AWS Billing Conductor

Guida per l'utente

AWS Billing Conductor: Guida per l'utente

Table of Contents

Cosa èAWSBilling Conductor?

AWSBilling Conductor è un servizio completamente gestito in grado di supportare i flussi di lavoro di showback e chargeback diAWSSolution Provider e clienti aziendali. Utilizzo diAWSBilling Conductor, puoi personalizzare i tuoi dati di fatturazione mensili. La console modella la relazione di fatturazione tra te e i tuoi clienti o le tue unità aziendali. Puoi anche personalizzare una versione pro forma dei tuoi dati di fatturazione ogni mese per mostrare o riaddebitare con precisione i tuoi clienti.AWS Billing Conductor non modifica il modo in cui Amazon Web Services ti fattura ogni mese. Invece, fornisce un meccanismo per configurare, generare e visualizzare le tariffe per determinati clienti in un determinato periodo di fatturazione. Puoi anche usarlo per analizzare la differenza tra i tassi che applichi ai tuoi raggruppamenti contabili rispetto ai tassi effettivi daAWS. Come risultato del tuoAWSConfigurazione Billing Conductor, l'account pagatore può anche visualizzare la tariffa personalizzata applicata nella pagina dei dettagli di fatturazione delAWSBilling Consoleoppure configura un rapporto sui costi e sull'utilizzo per gruppo di fatturazione.

È possibile configurare i gruppi di fatturazione e i piani tariffari utilizzando ilAWSBilling Conductoro ilAWSAPI Billing Conductor.

Per ulteriori informazioni suAWSQuote del servizio Billing Conductor, consultaQuote e restrizioni (p. 40).

Argomenti

- Funzionalità inAWSBilling Conductor (p. 1)
- Servizi correlati (p. 1)

Funzionalità inAWSBilling Conductor

Puoi utilizzare il pluginAWSBilling Conductor consente di eseguire le seguenti operazioni:

- Raggruppa i tuoi account in una serie di account che si escludono a vicenda (gruppi di fatturazione). Questi gruppi vengono utilizzati per fornire una vista aggregata di un set di account. Inoltre, la fattura di ciascun gruppo di fatturazione viene calcolata come fattura cliente autonoma. Ciò consente la condivisione localizzata dei vantaggi delle istanze riservate e dei Savings Plans, della suddivisione in livelli di volume, degli sconti eAWSPiano gratuito.
- Applica piani tariffari personalizzati: maggiorazioni o sconti globali e specifici per servizi relativi alle tariffe On-Demand.
- Crea e applica addebiti o crediti una tantum ai tuoi gruppi di fatturazione. Questi elementi di linea personalizzati possono essere creati come elementi piatti o in percentuale.
- Analizza i costi pro forma in base alla configurazione dei prezzi per ogni gruppo di fatturazione nelAWSBilling Console dettagli di fatturazionepagina.
- Configura un rapporto pro forma su costi e utilizzo per ogni gruppo di fatturazione.
- Analizza month-to-date e differenze storiche tra le tariffe applicate ai gruppi di fatturazione rispetto a quelle effettiveAWStariffe utilizzando ilReport del margine del gruppo di fatturazione. Per ulteriori informazioni, consulta la pagina Analisi dei margini per gruppo di fatturazione (p. 15) .

Servizi correlati

AWSBilling Console

IlAWSLa console di fatturazione è il portale per tuttiAWSclienti, da studenti e startup a grandi imprese. È possibile utilizzare la console per visualizzare le risorse in esecuzione nelAWSaccount, gestisci le

preferenze di fatturazione e accedi agli elementi di fatturazione necessari per effettuare pagamenti aAWS. IlAWSLa console di fatturazione fornisce anche una spiegazione dettagliata della spesa per il tuo account e funge da punto di accesso per l'iscrizione ai prodotti delAWSProdotti per la gestione dei costi.

Per ulteriori informazioni, consulta la Guida per l'utente AWS Billing.

Report di costi e utilizzo AWS

IlAWSReport di costi e utilizzo (AWSCUR) contengono il set più completo di dati di costo e utilizzo disponibili. Puoi utilizzare i report su costi e utilizzo per pubblicare i tuoiAWSreport di fatturazione in un bucket Amazon Simple Storage Service (Amazon S3) di cui sei proprietario. Puoi ricevere report che suddividono i costi per ora o giorno, per prodotto o risorsa di prodotto o per tag che definisci tu stesso.

AWSaggiorna il report nel bucket una volta al giorno in formato CSV (valori separati da virgola) o Apache Parquet. È possibile visualizzare i report utilizzando un software per fogli di calcolo come Microsoft Excel o Apache OpenOffice Calc. Puoi anche accedervi da un'applicazione utilizzando le API Amazon S3 o Amazon Athena.

AWSI report di costi e utilizzo consentono di monitorareAWSutilizza e fornisci una stima delle spese associate all'account. Il report contiene voci per ciascuna combinazione univoca di prodotti AWS, tipo di utilizzo e operazione utilizzata dal tuo account AWS.

AWS Identity and Access Management (IAM)

IlAWSIl servizio Billing Conductor è integrato conAWS Identity and Access Management(MIRINO). Puoi utilizzare IAM conAWSBilling Conductor per assicurarti che le altre persone che utilizzano il tuo account dispongano soltanto dell'accesso necessario a svolgere il loro lavoro.

Puoi anche usare IAM per controllare l'accesso a tutti i tuoiAWSrisorse. Ciò include, a titolo esemplificativo, i dati di fatturazione. È importante familiarizzare con i concetti di base e le best practice di IAM prima di andare avanzare troppo con la configurazione della struttura del tuo account AWS.

Per ulteriori informazioni su come lavorare con IAM, consultaChe cos'è IAM?eBest practice di sicurezza in IAMnelIAM User Guide.

AWS OrganizationsFatturazione consolidata

AWSi prodotti e i servizi possono ospitare aziende di ogni dimensione, dalle piccole startup alle imprese. Se la tua società è di grandi dimensioni o in espansione, puoi configurare più account AWS per rifletterne la struttura. Ad esempio, è possibile disporre di un account per l'intera società e un account per ciascun dipendente oppure di un account per l'intera società con utenti IAM per ciascun dipendente. È possibile avere un account per l'intera azienda, account per ciascun reparto o team all'interno della società e account per ciascun dipendente.

Se si creano più account, è possibile utilizzare la funzione di fatturazione consolidata diAWS Organizationsper riunire tutti i tuoi account membri in un unico account di gestione e ricevere un'unica fattura. Per ulteriori informazioni, consulta la paginaFatturazione consolidata per OrganizationsnelAWS BillingGuida per l'utente di.

Comprendere il tuoAWSBilling Conductor

IlAWSLa dashboard di Billing Conductor fornisce un riepilogo di alto livello delle metriche chiave per aiutarti a comprendere l'impatto delle dimensioni dei tuoi prezzi personalizzati.

Indicatori chiave di performance

Questa sezione definisce gli indicatori chiave di prestazione (KPI) disponibili sulAWSBilling Conductor. I KPI sono tutti month-to-date. Man mano che crei o aggiungi account al tuoAWS Organizations, gli account vengono assegnati a questo KPI. Quando elimini un gruppo di fatturazione, anche gli account in quel gruppo di fatturazione vengono attribuiti a questo KPI.

- Importo addebitato— L'importo totale del mese corrente per l'utilizzo maturato da tutti i gruppi di fatturazione, in base alla tariffa personalizzata definita dai piani tariffari applicati. Il calcolo non tiene conto degli sconti basati sugli impegni acquistati al di fuori del gruppo di fatturazione, delle tariffe non pubbliche o del credito consumato nel dominio fatturabile. Esempi di sconti basati su impegni includono istanze riservate e Savings Plans
- AWScosti— Il combinato month-to-date addebito per l'utilizzo maturato da tutti i gruppi di fatturazione, in base agli addebiti stimati sulAWSfattura. I calcoli includono eventuali sconti basati sugli impegni acquistati al di fuori del gruppo di fatturazione se tali vantaggi sono stati applicati nel dominio fatturabile, eventuali prezzi non pubblici, sconti per livelli di volume e crediti. Esempi di sconti basati su impegni includono istanze riservate e Savings Plans
- Margine— L'aggregato month-to-date margine maturato da tutti i gruppi di fatturazione. Il margine viene calcolato sottraendo ilAWScosti derivanti dall'importo addebitato. In base a fattori quali il piano tariffario e le voci personalizzate applicate, il margine può anche essere negativo.

  Note

  Le rettifiche successive al periodo di fatturazione influiscono sui margini storici. Per ulteriori informazioni, consulta la pagina Analisi dei margini per gruppo di fatturazione (p. 15) .
- Gruppi di fatturazione— Il numero di gruppi di account che si escludono a vicenda, con un account principale e un piano tariffario associato.
- Account— Il numero di account all'interno di una famiglia di fatturazione consolidata.
- Account non monitorati— Il numero di account all'interno di una famiglia di fatturazione consolidata che non sono stati assegnati a un gruppo di fatturazione.

