Guía del usuario

AWS Conductor de facturación

AWS Conductor de facturación: Guía del usuario

Table of Contents

¿Qué es AWS Billing Conductor?

AWS Billing Conductor es un servicio de facturación personalizado para socios de AWS Marketplace canal (socios) y organizaciones que tienen requisitos de devolución de cargos. En el caso de los socios, las devoluciones de cargo son un requisito previo para que sus clientes les paguen y se ajusten a un Cuenta de AWS límite de AWS Organizations facturación. En el caso de las organizaciones, las actividades de contracargos garantizan que las organizaciones asignen los costos de un equipo específico (por ejemplo, un conjunto de cuentas) al presupuesto interno correcto o al estado de pérdidas y ganancias (P&L) correcto.

Para llevar a cabo estas actividades, Billing Conductor permite a los clientes crear una segunda versión pro forma de sus costos para compartirla con sus clientes o propietarios de cuentas. Los costos pro forma representan el uso en las cuentas administradas por Billing Conductor (aquellas asignadas a grupos de facturación) a las tarifas de precios definidas en Billing Conductor (por ejemplo, mediante el uso de una regla de precios global para aplicar precios públicos a todos los usos).

> **Note**
>
> Los clientes observarán pequeñas diferencias de uso entre los costos facturables (que coinciden con la AWS factura) y los costos proforma (que coinciden con la configuración de Billing Conductor) a lo largo del mes. Sin embargo, los valores de uso coincidirán al final de cada mes, una vez que se emita la AWS factura.

La definición de los costos pro forma permite a los clientes modelar sus costos de manera uniforme para que coincidan con uno de los siguientes casos de uso:

1. Acuerdos con los clientes, que pueden ser un caso de uso con un socio negociado fuera de AWS
2. Prácticas de contabilidad interna, que suelen ser un caso de uso específico de la organización

Las configuraciones de Billing Conductor no afectan a las facturas AWS ni a las configuraciones de facturación existentes de los clientes (por ejemplo, el reparto de créditos o los descuentos basados en compromisos, como Reserved Instances o Savings Plans).

Los clientes pueden analizar los costos proforma desde la cuenta de administración realizando las siguientes tareas:

- Analice los márgenes (la diferencia entre los costos pro forma y los costos facturables para el mismo conjunto de cuentas) en Billing Conductor
- Consulta los costos proforma mensuales en la página de detalles de facturación
- Crea un AWS Cost and Usage Report (CUR) por grupo de facturación

Las cuentas administradas por Billing Conductor (cuentas en grupos de facturación) pueden analizar los costos proforma en AWS Cost Explorer los informes de costos y uso, el panel de facturación y la página de detalles de facturación.

Puede configurar los grupos de facturación, los planes de precios, las reglas de precios y las partidas personalizadas en la consola de Billing Conductor o mediante la API de Billing Conductor.

Para obtener más información sobre las cuotas de servicio de AWS Billing Conductor, consulteCuotas y limitaciones.

Temas

Características de AWS Billing Conductor

Puede utilizar las funciones de AWS Billing Conductor para hacer lo siguiente:

Cuentas grupales

Organice las cuentas en grupos de facturación para obtener una vista agregada de los costos pro forma. Simule los beneficios individuales para los clientes, como los descuentos entre servicios, y capa gratuita de AWS para cada grupo.

Precios personalizados

Establezca márgenes o descuentos globales o específicos y controle el acceso a la capa gratuita.

Cargos y créditos

Agrega cargos o créditos únicos o recurrentes fijos o basados en porcentajes a los grupos de facturación.

Análisis proforma

Analice los costos en función de las configuraciones de precios en la consola de facturación. Las cuentas de sus grupos de facturación pueden visualizar, pronosticar y crear informes personalizados de sus costos proforma en AWS Cost Explorer. La cuenta principal tendrá una vista multicuenta de todos los costos acumulados por las cuentas del grupo de facturación, mientras que las cuentas no principales verán sus propios costos.

Informes

Configure los informes de costos y uso para cada grupo de facturación.

Análisis de tarifas

Compare las tarifas aplicadas con las AWS tarifas reales con el informe de márgenes del grupo de facturación.

Servicios relacionados

AWS Consola de facturación

La consola AWS de facturación es el portal para todos AWS los clientes, desde estudiantes y empresas emergentes hasta grandes empresas. Puedes usar la consola para ver los recursos disponibles en tus AWS cuentas, administrar las preferencias de facturación y acceder a los dispositivos de facturación necesarios para realizar pagos AWS. La consola de AWS facturación también proporciona una explicación detallada de los gastos de tu cuenta y sirve como punto de partida para inscribirte en los productos de gestión de AWS costes.

Para más información, consulte la Guía del usuario de AWS Billing.

AWS Cost Explorer

Puede usar la interfaz Cost Explorer para visualizar, comprender y administrar AWS los costos y el uso a lo largo del tiempo. Comience rápidamente con la creación de informes personalizados que analicen los datos de costo y uso. Analice sus datos a un nivel alto (por ejemplo, los costos totales y el uso en todas las cuentas) o profundice en sus datos de costos y uso para identificar tendencias, identificar los factores que impulsan los costos y detectar anomalías.

Para obtener más información, consulte los temas siguientes:

- Realizar un análisis ad hoc de los costos pro forma en AWS Cost Explorer

- Análisis de sus costos con AWS Cost Explorer en la Guía del usuario de AWS Cost Management

AWS Informes de uso y costo

Los informes de AWS costos y uso (AWS CUR) contienen el conjunto más completo de datos de costo y uso disponible. Puedes utilizar los informes de costes y uso para publicar tus informes de AWS facturación en un bucket de Amazon Simple Storage Service (Amazon S3) de tu propiedad. Puede recibir informes con los costos desglosados por hora o mes, por producto o recurso de producto, o por etiquetas que defina usted mismo.

AWS actualiza el informe de tu bucket una vez al día en valores separados por comas (CSV) o en formato Apache Parquet. Puede ver los informes mediante un software de hojas de cálculo como Microsoft Excel o Apache OpenOffice Calc. También puede acceder a ellos desde una aplicación mediante las API de Amazon S3 o Amazon Athena.

AWS Los informes de costos y uso registran su AWS consumo y proporcionan una estimación de los cargos asociados a su cuenta. Cada informe contiene partidas para cada combinación única de AWS productos, tipo de uso y operación que utilices en tu AWS cuenta.

AWS Identity and Access Management (IAM)

El servicio AWS Billing Conductor está integrado con AWS Identity and Access Management (IAM). Puede utilizar IAM con AWS Billing Conductor para garantizar que las demás personas que trabajan en su cuenta solo tengan el acceso que necesiten para realizar su trabajo.

También utiliza IAM para controlar el acceso a todos sus AWS recursos. Esto incluye, entre otra, su información de facturación. Es importante que te familiarices con los conceptos básicos y las prácticas recomendadas de IAM antes de ir demasiado lejos con la configuración de la estructura de tu AWS cuenta.

Para obtener información acerca de la utilización de IAM, consulte ¿Qué es IAM? y Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

AWS Organizations (Facturación consolidada)

AWS los productos y servicios pueden adaptarse a empresas de todos los tamaños, desde pequeñas empresas emergentes hasta empresas. Si su empresa es grande, o probablemente vaya a crecer, quizá desee configurar varias cuentas de AWS que reflejen la estructura de la empresa. Por ejemplo, puede disponer de una cuenta para toda la empresa y de cuentas para cada empleado, o bien, de una cuenta para toda la empresa con usuarios de IAM para cada

empleado. Puede tener una cuenta para toda la empresa, cuentas para cada departamento o equipo dentro de la empresa y cuentas para cada empleado.

