplication Cost Profiler è protetto daAWSsicurezza globale della rete. Per informazioni sui servizi di sicurezza AWS e su come AWS protegge l'infrastruttura, consulta la pagina Sicurezza del cloud AWS. Per progettare l'ambiente AWS utilizzando le best practice per la sicurezza dell'infrastruttura, consulta la pagina Protezione dell'infrastruttura nel Pilastro della sicurezza di AWS Well-Architected Framework.

Tu usiAWSchiamate API pubblicate per accedere ad Application Cost Profiler tramite la rete. I clienti devono supportare quanto segue:

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

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

Monitoraggio degli eventi di profiler costo applicazione EventBridge

Puoi usare Amazon EventBridge per automatizzare il tuoAWSe rispondono automaticamente a eventi di sistema, come i problemi relativi alla disponibilità delle applicazioni o le modifiche delle risorse. Eventi diAWSi servizi vengono erogati a EventBridge quasi in tempo reale. Puoi compilare regole semplici che indichino quali eventi sono considerati di interesse per te e quali operazioni automatizzate intraprendere quando un evento corrisponde a una regola. Per ulteriori informazioni, consultaAmazon EventBridge Guida per l'utente di.

Puoi monitorareAWSEventi di profiler costo applicazione EventBridge. EventBridge indirizza i dati a destinazioni comeAWS Lambdae Amazon Simple Notification Service (Amazon SNS). Questi eventi sono gli stessi di quelli che appaiono su Amazon CloudWatch Eventi, che offre un near-real-time flusso di eventi di sistema che descrivono le modifiche apportateAWSrisorse AWS.

Monitoraggio della generazione di report con EventBridge

con EventBridge, è possibile creare regole che definiscono le operazioni da eseguire quando Application ost applicazione Ad esempio, è possibile creare una regola per ricevere un messaggio di posta elettronica ogni volta che viene generato un report.

Per monitorare la generazione di report

1. Effettua il loginAWSutilizzando un account che dispone delle autorizzazioni per utilizzare entrambi EventBridge e di profiler costo applicazione
2. Apri Amazon EventBridge consolehttps://console.aws.amazon.com/events/.
3. Utilizzando i seguenti valori, creare un EventBridge regola che monitora gli eventi creati quando viene generato un report:

   - Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).
   - PerOrigine eventi, scegliAltro.
   - NellaModello di eventisezione, scegliModelli personalizzati (editor JSON)e quindi incollare il modello di eventi seguente nell'area di testo:

     ```
     {
     ```

```
  "source": ["aws.application-cost-profiler"],
  "detail-type": ["Application Cost Profiler Report Generated"]
}
```

- PerTipi di target, scegliAWSservizioe perSeleziona un target, scegli ilAWSservizio che vuoi agire quando EventBridge rileva un evento del tipo selezionato. La destinazione viene attivata quando viene ricevuto un evento che corrisponde al modello di evento definito nella regola.

Per ulteriori informazioni sulla creazione di regole, consultaCreazione di Amazon EventBridge regole che reagiscono agli eventinellaAmazon EventBridge Guida per l'utente di.

Esempio di un evento generato da report

Questo evento ti informa quando un report viene generato e pronto per essere recuperato. La`message`fornisce il bucket e la chiave Amazon Simple Storage Service (Amazon S3) per l'oggetto Amazon S3 in cui è archiviato il report.

```
{
   "version": "0",
   "id": "01234567-EXAMPLE",
   "detail-type": "Application Cost Profiler Report Generated",
   "source": "aws.application-cost-profiler",
   "account": "123456789012",
   "time": "2021-03-31T10:23:43Z",
   "region": "us-east-1",
   "resources": [],
   "detail": {
     "message": "Application Cost Profiler report delivered in bucket: SampleBucket,
 key: SampleReport-112233445566"
   }
}
```

Cronologia dei documenti

La tabella seguente descrive le versioni della documentazione perAWSApplication Cost Profiler.

Modifica	Descrizione	Data
Notifica di obsolescenza del servizio	AWSApplication Cost Profiler verrà interrotto entro il 30 settembre 2024 e non accetta più nuovi clienti.	11 agosto 2023
Eventi di monitoraggio	A causa delle modifiche apportate alEventBridgeconsole, il modo in cui si creano le regole per monitorare gli eventi di Application Cost Profiler è cambiato. Per ulteriori informazioni, consulta, Monitoraggio degli eventi di Application Cost Profiler inEventBridge.	5 luglio 2022
Aggiornamenti ad esempi di policy relative ai bucket S3	Aggiornamento solo della documentazione agli esempi di policy sui bucket S3. Per ulteriori informazioni, consultaConfigurazione dei bucket Amazon S3 per Application Cost Profiler.	6 dicembre 2021
Disponibilità generale	La versione pubblica iniziale di Application Cost Profiler.	13 maggio 2021