Altre definizioni perAWSBilling Conductor

Questa sezione definisce altri termini che vengono utilizzati dappertutto.AWSBilling Conductor per aiutarti a utilizzare il servizio in modo efficace.

- Fatturabile— L'output di fatturazione generato daAWSe usato come pregiudizio per calcolare il tuoAWSfattura.
- Proforma— L'output generato daAWSBilling Conductor. È coerente con le modifiche desiderate nella gestione delle tariffe (configurazione dei prezzi) e nella visibilità aggregata dell'account (gruppi di fatturazione).

- Resource Group— Gli input utilizzati per calcolare le voci personalizzate in base alla percentuale. I valori delle risorse includono i costi accumulati per il gruppo di fatturazione e tutti gli articoli a riga fissa personalizzati associati a un determinato gruppo di fatturazione per un periodo di fatturazione.

Visualizzazione dei cinque gruppi di fatturazione principali per importo addebitato

Puoi comprendere i cinque principali gruppi di fatturazione che generano entrate facendo riferimento alla visualizzazione visiva e alla visualizzazione tabellare. Per gestire i gruppi di fatturazione esistenti, scegliGestisci i gruppi di fatturazionenella pagina del pannello di controllo.

Creazione di gruppi di fatturazione, configurazioni di prezzo e voci personalizzate

Questa sezione mostra come creare gruppi di fatturazione, configurazioni dei prezzi e voci personalizzate inAWSBilling Conductor Ogni sezione fornisce anche una panoramica su come utilizzare la tabella dei gruppi di fatturazione, la tabella delle regole di determinazione dei prezzi e la tabella delle voci personalizzate dopo aver creato ciascun articolo.

Argomenti

Creazione di gruppi di fatturazione

È possibile utilizzareAWSBilling Conductor per creare gruppi di fatturazione per organizzare i tuoi account. Per impostazione predefinita, gli account pagatori con autorizzazioni di amministratore possono creare gruppi di fatturazione. Ogni gruppo di fatturazione si esclude a vicenda. Ciò significa che un account può appartenere a un solo gruppo di fatturazione in un determinato periodo di fatturazione. Sebbene sia possibile visualizzare immediatamente la segmentazione del gruppo di fatturazione, sono necessarie fino a 24 ore dopo la creazione di un gruppo di fatturazione per visualizzare le tariffe personalizzate del gruppo.

> **Note**
>
> Il trasferimento degli account tra i gruppi di fatturazione a metà mese avvierà il ricalcolo di entrambi i gruppi di fatturazione all'inizio del periodo di fatturazione. Lo spostamento degli account a metà mese non influisce sui periodi di fatturazione precedenti.

Per creare un gruppo di fatturazione, segui i seguenti passaggi.

Per creare un gruppo di fatturazione

1. Accedi allaAWS Management Consolee apriAWSBilling Conductorhttps://console.aws.amazon.com/billingconductor/.
2. Nel riquadro di navigazione, scegliereGruppi di fatturazione.
3. ScegliCreazione di un gruppo di fatturazione.
4. PerDettagli di fatturururururur, immetti il nome del gruppo di fatturazione. Per le restrizioni relative ai nomi, vedereQuote e restrizioni (p. 40).
5. (Facoltativo) PerDescription (Descrizione), immetti una descrizione per il gruppo di fatturazione.
6. PerPiani tariffari, scegli un piano tariffario da associare al gruppo di fatturazione. Per creare un piano di determinazione dei prezzi, consultaCreazione di piani tariffari (p. 7).

7. SottoAccount, scegliere uno o più account da aggiungere al gruppo di fatturazioneoscegliereImporta unità organizzativa di importazioneper selezionare automaticamente gli account che si trovano all'interno di un'unità organizzativa. Per un esempio di policy per concedere l'accesso alla funzione di importazione delle unità organizzative, vedereGrantAWSAccesso a Billing Conductor alla funzionalità unità organizzativa (OU) di importazione (p. 33).

   Puoi utilizzare il filtro della tabella per ordinare in base ai nomi degli account, agli ID degli account o all'indirizzo email principale associato a un account.
8. PerSelezione dell'account principale, scegli un account come account principale per un gruppo di fatturazione.

   L'account principale eredita la possibilità di visualizzare costi e utilizzo pro forma in tutto il gruppo di fatturazione e può generare report di costi e utilizzo proforma (AWSCUR) per il gruppo di fatturazione.

   Note

   Devi selezionare il tuo account principale nel passaggio 7. Non puoi modificare il tuo account principale dopo aver creato il gruppo di fatturazione. Per assegnare un nuovo account principale, elimina il gruppo di fatturazione e raggruppa i tuoi account. Sebbene un conto pagatore possa essere incluso in un gruppo di fatturazione, a un conto pagatore non può essere assegnato il ruolo di account principale.
9. ScegliCreazione di un gruppo di fatturazione.

Tabella di fatturururururur

Dopo aver creato un gruppo di fatturazione, è possibile visualizzare i dettagli del gruppo di fatturazione in una tabella filtrabile. È possibile filtrare utilizzando le seguenti dimensioni:

- Nome di fatturururururur
- Nome dell'account principale
- ID dell'account principale
- Numero di account
- Nome del piano tariffario

Per visualizzare i dettagli per ogni gruppo di fatturazione, scegli il nome del gruppo di fatturazione nella tabella.

Creazione di regole personalizzate personalizzate

Puoi creare regole di prezzo inAWSBilling Conductor per personalizzare le tariffe di fatturazione in tutti i gruppi di fatturazione. Le regole di determinazione dei prezzi possono essere globali o specifiche del servizio. Per impostazione predefinita, un account pagatore con autorizzazioni di amministratore può creare regole di prezzo. Sono necessarie fino a 24 ore dall'applicazione di una regola di determinazione del prezzo a un gruppo di fatturazione per visualizzare le tariffe personalizzate per il gruppo di fatturazione.

Un unico piano tariffario può essere applicato a più gruppi di fatturazione.

Note

L'aggiornamento di una regola di determinazione dei prezzi aggiorna anche tutti i piani tariffari a cui è associata la regola di determinazione Un piano tariffario è una raccolta di regole tariffarie. Se il piano tariffario è associato a un gruppo di fatturazione o a un insieme di gruppi di fatturazione, questa modifica riguarda solo il periodo di fatturazione corrente. I periodi di fatturazione precedenti rimangono invariati.

Per creare una regola di determinazione dei prezzi, segui i seguenti passaggi.

Per creare una regola di determinazione dei prezzi

1. AprireAWSBilling Conductorhttps://console.aws.amazon.com/billingconductor/.
2. Nel riquadro di navigazione, scegliereConfigurazione di prezzi.
3. Scegli ilRegola di prezziTabulatore.
4. ScegliCreazione di regole tariffari.
5. PerDettagli di determinazione dei prezzi, inserisci il nome della regola di assegnazione del prezzo. Per le restrizioni relative ai nomi, vedereQuote e restrizioni (p. 40).
6. (Facoltativo) PerDescription (Descrizione), immetti una descrizione per la regola di determinazione dei prezzi.
7. PerScope, scegli`Global`o`Service`.

   - Globale: si applica a tutti gli usi.
   - Servizio: si applica solo a un determinato servizio. Quando scegli il servizio, scegli un codice di servizio per configurare le tariffe tariffarie.
8. PerType (Tipo), scegli uno dei dueDiscountsoMarkup.
9. PerPercentuale, inserire l'importo percentuale.

   Se si entra**0**in percentuale, il piano tariffario predefinito èAWSTariffa on-demand.
10. (Facoltativo) Per creare un'altra regola di determinazione del prezzo nello stesso flusso di lavoro, scegliAggiungere una regola di determinazione.
11. ScegliCreazione di regole tariffari.

Tabella di determinazione dei prezzi

Dopo aver creato una regola di determinazione dei prezzi, è possibile visualizzare i dettagli della regola di determinazione dei prezzi in una tabella filtrabile. È possibile filtrare in base alle seguenti dimensioni:

- Nome di determinazione dei prezzi
- Ambito
- Codice di servizio
- Tariffa

Creazione di piani tariffari

Puoi creare piani tariffari inAWSBilling Conductor per personalizzare l'output dei dati di fatturazione in tutti i gruppi di fatturazione. Per impostazione predefinita, un account pagatore con autorizzazioni di amministratore può creare piani tariffari. Sono necessarie fino a 24 ore dall'applicazione di un piano tariffario a un gruppo di fatturazione per visualizzare le tariffe personalizzate per il gruppo di fatturazione.

Un unico piano tariffario può essere applicato a più gruppi di fatturazione.

> Note
>
> L'aggiornamento di un piano tariffario influisce anche sui dettagli di fatturazione di ciascun gruppo di fatturazione a cui è associato il piano tariffario. Se il piano tariffario è associato a un gruppo di fatturazione o a un insieme di gruppi di fatturazione, questa modifica riguarda solo il periodo di fatturazione corrente. I periodi di fatturazione precedenti rimangono invariati.

Per creare un piano di determinazione dei prezzi, segui i seguenti passaggi.