Si crea varias cuentas, puede utilizar la característica de facturación unificada de AWS Organizations para combinar todas las cuentas miembro en una cuenta de administración y recibir una sola factura. Para obtener más información, consulte Facturación unificada para organizaciones en la Guía del usuario de AWS Billing .

Cómo entender el panel de control del Conductor de facturación de AWS

El panel de control del Conductor de facturación de AWS proporciona un resumen detallado de las métricas clave para ayudarle a entender el impacto de sus dimensiones de precios personalizadas.

Indicadores clave de rendimiento (KPI)

En esta sección se definen los indicadores clave de rendimiento (KPI) que están disponibles en su panel de control del Conductor de facturación de AWS. Todos los KPI son del mes hasta la fecha. A medida que crea o agrega cuentas a su AWS Organizations, las cuentas se acumulan según este KPI. Al eliminar un grupo de facturación, las cuentas de ese grupo de facturación también se acumulan según este KPI.

- Importe cobrado: los cargos combinados por el uso acumulado por todos los grupos de facturación, basados en la tarifa personalizada definida por los planes de precios aplicados. El cálculo no tiene en cuenta ningún descuento basado en compromisos que se hayan adquirido fuera del grupo de facturación, ningún precio no público ni ningún crédito consumido en el dominio facturable. Los ejemplos de descuentos basados en el compromiso incluyen instancias reservadas y Savings Plans.
- AWS Costos: el cargo combinado del mes hasta la fecha por el uso acumulado por todos los grupos de facturación, de acuerdo con los cargos estimados de la factura de AWS. Los cálculos incluyen cualquier descuento basado en compromisos adquirido fuera del grupo de facturación si esos beneficios se aplicaron en el dominio facturable, cualquier precio no público, descuentos por volumen y créditos. Los ejemplos de descuentos basados en el compromiso incluyen instancias reservadas y Savings Plans.
- Margen: el margen acumulado del mes hasta la fecha por todos los grupos de facturación. El margen se calcula restando los costos de AWS del importe cobrado. En función de factores como el plan de precios y las partidas personalizadas aplicadas, el margen también puede ser negativo.

> **Note**
>
> Los ajustes posteriores al período de facturación afectan a sus márgenes históricos. Para obtener más información, consulte Análisis de los márgenes por grupo de facturación.

- Grupos de facturación: el número de grupos de cuentas que se excluyen mutuamente, con una cuenta principal y un plan de precios asociado.
- Cuentas monitoreadas: el número de cuentas de una familia de facturación unificada que están actualmente asignadas a un grupo de facturación.
- Cuentas no monitoreadas: la cantidad de cuentas de una familia de facturación unificada que no se han asignado a un grupo de facturación.

Otras definiciones de Conductor de facturación de AWS

En esta sección se definen otros términos que se utilizan en el Conductor de facturación de AWS para ayudarle a utilizar el servicio de forma eficaz.

- Facturable: el resultado de facturación que genera AWS y se utiliza como sesgo al calcular la factura de AWS.
- Pro forma: el resultado generado por el Conductor de facturación de AWS. Es coherente con los cambios que desee realizar en la gestión de tarifas (configuración de precios) y en la visibilidad agregada de las cuentas (grupos de facturación).
- Valores de los recursos: las entradas que se utilizan para calcular las partidas personalizadas basadas en porcentajes. Los valores de los recursos incluyen los costos acumulados del grupo de facturación y cualquier partida fija personalizada que esté asociada a un grupo de facturación determinado durante un período de facturación.

Visualización de sus cinco principales grupos de facturación por importe cobrado

Para conocer los cinco grupos principales de facturación que generan ingresos, consulte la vista visual y la tabla. Para administrar sus grupos de facturación existentes, elija Administrar grupos de facturación en la página del panel de control.

Creación de grupos de facturación, configuraciones de precios y partidas personalizadas

Esta sección muestra cómo puede crear grupos de facturación, configuraciones de precios y partidas personalizadas en AWS Billing Conductor. Cada sección también proporciona una descripción general de cómo puede utilizar la tabla de grupos de facturación, la tabla de reglas de precios y la tabla de partidas personalizadas después de crear cada artículo.

Temas

Creación de grupos de facturación

Puedes usar AWS Billing Conductor para crear grupos de facturación para organizar tus cuentas. De forma predeterminada, las cuentas de pagador con permisos de administrador pueden crear grupos de facturación. Cada grupo de facturación se excluye mutuamente. Esto significa que una cuenta solo puede pertenecer a un grupo de facturación en un período de facturación determinado. Si bien puede ver la segmentación del grupo de facturación de forma inmediata, las tarifas personalizadas del grupo tardarán hasta 24 horas en verse reflejadas en él después de crear un grupo de facturación.

> **Note**
>
> Al mover las cuentas de un grupo de facturación a mediados de mes, se iniciará el nuevo cálculo de ambos grupos de facturación hasta el inicio del período de facturación. El traslado de cuentas a mitad de mes no afecta a los períodos de facturación anteriores.

Siga los siguientes pasos para crear un grupo de facturación.

Cómo crear un grupo de facturación

1. Inicia sesión en AWS Billing Conductor AWS Management Console y ábrelo en https://console.aws.amazon.com/billingconductor/.
2. En el panel de navegación, elija Grupos de facturación.
3. Elija Crear grupo de facturación.
4. En Detalles del grupo de facturación, introduzca el nombre del grupo de facturación. Para conocer las restricciones de nomenclatura, consulte Cuotas y limitaciones.
5. (Opcional) En Descripción, escriba una descripción para el grupo de facturación.
6. En Plan de precios, elija un plan de precios para asociarlo al grupo de facturación. Para crear un plan de precios, consulte Creación de planes de precios.
7. (Opcional) Para Configuración adicional, puede habilitar la asociación automática de cuentas para el grupo de facturación.

   > **Notas**
   >
   > - Solo un grupo de facturación puede tener una asociación automática de cuentas.
   > - Una vez que habilite esta característica, las cuentas que se creen o agreguen a su organización se asociarán automáticamente a este grupo de facturación.
   > - Si actualmente tienes un CloudTrail registro de registro, puedes revisar las asociaciones automáticas de tus cuentas en tu CloudTrail registro.

8. En Cuentas, seleccione una o más cuentas para añadirlas al grupo de facturación o seleccione Importar unidad organizativa para seleccionar automáticamente las cuentas que se encuentran dentro de una unidad organizativa. Para ver un ejemplo de política que permita el acceso a la característica de importación de UO, consulte Concesión de acceso a la característica de importación de unidades organizativas a Billing Conductor.

   Puede usar el filtro de tabla para ordenar por nombres de cuenta, ID de cuenta o la dirección de correo electrónico raíz asociada a una cuenta.
9. La cuenta principal hereda la capacidad de ver los costos y el uso proforma en todo el grupo de facturación y puede generar informes proforma de costos y uso (AWS CUR) para el grupo de facturación.

   Si eliges una cuenta principal que se unió a tu organización durante el mes en curso, los costos proforma de todas las cuentas de ese grupo de facturación solo incluirán el costo y el uso

acumulados desde que la cuenta principal se unió a la organización. Para comprobar la fecha de unión, seleccione Validar la fecha de incorporación. Para obtener más información, consulte Comprensión de la importancia de la fecha de registro de la cuenta principal.