Per creare un piano di determinazione dei prezzi

1. AprireAWSBilling Conductorhttps://console.aws.amazon.com/billingconductor/.
2. Nel riquadro di navigazione, scegliereConfigurazione dei prezzi.
3. DaPiani tariffarischeda, scegliCreazione di un piano tariffario.
4. PerDettagli del piano tariffario, inserisci il nome del piano tariffario. Per le restrizioni relative ai nomi, vedereQuote e restrizioni (p. 40).
5. (Facoltativo) PerDescription (Descrizione), immetti una descrizione per il piano di determinazione dei prezzi.
6. NelTabella delle regole tariffarie, scegli le regole tariffarie che desideri associare al piano tariffario. Puoi filtrare le regole di determinazione dei prezzi in base al nome, all'ambito, al codice del servizio o alla tariffa.
7. ScegliCreazione di un piano tariffario.

Tabella del piano tariffario

Dopo aver creato un piano tariffario, è possibile visualizzare i dettagli del piano tariffario in una tabella filtrabile. È possibile filtrare in base alle seguenti dimensioni:

- Il nome del piano tariffario
- Descrizione
- Il numero di regole tariffarie associate al piano tariffario

Creazione di voci personalizzate per gruppo di fatturazione

È possibile utilizzareAWSBilling Conductor per creare articoli di linea personalizzati e associarli a un gruppo di fatturazione. Utilizzando articoli di linea personalizzati, puoi allocare manualmente costi e sconti a tua discrezione. Le voci personalizzate possono essere calcolate utilizzando iladdebitooaddebitovalori. È possibile configurare l'elemento di riga personalizzato basato sulla percentuale per includere o escludere risorse. Queste risorse possono includere il costo del gruppo di fatturazione e altri articoli personalizzati fissi associati a un gruppo di fatturazione per un determinato periodo di fatturazione.

I casi d'uso comuni per la creazione di articoli di linea personalizzati includono, a titolo esemplificativo, i seguenti:

- Allocazione diAWS Supporttariffe
- Allocazione dei costi del servizio condiviso
- Applicazione delle tariffe dei servizi gestiti
- Applicazione di una tassa
- Distribuzione di crediti
- Distribuzione dei risparmi relativi al RI e ai piani di risparmio (anziché su richiesta)
- Aggiungere crediti organizzativi ed elementi delle linee di discount

Creazione di una riga personalizzata a pagamento

Utilizza i passaggi seguenti per creare una riga personalizzata che applichi una riga di credito o di commissione a un singolo gruppo di fatturazione.

Per creare una riga personalizzata

1. AprireAWSBilling Conductorhttps://console.aws.amazon.com/billingconductor/.
2. Nel riquadro di navigazione, scegliereVoci personalizzate.
3. ScegliCreazione di voci personalizzate.
4. PerDettagli personalizzate, immetti il nome della riga personalizzata. Per le restrizioni relative ai nomi, vedereQuote e restrizioni (p. 40).
5. PerDescription (Descrizione), immetti una descrizione per la riga personalizzata. Il limite di caratteri è 255.
6. PerPeritariffururur, scegli il periodo di fatturazione esistente o il periodo di fatturazione precedente.
7. PerGrupuppi di, scegliere un gruppo di fatturazione. È possibile associare l'adcede personalizzata solo a un gruppo di fatturazione alla volta.
8. ScegliSupport diper il tuoTipo di costo.
9. Scegli unvalore di costoe inserisci un importo in ingresso.

   Un articolo in discount aggiunge un credito. Ciò riduce l'importo addebitato al gruppo di fatturazione selezionato. Una voce di markup aggiunge un addebito. Ciò aumenta l'importo addebitato al gruppo di fatturazione selezionato. Tutti gli articoli personalizzati sono in USD.
10. Scegli Crea.

Creazione di una voce personalizzata con addebito percentuale

Utilizza i passaggi seguenti per creare una riga personalizzata che applichi una riga di credito o di commissione a un singolo gruppo di fatturazione.

Per creare una riga personalizzata

1. AprireAWSBilling Conductorhttps://console.aws.amazon.com/billingconductor/.
2. Nel riquadro di navigazione, scegliereVoci personalizzate.
3. ScegliCreazione di voci personalizzate.
4. PerDettagli personalizzate, immetti il nome della riga personalizzata. Per le restrizioni relative ai nomi, vedereQuote e restrizioni (p. 40).
5. PerDescription (Descrizione), immetti una descrizione per la riga personalizzata. Il limite di caratteri è 255.
6. PerPeritariffururur, scegli il periodo di fatturazione esistente o il periodo di fatturazione precedente.
7. PerGrupuppi di, scegliere un gruppo di fatturazione. È possibile associare l'adcede personalizzata solo a un gruppo di fatturazione alla volta.
8. Scegliaddebitoper il tuoTipo di costo.
9. Scegli unvalore di costoe inserisci un importo in ingresso.

   Un articolo in discount aggiunge un credito. Ciò riduce l'importo addebitato al gruppo di fatturazione selezionato. Una voce di markup aggiunge un addebito. Ciò aumenta l'importo addebitato al gruppo di fatturazione selezionato. Tutti gli articoli della linea personalizzata sono in USD.
10. (Facoltativo) Scegliete i valori delle risorse che desiderate includere nel calcolo. Per impostazione predefinita, il plugin`billing group cost`è selezionata come risorsa. Sono esclusi tutti gli articoli con linee personalizzate piatte.
11. (Facoltativo) Includi uno o più articoli con linee personalizzate piatte. Scegli ogni elemento a riga piatta personalizzata applicabile dalla tabella che desideri includere nel calcolo basato sulla percentuale.

Note

È possibile creare voci personalizzate in percentuale senza risorse associate. Questi voci personalizzate vengono visualizzate come`$0.00`valore nei dati di fatturazione.

12. Scegli Crea.

Tabella delle voci personalizzate

Dopo aver creato un elemento di riga personalizzato, è possibile visualizzare i dettagli dell'elemento riga in una tabella filtrabile. È possibile filtrare in base alle seguenti dimensioni:

- Il nome dell'elemento di riga
- La descrizione dell'Riga
- L'importo addebitato
- Il gruppo di fatturazione a cui è attribuita la voce
- La data di creazione della voce

Per visualizzare le voci personalizzate che hai creato nei periodi di fatturazione precedenti, utilizza ilData seltorelenco a discesa.

Come modificare voci personalizzate

Per modificare voci personalizzate, completa la procedura riportata di seguito.

Come modificare una riga personalizzata

1. AprireAWSBilling Conductorhttps://console.aws.amazon.com/billingconductor/.
2. Nel riquadro di navigazione, scegliereVoci personalizzate.
3. ScegliCreazione di voci personalizzate.
4. Scegliere la riga personalizzata che si desidera modificare.
5. Scegli Modifica.
6. Cambia i parametri che intendi modificare.

   Note

   Non puoi modificare il periodo di fatturazione, il gruppo di fatturazione, il tipo di addebito (fisso o percentuale) o il tipo di valore dell'addebito (credito o commissione).
7. Sceglie Save changes (Salva modifiche).

Eliminazione di voci personalizzate personalizzate

Per eliminare voci personalizzate, completa la procedura riportata di seguito.

Come modificare una riga personalizzata

1. AprireAWSBilling Conductorhttps://console.aws.amazon.com/billingconductor/.
2. Nel riquadro di navigazione, scegliereVoci personalizzate.
3. ScegliCreazione di voci personalizzate.

4. Scegliere la riga personalizzata da eliminare.
5. Sceglieliminare.
6. Leggi in che modo l'eliminazione dell'elemento di riga personalizzato potrebbe influire su di te, quindi scegliEliminare voci personalizzate.

Best practice perAWSBilling Conductor

Questa sezione evidenzia alcune best practice per quando lavori conAWSBilling Conductor.

Argomenti

Controllo dell'accesso aAWSBilling Conductor

La gestione della fatturazione e dei costi è accessibile solo agli utenti che hanno accesso all'account pagatore o di gestione. Per concedere agli utenti IAM l'autorizzazione a creare gruppi di fatturazione e vedere ilAWSBilling Conductor Key Performance Indicators (KPI) nella console di Billing and Cost Management, devi inoltre concedere agli utenti IAM quanto segue:

- Elenca gli account nelle Organizations

Per ulteriori informazioni su come concedere agli utenti la possibilità di creare gruppi di fatturazioneAWSConsole Billing Conductor, vediGestione delle identità e degli accessi perAWSBilling Conductor (p. 21).

Puoi anche creareAWSRisorse Billing Conductor utilizzando programmaticamente ilAWSBilling Conductor. Quando si configura l'accesso alAWSAPI Billing Conductor: ti consigliamo di creare un utente IAM univoco per consentire l'accesso programmatico. In tal modo puoi definire controlli degli accessi più precisi tra chi nella tua organizzazione ha accesso alAWSConsole Billing Conductor e API. Per fornire a più utenti IAM l'accesso alle queryAWSAPI Billing Conductor: ti consigliamo di creare un ruolo IAM per l'accesso programmatico per ciascuna.

Informazioni sulleAWSBilling Conductor

MentreAWSI modelli di dati Billing Conductor condividono molte somiglianze con lo standardAWSModello dei dati di fatturazione, ci sono alcune differenze.

IlAWSBilling Conductor non include:

- Crediti (riscattati a livello di pagatore o account collegato)
- Imposte
- AWS Supportaccuse

Inoltre,AWSBilling Conductor condivide le istanze riservate e Savings Plans con gli account inseriti nello stesso gruppo di fatturazione, indipendentemente dalle preferenze di condivisione nel dominio di fatturazione standard.

Informazioni sulleAWSBilling Conductor

llAWSIl calcolo di Billing Conductor è flessibile in base alle modifiche apportate in un determinato mese, pur mantenendo l'integrità storica dei dati di fatturazione del periodo precedente. È meglio descriverlo con un esempio.

In questo esempio, abbiamo due gruppi di fatturazione`AeB`. Gruppo di fatturazione`A`inizia il periodo di fatturazione con gli account da 1 a 3 del gruppo. A metà mese, il conto pagatore si sposta`Account 3`a`Billing Group B`. A quel punto, il ricalcolo dei costi per i gruppi di fatturazione`AeB`sono necessari per modellare con precisione l'ultima modifica. Quando`Account 3`viene spostato,`Billing Group A`l'utilizzo è modellato come se`Account 3`non faceva parte del gruppo di fatturazione durante il periodo di fatturazione corrente. Inoltre,`Billing Group B`l'utilizzo è modellato come se`Account 3`faceva parte di`Billing Group B`dall'inizio del periodo di fatturazione. Questo approccio elimina la necessità di calcolare tariffe complesse e modelli di chargeback quando gli account si spostano tra i gruppi durante il periodo di fatturazione.

Billing di fatturazione	giorni: 1 - 15 - 15	giorni: 16 - 30	Fine del mese
Account 1	$100	$100	200$
Account 2	$100	$100	200$
Account 3	$100	N/D	N/D
Totale	$300	200$	400$

Billing di fatturazione	giorni: 1 - 15 - 15	giorni: 16 - 30	Fine del mese
Account 4	$100	$100	200$
Account 5	$100	$100	200$
Account 6	$100	$100	200$
Account 3	$100	$100	200$
Totale	400$	400$	$800

Informazioni sulleAWSBilling Conductor

AWSi dati di fatturazione vengono aggiornati almeno una volta al giorno.AWS Billing Conductor utilizza questi dati per calcolare i dati di fatturazione pro forma. Gli articoli personalizzati generati per essere applicati al mese corrente vengono visualizzati entro 24 ore. Gli articoli personalizzati generati per essere applicati al periodo di fatturazione precedente potrebbero impiegare fino a 48 ore per essere visualizzati in un gruppo di fatturazioneAWSReport su costi e utilizzo o nella pagina delle fatture per un determinato gruppo di fatturazione.

Capire le differenze traAWSBilling ConductorAWSCUR e StandardAWSCURA

Ci sono poche differenze tra acquistate e acquistateAWSCUR creato utilizzandoAWSBilling Conductor.

- Lo StandardAWSCUR calcola il costo e l'utilizzo per ogni account della famiglia di fatturazione consolidata. Un pro formaAWSII CUR per gruppo di fatturazione include solo gli account del gruppo di fatturazione al momento del calcolo.
- Lo StandardAWSCUR compila la colonna della fattura una volta e la fattura viene generata daAWS. Un pro formaAWSCUR non compila la colonna della fattura. Attualmente, nessuna fattura viene generata o emessa daAWSbasato su dati di fatturazione pro forma.

Analisi dei margini per gruppo di fatturazione

Puoi utilizzare il report sui margini del gruppo di fatturazione inAWSBilling Conductor per analizzare i margini sia in forma aggregata che con gruppi di fatturazione specifici. Tutti i gruppi di fatturazione sono inclusi per impostazione predefinita.

Utilizza i passaggi seguenti per visualizzare i margini per un singolo gruppo di fatturazione o una serie di gruppi di fatturazione.

Per visualizzare i margini del gruppo di fatturazione

1. AprireAWSBillingConductor pressohttps://console.aws.amazon.com/billingconductor/.
2. Nel riquadro di navigazione, scegliereReport del margine del gruppo di fatturazione.
3. Pertipo di report, scegliSeleziona un gruppo di fatturazione.
4. Scegli uno o più gruppi di fatturazione per nome per vedere l'importo addebitato eAWScosti per ciascuno.

L'analisi dei margini viene mostrata come grafico a barre e in una tabella.

I margini negativi sono mostrati in rosso nel grafico, con un importo negativo in dollari e una percentuale negativa.

BillingConductor

La tabella di analisi dei margini del gruppo di fatturazione è ordinata in ordine cronologico inverso per impostazione predefinita. È possibile ordinare la tabella in base a tutte le colonne, tra cui:

- Mese
- Importo addebitato
- Costi AWS
- Importo del margine
- Percentuale del

Il grafico e la tabella restituiscono i valori degli ultimi 13 mesi dei gruppi di fatturazione selezionati. Se i gruppi di fatturazione sono stati creati in momenti diversi, assumiamo l'intervallo di tempo del gruppo di fatturazione selezionato più vecchio.

Visualizzazione dei dettagli del gruppo di fatturazione

Puoi utilizzare i dettagli del tuo gruppo di fatturazione per monitorare, analizzare e modificare il gruppo di fatturazione inAWSBilling Conductor. I dettagli del gruppo di fatturazione forniscono un month-to-date analisi dei margini, cronologia delle voci personalizzate applicate e possibilità di modificare ed eliminare il gruppo di fatturazione in base alle esigenze.

Visualizzazione dei dettagli di fatturazione in base alle dimensioni dei prezzi personalizzate

Dopo aver creato e assegnato i gruppi di fatturazione e i piani tariffari, puoi visualizzare le dimensioni di fatturazione personalizzate con la granularità del tipo di utilizzo per ogni gruppo di fatturazione gestito.

Per visualizzare i dettagli di fatturazione nel dominio proforma, utilizza la procedura riportata di seguito.

Per visualizzare i dettagli di fatturazione pro forma

1. Apri la console AWS Billing all'indirizzo https://console.aws.amazon.com/billing/.
2. Nel riquadro di navigazione selezionare Bills (Fatture).
3. SceglilImpostazioninell'angolo in alto a destra didettagli di fatturazione.
4. AbilitazioneVisualizzazione dati pro formato.
5. PerGruppo di fatturazione, scegli la fatturazione da analizzare.

È possibile analizzare l'utilizzo del gruppo di fatturazione per servizio eAWSRegione in cui visualizzare il costo di tale utilizzo, in linea con le tariffe definite inAWSBilling Conductor.

Puoi trovare gli articoli della linea personalizzata sotto il servizioAWSBilling ConductorsulDati di fatturazionepagina.

Configurazione dei report di costi e utilizzo per gruppo di fatturazione

Puoi creare pro formaAWSReport di utilizzo e dei costi (AWSCUR) per ogni gruppo di fatturazione che crei. La pro formaAWSCUR ha lo stesso formato di file, la stessa granularità e le stesse colonne dello standardAWSCUR e contiene il set più completo di dati di costo e utilizzo disponibili per un determinato periodo di tempo.

Puoi pubblicare la tua proformaAWSCUR per un bucket Amazon Simple Simple Storage Service (Amazon S3) di tua proprietà.

AWSaggiorna il report nel bucket una volta al giorno in formato CSV o Apache Parquet. È possibile visualizzare i report utilizzando software per fogli di calcolo come Microsoft Excel e Apache. OpenOffice Calc. Puoi anche accedervi da un'applicazione utilizzando le API Amazon S3 o Amazon Athena. Per ulteriori informazioni sullo standardAWSCUR, consulta laAWSReport di utilizzo e dei costi.

Attieniti alla seguente procedura per generare un pro formaAWSCUR per un gruppo di fatturazione.

Per creare report pro forma su costi e utilizzo per un gruppo di fatturazione

1. Apri la console AWS Billing all'indirizzo https://console.aws.amazon.com/billing/.
2. Nel riquadro di navigazione, scegliereRapporti su costi e utilizzo.
3. In alto a destra deltabella dei report, scegliImpostazioni.
4. Abilita laProformavisualizzazione dati.
5. Scegli Enable (Abilita).
6. Selezionare Create report (Crea report).
7. In Report name (Nome report), digitare un nome per il report.
8. PerVisualizzazione dati, sceglipro forma.
9. PerGruppo di fatturazione, scegliere un gruppo di fatturazione.
10. In Additional report details (Ulteriori dettagli del report), selezionare Include resource IDs (Includi ID risorse) per includere gli ID di ogni singola risorsa nel report.
11. PerImpostazioni di aggiornamento dei dati, seleziona se desideri ilAWSReport di costi e utilizzo da aggiornare seAWSapplica all'account rimborsi, crediti o costi di supporto dopo aver completato la fattura. Quando un report viene aggiornato, viene caricato un nuovo report su Amazon S3.
12. Seleziona Successivo.
13. Per S3 bucket (Bucket S3), scegliere Configure (Configura).
14. Nella finestra di dialogo Configure S3 Bucket (Configura bucket S3), procedere in uno dei seguenti modi:
    - Scegliere un bucket esistente dall'elenco a discesa, quindi sceglieSuccessivo.
    - Immetti il nome di un bucket eAWSRegione in cui creare un nuovo bucket e sceglieSuccessivo.
15. SelectHo confermato che la policy è correttae scegliSalva.
16. In Report path prefix (Prefisso percorso report), digitare il prefisso del percorso del report che si intende anteporre al nome del report.