10. Elija Crear grupo de facturación.

> **Notas**
>
> - Debe seleccionar su cuenta principal en el paso 9. No puede cambiar su cuenta principal una vez creado el grupo de facturación. Para asignar una nueva cuenta principal, elimine el grupo de facturación y reagrupe sus cuentas. Si bien una cuenta de pagador se puede incluir en un grupo de facturación, a una cuenta de pagador no se le puede asignar el rol de cuenta principal.
> - Si la cuenta principal de un grupo de facturación abandona su organización y este grupo de facturación tiene habilitada la asociación automática de cuentas, seguirá asociando cuentas automáticamente hasta final de mes. Después, el grupo de facturación se eliminará automáticamente. Puede habilitar la asociación automática de cuentas para un grupo de facturación existente o crear otro.

Tabla del grupo de facturación

Después de crear un grupo de facturación, puede ver los detalles del grupo de facturación en una tabla que se puede filtrar. Puede filtrar utilizando las siguientes dimensiones:

- Nombre del grupo de facturación
- Nombre de la cuenta principal
- ID de cuenta principal
- Número de cuentas
- Nombre del plan de precios

Para ver los detalles de cada grupo de facturación, seleccione el nombre del grupo de facturación en la tabla. El grupo de facturación que habilitó para la característica de asociación automática de cuentas tendrá un icono de asociación automática junto al nombre del grupo de facturación.

Creación de reglas de precios

Puedes crear reglas de precios en AWS Billing Conductor para personalizar tus tarifas de facturación en todos tus grupos de facturación. Las reglas de precios pueden ser globales, específicas del servicio, específicas de la entidad de facturación o de alcance específico de la SKU. Puede utilizar las reglas de precios para aplicar un descuento o un aumento de precio para cada ámbito de aplicación correspondiente. Los ámbitos no se superponen. Los ámbitos se aplican del más detallado al menos detallado cuando hay reglas de precios con diferentes ámbitos incluidas en un único plan de precios. Para las reglas de precios globales, también puede optar por desactivar o activar las tarifas de `Always Free Tier`. Las reglas de precios con nivel Siempre gratis desactivado establecen de forma predeterminada el primer nivel de pago para el tipo de uso o la operación. De forma predeterminada, una cuenta de pagador con permisos de administrador puede crear reglas de precios. Tras aplicar una regla de precios a un grupo de facturación, las tarifas personalizadas de ese grupo de facturación tardan hasta 24 horas en verse reflejadas.

Se puede aplicar un único plan de precios a varios grupos de facturación.

Para crear un repositorio privado, complete los pasos siguientes.

Cómo crear una regla de precios

1. Abre AWS Billing Conductor en https://console.aws.amazon.com/billingconductor/.
2. En el panel de navegación, elija Configuración de precios.
3. Elija la pestaña Reglas de precios.
4. Elija Crear reglas de precios.
5. En Detalles de la regla de precios, introduzca el nombre de la regla de precios. Para conocer las restricciones de nomenclatura, consulte Cuotas y limitaciones.
6. (Opcional) En Descripción, escriba una descripción para la regla de precios.
7. En Alcance, elija `Global`, `Service`, `Billing entity` oSKU.

   - Global: se aplica a todos los usos.
   - Servicio: solo se aplica a un servicio determinado. Al elegir servicio, elija un código de servicio para configurar las tarifas. Cuando elija un servicio, elija el código de servicio de la API de consulta de listas de precios que desee ajustar.
   - Entidad de facturación: solo se aplica a una entidad de facturación determinada. Una entidad de facturación es el vendedor de los servicios prestados por AWS sus filiales o proveedores externos a través de los cuales venden servicios AWS Marketplace.

- SKU: solo se aplica a la combinación única de código de servicio (producto), tipo de uso u operación.

8. En Tipo, seleccione Descuento, Aumento de precio o Agrupación por niveles.

> **Note**
>
> Agrupación por niveles solo está disponible para las reglas de precios globales y relacionadas con el servicio.

9. En Porcentaje, introduzca el importe porcentual.

   Si introduce **0** como porcentaje, el plan de precios utilizará de forma predeterminada la tarifa bajo demanda de AWS . Si introduce un valor decimal, se redondeará a los 2 decimales más próximos.

10. Para el tipo Agrupación en niveles, puede marcar la casilla situada debajo de Configuración de agrupación en niveles para desactivar el nivel nivel Siempre gratis o dejarla activada. El nivel Siempre gratis estará activado a menos que se desactive explícitamente.
11. (Opcional) Para crear otra regla de precios en el mismo flujo de trabajo, seleccione Añadir regla de precios.
12. Seleccione Crear regla de precios.

Tabla de reglas de precios

Después de crear una regla de precios, puede ver los detalles de la regla de precios en una tabla que se puede filtrar. Puede filtrar utilizando las siguientes dimensiones:

- Nombre de la regla de precios
- Ámbito
- Tipo
- Detalles
- Tarifa

Creación de planes de precios

Puede crear planes de precios en AWS Billing Conductor para personalizar la salida de sus detalles de facturación en todos sus grupos de facturación. De forma predeterminada, una cuenta de pagador con permisos de administrador puede crear planes de precios. Tras aplicar un plan de precios a un grupo de facturación, las tarifas personalizadas de ese grupo de facturación tardan hasta 24 horas en verse reflejadas.

Se puede aplicar un único plan de precios a varios grupos de facturación.

> **Note**
>
> La actualización de un plan de precios también afecta a los detalles de facturación de cada grupo de facturación al que está asociado el plan de precios. Si el plan de precios está asociado a un grupo o conjunto de grupos de facturación, este cambio solo afecta al período de facturación actual. Los períodos de facturación anteriores siguen siendo los mismos.

Siga los siguientes pasos para crear un plan de precios.

Cómo crear un plan de precios

1. Abre AWS Billing Conductor en https://console.aws.amazon.com/billingconductor/.
2. En el panel de navegación, elija Configuración de precios.
3. En la pestaña Plan de precios, seleccione Crear un plan de precios.
4. Para Detalles del plan de precios, introduzca el nombre del plan de precios. Para conocer las restricciones de nomenclatura, consulte Cuotas y limitaciones.
5. (Opcional) En Descripción, escriba una descripción para el plan de precios.
6. En la tabla de reglas de precios, seleccione las reglas de precios que desea asociar al plan de precios. Puede filtrar las reglas de precios por nombre de la regla de precios, alcance, detalles, tipo o tarifa.
7. Elija Crear plan de precios.

Tabla de planes de precios

Después de crear un plan de precios, podrá ver los detalles del plan de precios en una tabla que se puede filtrar. Puede filtrar utilizando las siguientes dimensiones:

- El nombre del plan de precios
- La descripción
- El número de reglas de precios asociadas al plan de precios

Creación de partidas personalizadas por grupo de facturación

Se utiliza AWS Billing Conductor para crear partidas personalizadas y aplicarlas a las partidas designadas Cuentas de AWS dentro de un grupo de facturación.

Puede asignar costos y descuentos mediante partidas personalizadas. Puede calcular una partida personalizada como un valor de cargo fijo o porcentual. Configure la partida personalizada basada en porcentajes para incluir o excluir recursos. Estos recursos incluirán los costos de los grupos de facturación y otras partidas personalizadas fijas que estén asociadas a un grupo de facturación durante un período de facturación. A continuación, puede configurar las partidas personalizadas para que se apliquen durante un mes o para que se repitan durante varios meses.

Los casos de uso más comunes para la creación de partidas personalizadas incluyen, entre otros, los siguientes:

- Asignación de tarifas AWS Support
- Asignación de costos de servicios compartidos
- Aplicación de tarifas de servicios gestionados
- Aplicación de impuestos
- Distribución de créditos
- Distribución de los ahorros de RI y Savings Plans (en lugar de hacerlo bajo demanda)
- Añadido de créditos organizativos y líneas de descuento

Creación de una partida personalizada con cargo fijo

Siga los siguientes pasos para crear una partida personalizada que aplique una partida de crédito o de tarifa a un grupo de facturación individual.

Cómo crear partidas personalizadas

1. Abra AWS Billing Conductor en https://console.aws.amazon.com/billingconductor/.
2. En el panel de navegación, elija Partidas personalizadas.

3. Seleccione Crear partida personalizada.
4. Para ver los detalles de la partida personalizada, introduzca el nombre de la partida personalizada. Para conocer las restricciones de nomenclatura, consulte Cuotas y limitaciones.
5. En Descripción, introduzca una descripción para la partida personalizada. El límite es de 255 caracteres.
6. En Período de facturación, elija el período de facturación existente o el período de facturación anterior.
7. En Duración, elija un mes o recurrente (sin fecha de finalización definida).
8. En Grupo de facturación, seleccione un grupo de facturación. Solo puede asociar el cargo personalizado a un grupo de facturación a la vez.

    - (Opcional) En el caso de las cuentas asignadas, puede aplicar su partida personalizada a la cuenta del grupo de facturación que prefiera. De forma predeterminada, su partida personalizada se aplica a la cuenta principal del grupo de facturación que elija.
9. Elija Cargo fijo para el tipo de artículo de línea personalizado.
10. Elige un tipo de cargo e introduce un importe de entrada.

    Una partida de descuento añade un crédito. Esto reduce el importe que se carga al grupo de facturación seleccionado. Una partida con aumento de precio añade un cargo. Esto aumenta el importe que se carga al grupo de facturación seleccionado. Todas las partidas personalizadas se indican en USD.
11. Seleccione Crear.

Creación de una partida personalizada con cargo porcentual

Siga los siguientes pasos para crear una partida personalizada que aplique una partida de crédito o de tarifa a un grupo de facturación individual.

Cómo crear partidas personalizadas

1. Abre AWS Billing Conductor en https://console.aws.amazon.com/billingconductor/.
2. En el panel de navegación, elija Partidas personalizadas.
3. Seleccione Crear partida personalizada.
4. Para ver los detalles de la partida personalizada, introduzca el nombre de la partida personalizada. Para conocer las restricciones de nomenclatura, consulte Cuotas y limitaciones.

5. En Descripción, introduzca una descripción para la partida personalizada. El límite es de 255 caracteres.
6. En Período de facturación, elija el período de facturación existente o el período de facturación anterior.
7. En Duración, elija un mes o recurrente (sin fecha de finalización definida).
8. En Grupo de facturación, seleccione un grupo de facturación. Solo puede asociar el cargo personalizado a un grupo de facturación a la vez.
    - (Opcional) En el caso de las cuentas asignadas, puede aplicar su partida personalizada a la cuenta del grupo de facturación que prefiera. De forma predeterminada, su partida personalizada se aplica a la cuenta principal del grupo de facturación que elija.
9. Elige el porcentaje de cargo para el tipo de artículo de línea personalizado.
10. Elige un tipo de cargo e introduce un importe de entrada.

    Una partida de descuento añade un crédito. Esto reduce el importe que se carga al grupo de facturación seleccionado. Una partida con aumento de precio añade un cargo. Esto aumenta el importe que se carga al grupo de facturación seleccionado. Todas las partidas personalizadas se indican en USD.
11. (Opcional) Para Valores de recursos, elija los valores que desee incluir en el cálculo. De forma predeterminada, el costo total del grupo de facturación se selecciona como recurso. Esto excluye todas las partidas fijas personalizadas.
    - (Opcional) De forma predeterminada, se incluyen los descuentos del Savings Plan. Para excluirlos del cálculo, active la casilla Excluir los descuentos del Plan de Ahorros.
12. (Opcional) Incluye una o más líneas de pedido personalizadas y planas. Elija cada línea de pedido personalizada plana aplicable de la tabla que desee incluir en el cálculo basado en porcentajes.

    > **Note**
    >
    > Puede crear partidas personalizadas porcentuales sin recursos asociados. Estas partidas personalizadas muestran un valor de `$0.00` en sus datos de facturación.
13. Seleccione Crear.

Tabla de partidas personalizadas

Después de crear una partida personalizada, puede ver los detalles del artículo de línea en una tabla que se puede filtrar. Puede filtrar utilizando las siguientes dimensiones:

- El nombre de la partida
- La descripción de la partida
- El importe que se cobra
- El grupo de facturación al que se atribuye la partida
- La fecha en que se creó la partida

Para ver las partidas personalizadas que creó en períodos de facturación anteriores, use la lista desplegable selector de fechas.

Edición de partidas personalizadas

Siga los pasos que se describen a continuación para editar sus partidas personalizadas.

Cómo editar una partida personalizada

1. Abra AWS Billing Conductor en https://console.aws.amazon.com/billingconductor/.
2. En el panel de navegación, elija Partidas personalizadas.
3. Seleccione Crear partida personalizada.
4. Elija la partida personalizada que desea editar.
5. Elija Editar.
6. Cambie los parámetros que desee editar.

> **Note**
>
> No puede cambiar el período de facturación, el grupo de facturación, la cuenta asignada, el tipo de cargo (fijo o porcentual) ni el tipo de valor del cargo (crédito o tarifa).

7. Elija Guardar cambios.

Eliminación de partidas personalizadas

Siga los pasos que se describen a continuación para eliminar partidas personalizadas.

Cómo editar una partida personalizada

1. Abre AWS Billing Conductor en https://console.aws.amazon.com/billingconductor/.
2. En el panel de navegación, elija Partidas personalizadas.
3. Seleccione Crear partida personalizada.
4. Elija la partida personalizada que desea eliminar.
5. Elija Eliminar.
6. Lea cómo le puede afectar la eliminación de la partida personalizada y, a continuación, seleccione Eliminar partida personalizada.

Mejores prácticas para AWS Billing Conductor

En esta sección se destacan algunas de las mejores prácticas para trabajar con AWS Billing Conductor.

Temas

Comprensión de la importancia de la fecha de registro de la cuenta principal

La fecha en que la cuenta principal se unió a su organización define el límite histórico de los costos proforma de ese grupo de facturación. Si eliges una cuenta principal que se creó o se vinculó a tu cuenta de administración a mediados de mes, los costos proforma no incluirán los costos de otras cuentas del grupo de facturación, incluidas las cuentas que formaban parte de tu organización antes de que se uniera la cuenta principal.

Por ejemplo, supongamos que la cuenta principal se unió a su organización el 15 de octubre. La factura proforma de todas las cuentas del grupo de facturación solo incluirá el costo y el uso a partir de esa fecha. La factura proforma comienza el 15 de octubre, incluso si otras cuentas del grupo de facturación eran miembros de la organización antes del mes en curso.

Habrá una discrepancia entre el dominio de facturación facturable y el dominio de facturación proforma durante el primer mes del grupo de facturación. El dominio pro forma no incluirá ningún uso acumulado antes del 15 de octubre. Después del primer mes, los costes proforma incluirán todo el uso.