    Questo passaggio è facoltativo per Amazon Redshift o Amazon QuickSight, ma obbligatorio per Amazon Athena.

Se non si specifica un prefisso, il prefisso predefinito è il nome specificato per il report nella fase 4 e l'intervallo date per il report, nel seguente formato:

```
/report-name/date-range/
```

17. In Time granularity (Granularità temporale), scegliere una delle seguenti opzioni:
    - Selezionare Hourly (Ogni ora) per aggregare le voci del report per ora.
    - Selezionare Daily (Ogni giorno) per aggregare le voci del report per giorno.
18. In Report versioning (Funzione Versioni multiple del report) scegliere se si vuole che ogni versione del report sovrascriva la versione precedente o venga inviata insieme alle versioni precedenti.
19. PerAbilita l'integrazione dei dati dei report per, scegli se caricare i report di costi e utilizzo su Amazon Athena, Amazon Redshift o Amazon QuickSight. Il report viene compresso nei formati seguenti:
    - Athena: Compressione del parquet
    - Amazon Redshift o Amazon QuickSight: compressione .gz
20. Seleziona Successivo.
21. Dopo aver esaminato le impostazioni per il report, scegliereRivedere e completare.

Utilizzo diAWSAPI Billing Conductor

L'API è facilmente disponibile in Java, Python, .NET e Go. Nuove funzionalità rilasciate nelAWSBilling Conductor sarà disponibile anche come API.

Per ulteriori informazioni sulle pagine delAWSAPI Billing Conductor, consulta laAWSRiferimento all'API Billing Conductor.

Sicurezza inAWSBilling Conductor

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, è possibile 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 AWS i servizi 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 aAWSBilling Conductor, consultorServizi AWS coperti dal programma di conformità.
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che utilizzi. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda, le leggi e le normative applicabili.

Questa documentazione consente di comprendere come applicare il modello di responsabilità condivisa quando si usaAWSBilling Conductor. Negli argomenti seguenti viene illustrato come configurareAWSBilling Conductor per soddisfare gli obiettivi di sicurezza e conformità. Vengono inoltre fornite informazioni su come utilizzare altri servizi AWS che consentono di monitorare e proteggere iAWSBilling Conductor.

Argomenti

Protezione dei dati inAWSBilling Conductor

IlAWS modello di responsabilità condivisasi applica alla protezione dei dati inAWSBilling Conductor. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che esegue tutto l'AWS Cloud. L'utente è responsabile di mantenere il controllo sui contenuti ospitati su questa infrastruttura. Questi contenuti comprendono la configurazione della protezione e le attività di gestione per i servizi 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 negli AWS.

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWS e di configurare singoli account utente con AWS Identity and Access Management (IAM). In questo modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere il suo lavoro. 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 consigliabile TLS 1.2 o versioni successive.
- Configura la registrazione delle API e delle attività degli utenti con AWS CloudTrail.

- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza di default all'interno dei servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, ad esempio Amazon Macie, che aiutano a individuare e proteggere i dati personali archiviati in Amazon S3.
- Se si richiedono moduli crittografici convalidati FIPS 140-2 quando si accede ad AWS tramite una CLI o un'API, utilizzare un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti suggeriamo vivamente di non inserire mai informazioni identificative sensibili, ad esempio i numeri di account dei clienti, in campi a formato libero, ad esempio un campo Name (Nome). Ciò include quando lavori conAWSBillingAWSServizi che utilizzano la console, API,AWS CLI, oppureAWSSDK. I dati inseriti nei tag o nei campi in formato libero utilizzati per i nomi possono essere utilizzati per i registri di fatturazione o 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.

Gestione delle identità e degli accessi perAWSBilling Conductor

AWS Identity and Access Management (IAM) è un Servizio AWS che consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi può essereautenticate(registrato) eautorizzati(disponi dei permessi) da usareAWSBilling Conductor. IAM è un Servizio AWS il cui utilizzo non comporta costi aggiuntivi.

Argomenti

Destinatari

Come utilizziAWS Identity and Access Management(IAM) differisce in base alle operazioni eseguite inAWSBilling Conductor.

Utente del servizio— Se utilizzi il toolAWSServizio Billing Conductor per eseguire il tuo lavoro, quindi l'amministratore fornisce le credenziali e le autorizzazioni necessarie. Man mano che ne usi di piùAWSFunzionalità di Billing Conductor per svolgere il tuo lavoro, potrebbero essere necessarie ulteriori autorizzazioni. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità diAWSBilling Conductor, consultorRisoluzione dei problemiAWSBilling (p. 36).

Amministratore del servizio— Se sei responsabile diAWSRisorse per il responsabile della Fatturazione presso la tua azienda, probabilmente disponi dell'accesso completo aAWSBilling Conductor. Il tuo compito è determinare qualeAWSFunzionalità e risorse di Billing Conductor a cui gli utenti del servizio devono accedere. 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 conAWSBilling Conductor, consultorComeAWSBilling Conductor funziona con IAM (p. 25).

Amministratore IAM— Se sei un amministratore IAM, potresti essere interessato a ottenere informazioni su come scrivere policy per gestire l'accesso aAWSBilling Conductor. Per visualizzare un esempioAWSpolicy basate su identità di Billing Conductor che puoi utilizzare in IAM, consultaAWSEsempi policy basate su identità di Billing Conductor (p. 30).

Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWS utilizzando le credenziali di identità. Per ulteriori informazioni sull'accesso tramite la AWS Management Console, consulta Accesso alla AWS Management Console come utente IAM o utente root nella Guida per l'utente di IAM.

È necessario essere autenticato (connesso a AWS) come utente root Account AWS, come utente IAM o assumere un ruolo IAM. È anche possibile utilizzare l'autenticazione Single Sign-On (SSO) della propria azienda oppure collegarsi utilizzando Google o Facebook. In questi casi, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando si accede ad AWS utilizzando le credenziali di un'altra azienda, si assume indirettamente un ruolo.

Per accedere direttamente alla AWS Management Console, utilizza la password con l'indirizzo e-mail dell'utente root o il nome utente IAM. È possibile effettuare l'accesso a AWS a livello di programmazione utilizzando le chiavi di accesso dell'utente root o dell'utente IAM. AWS fornisce SDK e gli strumenti a riga di comando per firmare in maniera crittografica la richiesta utilizzando le tue credenziali. Se non utilizzi gli strumenti AWS, è necessario firmare la richiesta personalmente. A questo scopo, utilizza Signature Version 4, un protocollo per l'autenticazione di richieste API in entrata. Per ulteriori informazioni sull'autenticazione delle richieste, consulta Processo di firma con Signature Version 4 nei Riferimenti generali di AWS.

Indipendentemente dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. AWS consiglia ad esempio di utilizzare la multi-factor authentication (MFA) per aumentare la sicurezza dell'account. Per ulteriori informazioni, consultare 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. È vivamente consigliato 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 Attività che richiedono credenziali dell'utente root in Riferimenti generali AWS.

Utenti e gruppi IAM

Un utente IAM è una identità all'interno del tuo Account AWS che dispone di autorizzazioni specifiche per un singolo utente o applicazione. Un utente IAM può disporre di credenziali a lungo termine, ad esempio un nome utente e una password oppure un set di chiavi di accesso. Per informazioni su come generare le chiavi di accesso, consulta Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente di IAM. Quando generi le chiavi di accesso per un utente IAM, assicurati di visualizzare e salvare la coppia di chiavi in modo sicuro. Non sarà possibile recuperare la chiave di accesso segreta in futuro. Al contrario, sarà necessario generare una nuova coppia di chiavi di accesso.