Para evitar esta discrepancia inicial entre los datos facturables y proforma de la primera factura del grupo de facturación, elige una cuenta principal que haya estado vinculada a la cuenta de administración durante todo el mes o antes.

Controlar el acceso a Billing Conductor AWS

Solo los usuarios con acceso a la cuenta de administración o pagadora pueden acceder a Administración de costos y facturación. Para conceder a los usuarios de IAM permiso para crear grupos de facturación y ver los indicadores clave de rendimiento (KPI) de AWS Billing Conductor en la consola de Billing and Cost Management, también debe conceder a los usuarios de IAM lo siguiente:

- Listado de cuentas dentro de organizaciones

Para obtener más información sobre cómo ofrecer a los usuarios la posibilidad de crear grupos de facturación y planes de precios en la consola de AWS Billing Conductor, consulte. Administración de identidad y acceso para AWS Billing Conductor

También puede crear recursos de AWS Billing Conductor mediante programación mediante la API de AWS Billing Conductor. Cuando configure el acceso a la API de AWS Billing Conductor, le recomendamos crear un usuario de IAM único para permitir el acceso mediante programación. Esto le ayuda a definir controles de acceso más precisos entre las personas de su organización que tienen acceso a la consola de AWS Billing Conductor y a la API. Para permitir que varios usuarios de IAM accedan mediante consultas a la API de AWS Billing Conductor, recomendamos crear una función de IAM de acceso programático para cada uno de ellos.

Comprender el conjunto de AWS datos de Billing Conductor

Si bien los modelos de datos de AWS Billing Conductor comparten muchas similitudes con el modelo de datos de AWS facturación estándar, existen algunas diferencias.

El conductor de AWS facturación no incluye:

- Créditos (canjeados a nivel del pagador o de la cuenta vinculada)
- Impuestos
- AWS Support cargos

Además, AWS Billing Conductor comparte las instancias reservadas y los Savings Plans con las cuentas incluidas en el mismo grupo de facturación, independientemente de sus preferencias de uso compartido en el dominio de facturación estándar.

Comprensión de la lógica computacional de AWS Billing Conductor

El cálculo AWS de Billing Conductor se adapta a los cambios que realices en un mes determinado y, al mismo tiempo, conserva la integridad histórica de los datos de facturación del período anterior. La mejor forma de describir esto es con un ejemplo.

En este ejemplo, tenemos dos grupos de facturación: `A` y `B`. El grupo de facturación `A` comienza el período de facturación con las cuentas 1 a 3 del grupo. A mediados de mes, la cuenta del pagador pasa de `Account 3` a `Billing Group B`. En ese momento, es necesario volver a calcular los costos de los grupos de facturación `A` y `B` para modelar con precisión el último cambio. Cuando `Account 3` se mueve, el uso de `Billing Group A` se modela como si `Account 3` no hubiera formado parte del grupo de facturación durante el período de facturación actual. Además, el uso de `Billing Group B` se modela como si `Account 3` hubiera formado parte de `Billing Group B` desde el comienzo del período de facturación. Este enfoque elimina la necesidad de calcular tarifas complejas y modelos de reintegros cuando las cuentas se mueven de un grupo a otro durante el período de facturación.

Grupo de facturación A	Días: 1 a 15	Días: 16 a 30	Fin de mes
Cuenta 1	100$	100$	200$
Cuenta 2	100$	100$	200$
Cuenta 3	100$	N/A	N/A
Total	300$	200$	400$

Grupo de facturación B	Días: 1 a 15	Días: 16 a 30	Fin de mes
Cuenta 4	100$	100$	200$

Grupo de facturación B	Días: 1 a 15	Días: 16 a 30	Fin de mes
Cuenta 5	100$	100$	200$
Cuenta 6	100$	100$	200$
Cuenta 3	100$	100$	200$
Total	400$	400$	800$

Conozca la frecuencia de actualización AWS de Billing Conductor

AWS los datos de facturación se actualizan al menos una vez al día. AWS Billing Conductor utiliza estos datos para calcular sus datos de facturación proforma. Las partidas personalizadas que se generan para aplicarse al mes actual se ven reflejadas en un plazo de 24 horas. Las partidas personalizadas que se generan para aplicarse al período de facturación anterior pueden tardar hasta 48 horas en reflejarse en los informes de AWS costos y uso de un grupo de facturación o en la página de facturas de un grupo de facturación determinado.

Comprender las diferencias entre el conductor AWS de facturación (AWS CUR) y el CUR estándar AWS

Existen algunas diferencias entre los informes de costo y uso estándar y el AWS CUR pro forma creado con la configuración de AWS Billing Conductor.

- El AWS CUR estándar calcula el costo y el uso de cada cuenta de la familia de facturación unificada. Un AWS CUR pro forma por grupo de facturación solo incluye las cuentas del grupo de facturación en el momento del cálculo.
- El AWS CUR estándar rellena la columna de la factura una vez y la factura la genera. AWS Un AWS CUR proforma no rellena la columna de la factura. Actualmente, no se genera ni emite ninguna factura en AWS función de los datos de facturación proforma.

Análisis de los márgenes por grupo de facturación

Puedes usar el resumen de márgenes y los detalles de los márgenes en AWS Billing Conductor para analizar tus márgenes tanto en conjunto como con grupos de facturación específicos.

Utilice los siguientes pasos para ver los márgenes de un grupo de facturación individual o de un conjunto de grupos de facturación.

Temas

Vea sus márgenes en conjunto mediante el resumen de márgenes

Para ver el resumen de los márgenes de tu grupo de facturación

1. Abre AWS Billing Conductor en https://console.aws.amazon.com/billingconductor/.
2. En el panel de navegación, en Analytics, selecciona Resumen de márgenes.
3. En Tipo de informe, selecciona Todos los grupos de facturación o Selecciona el grupo de facturación.
4. Si seleccionó Seleccionar grupos de facturación, elija un período de facturación y uno o más grupos de facturación.
5. En la sección de onth-to-date resumen de M, puedes ver el importe cobrado, AWS los costes y el margen.
6. Puedes ver tu análisis de márgenes de dos maneras:
   - Como gráfico de barras en la sección Rendimiento (hasta los últimos 13 meses).
   - Como una tabla de la tabla de análisis de márgenes.

   Los márgenes negativos se muestran en rojo en el gráfico, con un importe en dólares negativo y un porcentaje negativo.

Comprenda su tabla de análisis de márgenes

La tabla de análisis de márgenes del grupo de facturación se ordena en orden cronológico inverso de forma predeterminada. Puede ordenar la tabla por todas las columnas, entre las que se incluyen las siguientes:

- Mes
- Importe cobrado
- AWS costos
- Importe del margen
- Porcentaje de margen

El gráfico y la tabla muestran los valores de los últimos 13 meses de los grupos de facturación seleccionados. Si los grupos de facturación se crearon en momentos diferentes, asumimos el intervalo de tiempo del grupo de facturación seleccionado más antiguo.

Puede exportar la tabla de análisis de márgenes a un archivo CSV descargable. Junto a la tabla de análisis de márgenes, seleccione Descargar CSV. La descarga se iniciará automáticamente.

> **Note**
>
> Para descargar un archivo CSV con el análisis de márgenes de su grupo de facturación, debe añadir el permiso de `billingconductor:ListBillingGroupCostReport` a su política de IAM.