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 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'operazione 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:

- Autorizzazioni utente IAM temporanee: un utente IAM può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso di utenti federati: anziché creare un utente IAM, puoi utilizzare le identità utente esistenti da AWS Directory Service, la directory utente aziendale, un provider di identità Web o un archivio di identità di IAM Identity Center. Queste identità sono conosciute come identità federate. Per assegnare le autorizzazioni alle identità federate, puoi creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità esterna viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Se utilizzi IAM Identity Center, configuri 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 sulla federazione delle identità, consulta Creazione di un ruolo per un provider di identità di terze parti nella Guida per l'utente di IAM. Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center (successor to AWS Single Sign-On).
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (entità di sicurezza attendibile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso tra 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 tra servizi: alcuni Servizi AWS utilizzano funzionalità che eseguono 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 operazioni in AWS, si viene considerati un principale. Le policy concedono autorizzazioni a un'entità. 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 verificare se un'operazione richiede ulteriori operazioni dipendenti in una policy, consultaOperazioni, risorse e chiavi di condizione perAWSBilling ConductornelService 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 da 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 conto dell'utente. I ruoli collegati ai servizi sono visualizzati nell'account IAM e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non può 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 CLI o 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 tramite 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 nella policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene archiviata in AWS sotto 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 AWS JSON per specificare l'accesso ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

Ogni entità IAM (utente o ruolo) inizialmente non dispone di autorizzazioni. Di default, gli utenti non possono eseguire alcuna operazione, neppure modificare la propria password. Per autorizzare un utente a eseguire operazioni, un amministratore deve allegare una policy di autorizzazioni a tale utente. In alternativa, l'amministratore può aggiungere l'utente a un gruppo che dispone delle autorizzazioni desiderate. Quando un amministratore fornisce le autorizzazioni a un gruppo, le autorizzazioni vengono concesse a tutti gli utenti in tale gruppo.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, indipendentemente 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 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 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 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 trust 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 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 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 della lista di controllo accessi 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 suoi 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 Organizations è un servizio per il raggruppamento e la gestione centralizzata degli Account AWS multipli di proprietà dell'azienda. Se si abilitano tutte le caratteristiche in un'organizzazione, è possibile applicare le policy di controllo dei servizi (SCP) a uno o tutti i propri account. Una SCP limita le autorizzazioni per le entità negli account membri, compreso ogni utente root Account AWS. Per ulteriori informazioni su Organizations e le policy SCP, consulta Utilizzo delle SCP nella Guida per l'utente di AWS Organizations.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono passate 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 sull'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.

ComeAWSBilling Conductor funziona con IAM

Prima di utilizzare IAM per gestire l'accesso aAWSBilling Conductor, dovresti comprendere quali funzionalità IAM sono disponibili per l'uso conAWSBilling Conductor. Per avere una visione d'insieme di comeAWSBillingAWSi servizi funzionano con IAM, consultaAWSServizi supportati da IAMnelIAM User Guide.

Argomenti

AWSBilling

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o rifiutate, nonché le condizioni in base alle quali le operazioni sono consentite o rifiutate. AWS Billing Conductor supporta specifiche operazioni, risorse e chiavi di condizione. 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 di IAM.

Operazioni

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 un criterio. Le operazioni della policy hanno spesso lo stesso nome dell'operazione API AWS. 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 chiamate operazioni dipendenti.

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

Operazioni di policy inAWSBilling Conductor utilizza il seguente prefisso prima dell'operazione: `AWS Billing Conductor:`. Ad esempio, per concedere a qualcuno l'autorizzazione per eseguire un'istanza Amazon EC2 con Amazon EC2 con Amazon EC2`RunInstances`Funzionamento dell'API, includi il`ec2:RunInstances`azione nella loro politica. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. AWS Billing Conductor definisce un proprio set di operazioni che descrivono le attività che puoi eseguire con quel servizio.

Per specificare più operazioni in una sola istruzione, separa ciascuna di esse con una virgola come mostrato di seguito:

```
"Action": [
      "ec2:action1",
      "ec2:action2"
```

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

```
"Action": "ec2:Describe*"
```

Per visualizzare l'elenco delle.AWSAzioni di Billing Conductor, vediAzioni definite daAWSBilling ConductornellIAM User Guide.

Risorse

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 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 Amazon Resource Name (ARN). È possibile eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, noto 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": "*"
```

La risorsa istanza Amazon EC2 dispone del seguente ARN:

```
arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}
```

Per ulteriori informazioni sul formato degli ARN, consulta Amazon Resource Name (ARN) e spazi dei nomi del servizio AWS.

Ad esempio, per specificare l'istanza `i-1234567890abcdef0` nell'istruzione, utilizza il seguente ARN:

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

Per specificare tutti le istanze che appartengono ad un account specifico, utilizza il carattere jolly (*):

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

MedioAWSLe operazioni di Billing Conductor, ad esempio quelle per la creazione di risorse, non possono essere eseguite su una risorsa specifica. In questi casi, è necessario utilizzare il carattere jolly (*).

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

Molte operazioni API di Amazon EC2 coinvolgono più risorse. Ad esempio, `AttachVolume` collega un volume Amazon EBS a un'istanza, pertanto un utente IAM dovrà disporre delle autorizzazioni per utilizzare il volume e l'istanza. Per specificare più risorse in una singola istruzione, separa gli ARN con le virgole.

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

Per visualizzare l'elenco delle.AWSTipi di risorse di Billing Conductor e relativi ARN, consultaRisorse definite daAWSBilling ConductornelIAM User Guide. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consultaAzioni definite daAWSBilling Conductor.

Chiavi di condizione

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

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

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

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi 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 per il servizio. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente di IAM.

AWSBilling Conductor definisce il proprio set di chiavi di condizione e supporta anche l'uso di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione globali diAWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente di IAM.

Tutte le azioni Amazon EC2 supportano le chiavi di condizione `aws:RequestedRegion` e `ec2:Region`. Per ulteriori informazioni, consulta la paginaEsempio: Limitazione dell'accesso a una regione specifica.

Per visualizzare l'elenco delle.AWSBilling Conductor, consultaChiavi di condizione perAWSBilling ConductornelIAM User Guide. Per informazioni sulle operazioni e risorse con cui è possibile utilizzare una chiave di condizione, consultaAzioni definite daAWSBilling Conductor.

Examples (Esempi)

Per visualizzare esempi diAWSpolicy basate su identità di Billing Conductor, consultaAWSEsempi policy basate su identità di Billing Conductor (p. 30).

AWSBilling

Le policy basate su risorse sono documenti di policy JSON che specificano le operazioni che possono essere eseguite da un'entità specificata sulAWSRisorsa Billing Conductor e a quali condizioni. Amazon S3 supporta policy basate su risorse per Amazon S3*secchi*. Le policy basate su risorse consentono di concedere l'autorizzazione all'utilizzo ad altri account per ogni risorsa. Puoi anche utilizzare una policy basata su risorse per consentire aAWSservizio per accedere al tuo Amazon S3*secchi*.

Per consentire l'accesso a più account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata su risorse. L'aggiunta di un'entità principale a più account a una policy basata su risorse rappresenta solo una parte della relazione di trust. Quando l'entità principale e la risorsa si trovano in account AWS diversi, devi anche concedere all'entità principale l'autorizzazione per accedere alla risorsa. Concedi l'autorizzazione collegando una policy basata sull'identità all'entità. Tuttavia, se una policy basata su risorse concede l'accesso a un'entità principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente IAM.

Il servizio Amazon S3 supporta solo un tipo di policy basata su risorse detta a*secchio*informativa, che è collegato a*secchio*. Questa policy definisce quali entità principali (account, utenti, ruoli e utenti federati) possono eseguire operazioni su*AWSBilling Conductor*.

Examples (Esempi)

Per visualizzare esempi diAWSpolicy basate su risorse di Billing Conductor, consultaAWSEsempi policy basate su risorse di Billing Conductor (p. 35),

Liste di controllo accessi (ACL)

Le liste di controllo degli accessi sono elenchi di assegnatari da associare alle risorse. Essi concedono le autorizzazioni di accesso alla risorsa a cui sono associati. Puoi collegare gli ACL a un Amazon S3*secchio*risorsa.

Con le liste di controllo accessi (ACL) di Amazon S3, è possibile gestire l'accesso a*secchio*risorse. A ogni *bucket* è associata una ACL come risorsa secondaria. Definisce qualeAWSagli account, agli utenti o ai gruppi di utenti IAM o ai ruoli IAM viene concesso l'accesso e il tipo di accesso. Quando si riceve una richiesta relativa a una risorsa, AWS controlla l'ACL corrispondente per verificare che il richiedente possieda le autorizzazioni d'accesso necessarie.

Quando crei una.*secchio*risorsa, Amazon S3 crea un'ACL predefinita che concedere al proprietario della risorsa il controllo completo su di essa. Nel seguente esempio di ACL del *bucket*, Mario Rossi viene elencato come proprietario del *bucket* e gli viene concesso un controllo totale sul *bucket*. Una ACL può avere fino a 100 di questi elementi.