Vea sus márgenes Servicio de AWS por unidad utilizando los detalles de los márgenes

Para ver los márgenes de tu grupo de facturación por servicio

1. Abre AWS Billing Conductor en https://console.aws.amazon.com/billingconductor/.
2. En el panel de navegación, en Analytics, selecciona Detalles del margen.
3. En Parámetros del informe, elija un período de facturación y un grupo de facturación.
4. Puedes ver tu análisis de márgenes de dos maneras:

- Como gráfico de líneas en la sección de tendencia de los márgenes según los 5 principales servicios.
- Como una tabla de la tabla de análisis de márgenes.

Comprenda su gráfico de tendencias de márgenes

Los detalles de tus márgenes mostrarán un gráfico de líneas con los cinco principales servicios por margen para el período de facturación elegido. El gráfico de líneas mostrará los márgenes de cada servicio durante los últimos tres meses a modo de comparación.

El gráfico también incluirá una tabla en la que se muestran los márgenes de cada servicio para el período de facturación elegido. La tabla muestra el margen promedio calculado durante los últimos tres meses, que incluye las siguientes columnas:

- Nombre del servicio
- Media
- Margen

Si el grupo de facturación no estuvo activo durante los últimos tres meses, el gráfico solo mostrará los datos del informe de costos que estén disponibles.

Comprenda su tabla de análisis de márgenes

La tabla de análisis de márgenes del grupo de facturación incluye las siguientes columnas:

- Nombre del servicio
- Importe cobrado
- AWS costes
- Importe del margen
- Porcentaje de margen

Puede exportar la tabla de análisis de márgenes a un archivo CSV descargable. Junto a la tabla de análisis de márgenes, seleccione Descargar CSV. La descarga se iniciará automáticamente.

> **Note**
>
> Para descargar un archivo CSV con el análisis de márgenes de su grupo de facturación, debe añadir el permiso de `billingconductor:GetBillingGroupCostReport` a su política de IAM.

Visualización de los detalles del grupo de facturación

Puede usar los detalles de su grupo de facturación para monitorear, analizar y editar su grupo de facturación en el Conductor de facturación de AWS. Los detalles del grupo de facturación proporcionan un análisis de los márgenes del mes hasta la fecha, un historial de las partidas personalizadas aplicadas y la posibilidad de editar y eliminar el grupo de facturación según sea necesario.

Visualización de los detalles de facturación por dimensiones de precios personalizadas

Después de crear y asignar los grupos de facturación y los planes de precios, puede ver las dimensiones de facturación personalizadas con detalle por tipo de uso para cada grupo de facturación gestionado.

Siga estos pasos para ver los detalles de facturación en el dominio proforma.

Para ver sus detalles de facturación proforma

1. Abra la consola de AWS Billing en https://console.aws.amazon.com/billing/.
2. En el panel de navegación, seleccione Facturas.
3. Seleccione Configuración en la esquina superior derecha de los detalles de facturación.
4. Active la Vista de datos proforma.
5. En Grupo de facturación, seleccione la facturación que desea analizar.

Puede analizar el uso del grupo de facturación por servicio y región de AWS para ver el coste de ese uso, de acuerdo con las tarifas definidas en Conductor de facturación de AWS.

Puede encontrar las partidas personalizadas en el servicio Conductor de facturación de AWS, en la página Detalles de facturación.

Configuración de Informes de coste y uso por grupo de facturación

Puede crear Informes de coste y uso de AWS proforma (CUR de AWS) para cada grupo de facturación que cree. El CUR de AWS proforma tiene el mismo formato de archivo, granularidad y columnas que el CUR de AWS estándar, y contiene el conjunto de datos de coste y uso más completo disponible para un período de tiempo determinado.

Puede publicar su CUR de AWS proforma en un bucket de Amazon Simple Storage Service (Amazon S3) de su propiedad.

AWS actualiza el informe en el bucket una vez al día en un archivo con formato de valores separados por comas (CSV). Puede ver los informes con un software de hojas de cálculo como Microsoft Excel o Apache OpenOffice Calc. También puede acceder a ellos desde una aplicación mediante las API de Amazon S3 o Amazon Athena. Para obtener información acerca de AWS, consulte AWSla Guía de informes de uso y costos.

Siga los siguientes pasos para generar un CUR de AWS proforma para un grupo de facturación.

Para crear Informes de costos y uso proforma para un grupo de facturación

1. Abra la consola de AWS Billing en https://console.aws.amazon.com/billing/.
2. En el panel de navegación, elija Informes de costos y uso.
3. En la parte superior derecha de la tabla de informes, seleccione Configuración.
4. Active la vista de datos Pro forma .
5. Elija Habilitar.
6. Elija Crear informe.
7. En Nombre del informe, escriba un nombre para su informe.
8. Para Vista de datos, elija pro forma.
9. Para Grupo de facturación, seleccione un grupo de facturación.
10. En Detalles adicionales del informe, seleccione Incluir ID de recurso para incluir los ID de cada recurso individual en el informe.
11. En Configuración de actualización de datos, seleccione si desea que los Informes de coste y uso de AWS se actualicen con cualquier cambio nuevo en sus datos de coste y uso una vez finalizada la factura. Cuando se actualiza un informe, se carga uno nuevo en Amazon S3.

> **Note**
>
> Los Informes de coste y uso del grupo de facturación no incluyen créditos, impuestos ni cargos de soporte.

12. Elija Siguiente.
13. En Bucket de S3, seleccione Configuración.
14. En el cuadro de diálogo Configurar bucket de S3, realice una de las acciones siguientes:
    - Seleccione un bucket existente de la lista desplegable y elija Siguiente.
    - Escriba un nombre de bucket y la región de AWS en la que desee crear un nuevo bucket y elija Siguiente.
15. Seleccione He confirmado que esta política es correcta y elija Guardar.
16. En Prefijo de ruta de informe, escriba el prefijo de la ruta de informe que desee anexar al nombre del informe.

    Este paso es opcional para Amazon Redshift o Amazon QuickSight, pero obligatorio para Amazon Athena.

    Si no especifica un prefijo, el prefijo predeterminada será el nombre que especificó para el informe en el paso 4 y el intervalo de fechas del informe en el siguiente formato:

    ```
    /report-name/date-range/
    ```
17. En Grado de detalle del periodo de tiempo, elija una de las opciones siguientes:
    - Por hora si desea que las partidas del informe se agreguen hora a hora.
    - Por día si desea que las partidas del informe se agreguen día a día.
18. En Control de versiones de informe, elija si desea que cada versión del informe sobrescriba la versión anterior del mismo o que se facilite además de las versiones anteriores.
19. En Habilitar la integración de datos de informes para, elija si quiere cargar sus Informes de coste y uso a Amazon Athena, Amazon Redshift o Amazon QuickSight. El informe está comprimido en los siguientes formatos:
    - Athena: compresión de parquet
    - Amazon Redshift o Amazon QuickSight: compresión .gz
20. Elija Siguiente.

21. Tras terminar de revisar la configuración de su informe, elija Revisar y finalizar.

Realizar un análisis ad hoc de los costos pro forma en AWS Cost Explorer

Cuentas de AWSen Billing Conductor, los grupos de facturación pueden analizar, pronosticar e informar los costos pro forma en Cost Explorer. La cuenta principal de un grupo de facturación puede realizar estas actividades para todas las cuentas del grupo. Si lo usaAWS Organizations, las cuentas de administración no pueden analizar, pronosticar ni informar los costos pro forma en Cost Explorer.