```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://AWS Billing Conductor.amazonaws.com/doc/2006-03-01/">
  <Owner>
    <ID>c1daexampleaaf850ea79cf0430f33d72579fd1611c97f7ded193374c0b163b6</ID>
    <DisplayName>john-doe</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xsi:type="Canonical User">
        <ID>c1daexampleaaf850ea79cf0430f33d72579fd1611c97f7ded193374c0b163b6</ID>
        <DisplayName>john-doe</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>
  </AccessControlList>
</AccessControlPolicy>
```

Il campo ID nell'ACL è l'ID utente canonico dell'account AWS. Per informazioni su come visualizzare questo ID in un account di tua proprietà, consulta l'argomento Trovare un ID utente canonico dell'account AWS.

Autorizzazione basata suAWSBilling

Puoi allegare tag aAWSRisorse per Billing Conductor o passali in una richiesta aAWSBilling Conductor. Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `AWS Billing Conductor:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* o `aws:TagKeys`.

AWSBilling

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

Utilizzo di credenziali temporanee conAWSBilling Conductor

È possibile utilizzare credenziali temporanee per effettuare l'accesso con la federazione, assumere un ruolo IAM o un ruolo multi-account. Per ottenere le credenziali di sicurezza temporanee, eseguiAWS STSOperazioni API comeAssumeRoleoGetFederationToken.

AWSBilling Conductor supporta l'uso 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 IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non può modificarle.

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 IAM può modificare le autorizzazioni per questo ruolo. Tuttavia, questo potrebbe pregiudicare la funzionalità del servizio.

AWSBilling Conductor supporta i ruoli del servizio.

Scelta di un ruolo IAM inAWSBilling Conductor

Quando crei una risorsa inAWSBilling Conductor, devi scegliere un ruolo da consentireAWSBilling Conductor per accedere ad Amazon EC2 per tuo conto. Se hai già creato un ruolo di servizio o un ruolo collegato ai servizi in precedenza,AWSBilling Conductor ti fornisce un elenco di ruoli tra cui scegliere. È importante scegliere un ruolo che consenta l'accesso per avviare e arrestare istanze Amazon EC2.

AWSEsempi policy basate su identità di Billing Conductor

Per impostazione predefinita, gli utenti e i ruoli IAM non dispongono dell'autorizzazione per creare o modificareAWSBilling Conductor. Inoltre, non sono in grado di eseguire attività utilizzando la AWS Management Console, AWS CLI o un'API AWS. Un amministratore IAM deve creare policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate 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 di IAM.

Argomenti

Best practice delle policy

Le policy basate su identità determinano se qualcuno può creare, accedere o eliminareAWSRisorse di Billing Conductor nel tuo account. Queste operazioni possono comportare costi aggiuntivi per il proprio Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e suggerimenti:

- Nozioni di base sulle policy gestite da AWS e passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite da AWS che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWS specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni di processo nella Guida per l'utente di IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione politica 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 paginaElementi delle policy JSON IAM: ConditionnelIAM User Guide.

- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer fornisce oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo account, attiva MFA per una maggiore sicurezza. Per richiedere l'AMF quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

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

AWSEsempi policy basate su identità di Billing Conductor

Questo argomento contiene esempi di policy che puoi allegare al tuo utente o gruppo IAM per controllare l'accesso alle informazioni e agli strumenti del tuo account.

Argomenti

Concessione dell'accesso completo allaAWSBilling

Per accedere alAWSConsole Billing Conductor, è necessario disporre di un set di autorizzazioni minimo. Queste autorizzazioni devono consentire di elencare e visualizzare i dettagli relativi aiAWSRisorse Billing Conductor nel tuoAWSaccount. 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 ancora utilizzare ilAWSConsole Billing Conductor, allega anche quanto segueAWSPolicy gestite dalle entità. Per ulteriori informazioni, consultare Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM:

Oltre al`billingconductor:*`autorizzazioni,`pricing:DescribeServices`è necessario per la creazione di regole di determinazione dei prezzi e`organizations:ListAccounts`è necessario per elencare gli account collegati al conto pagatore.

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

```
        {
            "Effect": "Allow",
            "Action": "organizations:ListAccounts",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "pricing:DescribeServices",
            "Resource": "*"
        }
    ]
}
```

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

Concessione dell'accesso completo allaAWSBilling

In questo esempio, concedi a un utente IAM l'accesso completo solo alAWSBilling Conductor.

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

Concessione dell'accesso in sola lettura allaAWSBilling

In questo esempio, si concede a un utente IAM l'accesso in sola lettura alAWSBilling Conductor.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "billingconductor:List*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "organizations:ListAccounts",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "pricing:DescribeServices",
            "Resource": "*"
        }
    ]
}
```

GrantAWSAccesso a Billing Conductor tramite la console di fatturazione

In questo esempio, gli utenti IAM possono attivare e visualizzare i dati di fatturazione pro forma tramite la pagina delle fatture nella loro console di fatturazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "billing:ListBillingViews",
                "aws-portal:ViewBilling"
            ]
            "Resource": "*"
        }
    ]
}
```

GrantAWSBilling Conductor tramiteAWSReport di utilizzo

In questo esempio, gli utenti IAM possono attivare e visualizzare i dati di fatturazione proforma tramite la pagina Report di costi e utilizzo nella loro console di fatturazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "billing:ListBillingViews",
                "aws-portal:ViewBilling",
                "cur:DescribeReportDefinitions"
            ],
            "Resource": "*"
        }
    ]
}
```

GrantAWSAccesso a Billing Conductor alla funzionalità unità organizzativa (OU) di importazione

In questo esempio, gli utenti IAM dispongono dell'accesso in sola lettura alle specificheAWS OrganizationsLe API necessarie per importare gli account delle unità organizzative durante la creazione di un gruppo di fatturazione. La funzione di importazione dell'unità organizzativa è disponibile nelAWSBilling Conductor.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListRoots",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

AWSPolicy gestite da perAWSBilling Conductor

Per aggiungere le autorizzazioni a utenti, gruppi e ruoli, è più semplice utilizzare policy gestite da AWS piuttosto che scrivere autonomamente le policy. La creazione di policy gestite dai clienti IAM che forniscono al tuo team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, utilizza le nostre policy gestite da AWS. Queste policy coprono i casi d'uso comuni e sono disponibili nel tuo Account AWS. Per ulteriori informazioni sulle policy gestite da AWS, consulta Policy gestite da AWS nella Guida per l'utente di IAM.

I servizi AWS mantengono e aggiornano le policy gestite da AWS. Non è possibile modificare le autorizzazioni nelle policy gestite da AWS. I servizi occasionalmente aggiungono altre autorizzazioni a una policy gestita da AWS per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una policy gestita da AWS quando viene avviata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy gestita da AWS, pertanto gli aggiornamenti delle policy non interrompono le autorizzazioni esistenti.

Inoltre, AWS supporta policy gestite per le funzioni di processi che coprono più servizi. Ad esempio, laReadOnlyAccess AWSpolicy gestita fornisce accesso in sola lettura a tuttiAWSservizi e risorse. Quando un servizio avvia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei processi, consulta la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente di IAM.

AWSPolicy gestita: AWSBillingConductorFullAccess

Il AWSBillingConductorFullAccess la policy gestita garantisce l'accesso completo aAWSConsole e API Billing Conductor. Gli utenti possono elencare, creare ed eliminareAWSBilling Conductor.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "billingconductor:*",
               "organizations:ListAccounts",
               "pricing:DescribeServices",
             ]
            "Resource": "*"
        }
    ]
}
```

AWSPolicy gestita: AWSBillingConductorReadOnlyAccess

Il AWSBillingConductorReadOnlyAccess la policy gestite concede l'accesso in sola lettura allaAWSConsole e API Billing Conductor. Gli utenti possono visualizzare ed elencare tuttoAWSBilling Conductor. Gli utenti non possono creare o eliminare risorse.

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

```
            "Action": [
               "billingconductor:List*",
               "organizations:ListAccounts",
               "pricing:DescribeServices"
             ]
            "Resource": "*"
        }
    ]
}
```

AWSBilling Conductor diAWSpolicy gestite

Visualizza i dettagli sugli aggiornamenti diAWSPolicy gestite da perAWSBilling Conductor da quando questo servizio ha iniziato a tenere traccia delle modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivere il feed RSS alla paginaAWSPagina della cronologia del documento Billing Conductor.

Modifica	Descrizione	Data
AWSBillingConductorFullAccess	Policy creata	29 marzo 2022
AWSBillingConductorReadOnlyAccess	Policy creata	29 marzo 2022
AWSPubblicato il registro delle modifiche di Billing Conductor	AWSBilling Conductor ha iniziato a monitorare le modifiche perAWSPolicy gestita.	29 marzo 2022

AWSEsempi policy basate su risorse di Billing Conductor

Argomenti

- Limitazione dell'accesso ai bucket Amazon S3 a indirizzi IP specifici (p. 35)

Limitazione dell'accesso ai bucket Amazon S3 a indirizzi IP specifici

L'esempio seguente concede autorizzazioni a qualsiasi utente per eseguire operazioni di Amazon S3 sugli oggetti nel bucket specificato. La richiesta deve, tuttavia, avere origine dall'intervallo di indirizzi IP specificati nella condizione.

La condizione in questa istruzione identifica l'intervallo 54.240.143.* di indirizzi IP Internet Protocol versione 4 (IPv4) consentiti, con un'eccezione: 54.240.143.188.

Il blocco `Condition` utilizza le condizioni `IpAddress` e `NotIpAddress` e la chiave di condizione `aws:SourceIp`, che è una chiave di condizione AWS. Per ulteriori informazioni su queste chiavi di condizione, consultaSpecifica delle condizioni in una policy. I valori IPv4 `aws:sourceIp` utilizzano la notazione CIDR standard. Per ulteriori informazioni, consulta Operatori di condizione con indirizzo IP nella Guida per l'utente di IAM.

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

```
  "Id": "S3PolicyId1",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::examplebucket/*",
      "Condition": {
         "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
         "NotIpAddress": {"aws:SourceIp": "54.240.143.188/32"}
      }
    }
  ]
}
```

Risoluzione dei problemiAWSBilling

Utilizza le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo diAWSBilling Conductor e IAM.

Argomenti

Non sono autorizzato a eseguire un'operazione inAWSBilling Conductor

Se la AWS Management Console indica che non sei autorizzato a eseguire un'operazione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è la persona da cui si sono ricevuti il nome utente e la password.

L'errore di esempio seguente si verifica quando`mateojackson`L'utente IAM cerca di utilizzare la console per visualizzare i dettagli relativi a*`AWSBilling Conductor`*ma non ha`AWS Billing Conductor:`*`GetWidget`*autorizzazioni.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: AWS Billing
 Conductor:GetWidget on resource: my-example-AWS Billing Conductor
```

In questo caso, Mateo richiede al suo amministratore di aggiornare le sue policy per poter accedere alla risorsa *`my-example-AWS Billing Conductor`* utilizzando l'operazione `AWS Billing Conductor:`*`GetWidget`*.