Las cuentas administradas por grupos de facturación (miembros del grupo de facturación) pueden ver los datos de costo y uso de los períodos de facturación en los que fueron miembros del grupo de facturación, y hay datos proforma disponibles. No pueden ver los datos históricos de costos y uso facturables.

Notas

- Las cuentas administradas por Billing Conductor (miembros del grupo de facturación) pueden ver los costos pro forma en Cost Explorer.
- Los datos de granularidad horaria no son compatibles con los costos pro forma en Cost Explorer.
- Para obtener más información sobre los flujos de trabajo principales compatibles con el Explorador de costos, consulte Exploración de sus datos con el Explorador de costos en la Guía del usuario de AWS Cost Management.

Para obtener una lista de Servicios de AWS esos costos proforma de soporte, consulteServicios de AWS que respaldan los costos pro forma.

Servicios de AWS que respaldan los costos pro forma

Los siguientes servicios de administración financiera en la nube y sus funciones respaldan los costos proforma.

Características de los servicios	Support level by Cuenta de AWS type		
	Pagador (cuenta de administración)	Cuenta principal	Vinculada (cuenta de miembro)
AWS Cost and Usage Report	Sí	Sí	Sí
Asignación de costos divididos	No	No	No
AWS Billing	No	Sí	Sí
Panel de control	No	Sí	Sí
Detalles de facturación	Sí	Sí	Sí
Descargar CSV	No	No	No
AWS Cost Explorer	No	Sí	Sí
Previsiones	No	Sí	Sí
Informes guardados	No	Sí	Sí
Recomendaciones de redimensionamiento	No	No	No
Monitores de anomalías de costos	No	No	No

Características de los servicios	Support level by Cuenta de AWS type		
Recomendaciones de Savings Plans	No	No	No
Informe de uso de Savings Plans	No	No	No
Informe de cobertura de Savings Plans	No	No	No
Recomendaciones de las reservas	No	No	No
Informe de uso de las reservas	No	No	No
Informe de cobertura de las reservas	No	No	No
AWS Budgets	No	No	No
Informes de presupuestos	No	No	No

En el caso de los servicios y funciones que no admiten costes proforma, Cuentas de AWS verá los costes según las tarifas facturables, que coincidan con las de la AWS factura.

Información relacionada

Para gestionar el acceso de las cuentas vinculadas a los reembolsos, créditos y descuentos facturables, consulte la sección AWS Cost Explorer de la página Preferencias de la Consola de administración de costos.

Si no quiere que sus entidades de IAM vean las tarifas facturables específicas de estos servicios y características, puede utilizar las políticas de IAM para denegar el acceso. Para ver una política de IAM de ejemplo, consulte Denegar a Billing y Cost Explorer el acceso a servicios y funciones que no admiten costos pro forma.

También puede personalizar sus políticas de IAM para permitir o denegar permisos específicos. Para obtener una lista detallada de las acciones de IAM para Administración de costos y facturación, consulte los siguientes temas:

- Migración del control de acceso para AWS Cost Management en la Guía del usuario de AWS Cost Management
- Migración del control de acceso para AWS Billing y en la Guía del usuario de AWS Billing

Uso de la API AWS Billing Conductor

La API del Conductor de facturación está disponible en Java, Python, .NET y Go. Las nuevas capacidades publicadas en el Conductor de facturación también estarán disponibles como API.

Para obtener más información acerca de la API del Conductor de facturación de AWS, consulte la Referencia de la API de AWS Billing Conductor.

Seguridad en AWS Billing Conductor

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener información sobre los programas de conformidad que se aplican a AWS Billing Conductor, consulte AWS Services in Scope by Compliance Program .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a entender cómo aplicar el modelo de responsabilidad compartida al utilizar AWS Billing Conductor. Los siguientes temas le muestran cómo configurar AWS Billing Conductor para cumplir sus objetivos de seguridad y cumplimiento. También aprenderá a utilizar otros servicios de AWS que le ayudan a supervisar y proteger sus recursos de AWS Billing Conductor.

Temas

Protección de datos en AWS Billing Conductor

El modelo de se aplica a protección de datos en AWS Billing Conductor. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con AWS Billing Conductor u otra persona Servicios de AWS mediante la consola, la API o los SDK. AWS CLI AWS Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos

encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Administración de identidad y acceso para AWS Billing Conductor

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién se puede autenticar (iniciar sesión) y recibir autorización (tener permisos) para utilizar Billing Conductor. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realice en Billing Conductor.

Usuario del servicio: si utiliza el servicio de Billing Conductor para realizar su trabajo, su administrador le proporcionará las credenciales y los permisos que necesita. A medida que utilice más características de Billing Conductor para realizar su trabajo, es posible que necesite otros permisos. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica de Billing Conductor, consulte Solución de problemas AWS Billing Conductor de identidad y acceso.

Administrador del servicio: si está a cargo de los recursos de Billing Conductor en su empresa, probablemente disponga de acceso total a Billing Conductor. Su trabajo consiste en determinar a

qué características y recursos de Billing Conductor deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Billing Conductor, consulte ¿Cómo AWS Billing Conductor funciona con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera obtener más detalles sobre cómo escribir políticas para administrar el acceso a Billing Conductor. Para consultar ejemplos de políticas basadas en la identidad de Billing Conductor que puede utilizar en IAM, consulte AWS Billing Conductor ejemplos de políticas basadas en la identidad.

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, asumes un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Usuario raíz de la cuenta de AWS

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos de Servicios de AWS la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede

asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS Single Sign-On.
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para

obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

- Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en

función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

¿Cómo AWS Billing Conductor funciona con IAM

Antes de utilizar IAM para administrar el acceso a Billing Conductor, debe comprender qué características de IAM están disponibles para su uso con Billing Conductor. Para obtener una visión general de cómo funcionan Billing Conductor y otros AWS servicios con IAM, consulte AWS Servicios que funcionan con IAM en la Guía del usuario de IAM.

Temas

- Políticas basadas en identidades de Billing Conductor
- Políticas basadas en recursos de Billing Conductor
- Listas de control de acceso (ACL)
- Autorización basada en etiquetas de Billing Conductor
- Roles de IAM de Billing Conductor

Políticas basadas en identidades de Billing Conductor

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Billing Conductor admite acciones, claves de condiciones y recursos específicos. Para obtener información sobre todos los elementos que utiliza en una política JSON, consulte Referencia de los elementos de las políticas JSON de IAM en la Guía del usuario de IAM.

Acciones

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones de políticas de Billing Conductor utilizan el siguiente prefijo antes de la acción: `Billing Conductor:`. Por ejemplo, para conceder a alguien permiso para ejecutar una instancia de Amazon EC2 con la operación `RunInstances` de la API de Amazon EC2, debe incluir la acción `ec2:RunInstances` en la política. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. Billing Conductor define su propio conjunto de acciones que describen las tareas que se pueden realizar con este servicio.

Para especificar varias acciones en una única instrucción, sepárelas con comas del siguiente modo:

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

Puede utilizar caracteres comodín para especificar varias acciones (*). Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción:

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

Para ver una lista de las acciones del responsable de facturación, consulte las acciones definidas por el responsable AWS de facturación en la guía del usuario de IAM.

Recursos

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

El recurso de instancia de Amazon EC2 tiene el siguiente ARN:

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

Para obtener más información sobre el formato de los ARN, consulte Nombres de recursos de Amazon (ARN) y espacios de nombres de AWS servicio.