Non sono autorizzato a eseguire iam:PassRole

Se ricevi un errore che indica che non hai l'autorizzazione a eseguire il`iam:PassRole`azione, le policy devono essere aggiornate per poter passare un ruolo aAWSBilling Conductor.

Alcuni Servizi AWS consentono di passare 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 passare il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato`marymajor`cerca di utilizzare la console per eseguire un'operazione inAWSBilling Conductor. Tuttavia, l'operazione 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 colui che ti ha fornito le credenziali di accesso.

Desidero visualizzare le mie chiavi di accesso

Dopo aver creato le chiavi di accesso utente IAM, è possibile visualizzare il proprio ID chiave di accesso in qualsiasi momento. Tuttavia, non è possibile visualizzare nuovamente la chiave di accesso segreta. Se perdi la chiave segreta, dovrai creare una nuova coppia di chiavi di accesso.

Le chiavi di accesso sono composte da due parti: un ID chiave di accesso (ad esempio `AKIAIOSFODNN7EXAMPLE`) e una chiave di accesso segreta (ad esempio, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Come un nome utente e una password, è necessario utilizzare sia l'ID chiave di accesso sia la chiave di accesso segreta insieme per autenticare le richieste dell'utente. Gestisci le tue chiavi di accesso in modo sicuro mentre crei il nome utente e la password.

> **Important**
>
> Non fornire le chiavi di accesso a terze parti, neppure per aiutare a trovare l'ID utente canonico. Se lo facessi, daresti a qualcuno accesso permanente al tuo account.

Quando crei una coppia di chiavi di accesso, ti viene chiesto di salvare l'ID chiave di accesso e la chiave di accesso segreta in una posizione sicura. La chiave di accesso segreta è disponibile solo al momento della creazione. Se si perde la chiave di accesso segreta, è necessario aggiungere nuove chiavi di accesso all'utente IAM. È possibile avere massimo due chiavi di accesso. Se se ne hanno già due, è necessario eliminare una coppia di chiavi prima di crearne una nuova. Per visualizzare le istruzioni, consulta Gestione delle chiavi di accesso nella Guida per l'utente di IAM.

Sono un amministratore e desidero consentire ad altri utenti di accedere aAWSBilling Conductor

Per consentire ad altri di accedereAWSBilling Conductor, è necessario creare un'entità IAM (utente o ruolo) per la persona o l'applicazione che richiede l'accesso. Tale utente o applicazione utilizzerà le credenziali dell'entità per accedere ad AWS. Dovrai quindi collegare all'entità una policy che conceda le autorizzazioni corrette inAWSBilling Conductor.

Per iniziare immediatamente, consulta Creazione dei primi utenti e gruppi delegati IAM nella Guida per l'utente di IAM.

Voglio consentire a persone al di fuori del mioAWSaccount per accedere al mioAWSBilling

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 seAWSBilling Conductor supporta queste funzionalità, consultaComeAWSBilling Conductor funziona con IAM (p. 25).
- Per informazioni su come garantire l'accesso alle risorse negli Account AWS che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS in tuo possesso nella Guida per l'utente di 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 di 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, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Registrazione e monitoraggio inAWSBilling Conductor

Il monitoraggio è importante per mantenere l'affidabilità, la disponibilità e le prestazioni dell'account AWS. Ci sono diversi strumenti disponibili per monitorareAWSBilling Conductor.

Report di utilizzo e dei costi AWS

I report di utilizzo e dei costi AWS consentono di monitorare l'utilizzo di AWS e offrono una stima delle spese associate all'account. Il report contiene voci per ciascuna combinazione univoca di prodotti AWS, tipo di utilizzo e operazione utilizzata dal tuo account AWS. Puoi personalizzare i report di utilizzo e dei costi AWS per aggregare le informazioni in base all'ora oppure al giorno.

Per ulteriori informazioni sulla creazione di un report di utilizzo e dei costi AWS, consulta la guida ai report di utilizzo e dei costi.

Convalida della conformità perAWSBilling Conductor

Revisori di terze parti valutano la sicurezza e la conformità diAWSservizi come parte di piùAWSprogrammi di conformità.AWS Billing Conductor non rientra nell'ambito di alcun programma di conformità di AWS.

Per un elenco dei servizi AWS coperti da programmi di conformità specifici, consulta Servizi AWS coperti dal programma di compliance. Per informazioni generali, consultare Programmi per la conformità di AWS.

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

La tua responsabilità di conformità durante l'utilizzoAWSBilling Conductor è determinata dalla riservatezza dei dati, dagli obiettivi dell'azienda e dalle leggi e normative applicabili.AWSfornisce le seguenti risorse per facilitare la conformità:

- Security and Compliance Quick Start Guides (Guide Quick Start Sicurezza e compliance): queste guide alla distribuzione illustrano considerazioni relative all'architettura e forniscono procedure per la distribuzione di ambienti di base incentrati sulla sicurezza e sulla conformità su AWS.
- 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 lo sviluppatore di AWS Config: il servizio AWS Config valuta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti.
- AWS Security Hub: questo servizio AWS fornisce una visione completa dello stato di sicurezza all'interno di AWS che consente di verificare la conformità con gli standard e le best practice di sicurezza del settore.

Resilienza inAWSBilling Conductor

L'infrastruttura globale di AWS è basata su regioni e zone di disponibilità AWS. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e velocità effettiva elevata. Con le Zone di disponibilità, è possibile progettare e gestire 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 disponibilità, consulta Infrastruttura globale di AWS.

Sicurezza dell'infrastruttura inAWSBilling Conductor

Come servizio gestito,AWSBilling Conductor è protetto daAWSprocedure globali di sicurezza della rete descritte nellaAmazon Web Services: Panoramica dei processi di sicurezzawhite paper.

Tu usiAWSchiamate API pubblicate di per accedereAWSBilling Conductor tramite la rete. I client devono supportare Transport Layer Security (TLS) 1.0 o versioni successive. È consigliabile TLS 1.2 o versioni successive. I client devono, inoltre, supportare le suite di cifratura con PFS (Perfect Forward Secrecy), 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.

Quote e restrizioni

Nella tabella seguente vengono descritte le quote e le restrizioni all'interno diAWSBilling Conductor.

Quote

Numero di account per gruppo di fatturazione	1.000
Numero di piani tariffari	5.000
Numero di regole tariffarie	50.000
Numero di regole tariffarie associabili a un piano tariffario	500
Numero di piani tariffari associabili a una regola di determinazione dei prezzi	1.000
Numero di voci personalizzate	50.000

Restrizioni

Le altre restrizioni nella tabella seguente non possono essere aumentate.

Numero di report sui costi e sull'utilizzo del gruppo di fatturazione per gruppo di fatturazione	10
Nome gruppo di fatturazione	• Deve contenere fino a 128 caratteri • Non può contenere `unspace` • Non può contenere caratteri speciali
Descrizione del gruppo di fatturazione	Deve contenere 1.024 caratteri
Nome del piano tariffario	• Deve contenere fino a 128 caratteri • Non può contenere `unspace` • Non può contenere caratteri speciali
Descrizione del piano tariffario	Deve contenere 1.024 caratteri
Riga personalizzata del nome	• Deve contenere fino a 128 caratteri • Non può contenere `unspace` • Non può contenere caratteri speciali

Cronologia dei documenti per la Guida per l'utente

La tabella seguente descrive la documentazione per questa versione diAWSBilling Conductor.

update-history-change	update-history-description	update-history-date
Versione iniziale (p. 41)	Versione iniziale diAWSGuida per l'utente e riferimento delle API di Billing Conductor.	16 marzo 2022

Glossario AWS

Per la terminologia di AWS più recente, consulta il Glossario AWS nei Riferimenti generali AWS.

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.