Por ejemplo, para especificar la instancia de `i-1234567890abcdef0` en su instrucción, utilice el siguiente ARN:

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

Para especificar todas las instancias que pertenecen a una cuenta específica, utilice el carácter comodín (*):

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

Algunas acciones de Billing Conductor, como las empleadas para la creación de recursos, no se pueden llevar a cabo en un recurso específico. En dichos casos, debe utilizar el carácter comodín (*).

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

En muchas acciones de la API de Amazon EC2 se utilizan varios recursos. Por ejemplo, `AttachVolume` asocia un volumen de Amazon EBS a una instancia, por lo que un usuario de IAM debe tener permisos para utilizar el volumen y la instancia. Para especificar varios recursos en una única instrucción, separe los ARN con comas.

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

Para ver una lista de los tipos de recursos de Billing Conductor y sus ARN, consulte los recursos definidos por AWS Billing Conductor en la Guía del usuario de IAM. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por el conductor de AWS facturación.

Claves de condición

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Billing Conductor define su propio conjunto de claves de condición y también admite el uso de algunas claves de condición globales. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Todas las acciones de Amazon EC2 admiten las claves de condición `aws:RequestedRegion` y `ec2:Region`. Para obtener más información, consulte Ejemplo: restricción del acceso a una región específica.

Para ver una lista de las claves de condición de Billing Conductor, consulte las claves de condición de AWS Billing Conductor en la Guía del usuario de IAM. Para saber con qué acciones y recursos

puede utilizar una clave de condición, consulte Acciones definidas por el director AWS de facturación.

Ejemplos

Para ver ejemplos de políticas basadas en identidad de Billing Conductor, consulte AWS Billing Conductor ejemplos de políticas basadas en la identidad.

Políticas basadas en recursos de Billing Conductor

Las políticas basadas en recursos son documentos de política JSON que especifican qué acciones puede realizar una entidad principal especificada en el recurso de Billing Conductor y en qué condiciones. Amazon S3 admite políticas de permisos basadas en recursos para *buckets* de Amazon S3. Las políticas basadas en recursos le permiten otorgar permiso de uso a otras cuentas por recurso. *También puede usar una política basada en recursos para permitir que un AWS servicio acceda a sus buckets de Amazon S3.*

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política basada en recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Si el principal y el recurso están en AWS cuentas diferentes, también debe conceder permiso a la entidad principal para acceder al recurso. Conceda permiso asociando a la entidad una política basada en identidades. Sin embargo, si la política basada en recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

El servicio de Amazon S3 solo admite un tipo de política basada en recursos denominada política de *bucket*, que se adjunta a un *bucket*. Esta política indica las entidades principales (cuentas, usuarios, funciones y los usuarios federados) que pueden realizar acciones en *Billing Conductor*.

Ejemplos

Para ver ejemplos de políticas basadas en los recursos de Billing Conductor, consulte Ejemplos de políticas basadas en recursos de AWS Billing Conductor.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) son listas de beneficiarios que se pueden adjuntar a los recursos. Conceden a las cuentas permisos de acceso al recurso al que están adjuntadas. Puede adjuntar las ACL a un recurso de *bucket* de Amazon S3.

Con las listas de control de acceso (ACL) de Amazon S3, puede administrar el acceso a los recursos del *bucket*. Cada *bucket* incluye una ACL como un subrecurso. Define a qué AWS cuentas, usuarios o grupos de usuarios de IAM o funciones de IAM se les concede acceso y el tipo de acceso. Cuando se recibe una solicitud de un recurso, AWS comprueba la ACL correspondiente para comprobar que el solicitante tiene los permisos de acceso necesarios.

Cuando crea un recurso de *bucket*, Amazon S3 crea una ACL predeterminada que concede al propietario del recurso control total sobre el recurso. En el ejemplo siguiente de ACL de *bucket*, John Doe aparece como el propietario del *bucket* y se le concede el control total de ese *bucket*. Una ACL puede tener hasta 100 beneficiarios.

```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://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>
```

El campo ID de la ACL es el ID de usuario canónico de la AWS cuenta. Para obtener información sobre cómo ver este identificador en una cuenta de tu propiedad, consulta Cómo encontrar un seudónimo canónico de una AWS cuenta.

Autorización basada en etiquetas de Billing Conductor

Puede adjuntar etiquetas a los recursos de Billing Conductor o transferirlas en una solicitud a Billing Conductor. Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `Billing Conductor:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Roles de IAM de Billing Conductor

Un rol de IAM es una entidad de tu AWS cuenta que tiene permisos específicos.

Uso de credenciales temporales con Billing Conductor

Puede utilizar credenciales temporales para iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Para obtener credenciales de seguridad temporales, puede llamar a operaciones de AWS STS API como AssumeRoleo GetFederationToken.

Billing Conductor admite el uso de credenciales temporales.

Roles vinculados al servicio

Los roles vinculados a un servicio permiten a AWS los servicios acceder a los recursos de otros servicios para completar una acción en tu nombre. Los roles vinculados a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Roles de servicio

Esta característica permite que un servicio asuma un rol de servicio en su nombre. Este rol permite que el servicio obtenga acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles de servicio aparecen en su cuenta de IAM y son propiedad de la cuenta. Esto significa que un administrador de IAM puede cambiar los permisos de este rol. Sin embargo, hacerlo podría deteriorar la funcionalidad del servicio.

Billing Conductor admite roles de servicio.

Elección de un rol de IAM en Billing Conductor

Cuando se crea un recurso en Billing Conductor, debe elegir un rol para permitir el acceso de Billing Conductor a Amazon EC2 en su nombre. Si ha creado previamente un rol de servicio o un rol

vinculado a servicios, Billing Conductor le proporciona una lista de roles para elegir. Es importante seleccionar un rol que permita el acceso para iniciar y detener instancias de Amazon EC2.

AWS Billing Conductor ejemplos de políticas basadas en la identidad

De forma predeterminada, los usuarios y los roles de IAM no tienen permiso para crear o modificar los recursos de Billing Conductor. Tampoco pueden realizar tareas con la API AWS Management Console AWS CLI, o AWS . Un administrador de IAM debe crear políticas de IAM que concedan permisos a los usuarios y a los roles para realizar operaciones de la API concretas en los recursos especificados que necesiten. El administrador debe adjuntar esas políticas a los usuarios o grupos de IAM que necesiten esos permisos.

Para obtener información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas JSON de ejemplo, consulte Creación de políticas en la pestaña JSON en la Guía del usuario de IAM.

Temas

- Prácticas recomendadas relativas a políticas
- Ejemplos de políticas basadas en identidades de Billing Conductor

Prácticas recomendadas relativas a políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Billing Conductor de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos en muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos

como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades de Billing Conductor

Este tema contiene políticas de ejemplo que puede adjuntar a un usuario o grupo de IAM para controlar el acceso a la información y herramientas de su cuenta.

Temas

- Concesión de acceso total a la consola de Billing Conductor
- Concesión de acceso total a la API de Billing Conductor
- Concesión de acceso de solo lectura a la consola de Billing Conductor
- Concesión de acceso a Billing Conductor a través de la consola de facturación
- Otorgar a Billing Conductor acceso a través de los informes AWS de costos y uso

- Concesión de acceso a la característica de importación de unidades organizativas a Billing Conductor
- Denegar a Billing y Cost Explorer el acceso a servicios y funciones que no admiten costos pro forma

Concesión de acceso total a la consola de Billing Conductor

Para obtener acceso a la consola de Billing Conductor, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle registrar y consultar los detalles acerca de los recursos de Billing Conductor en su Cuenta de AWS. Si crea una política basada en identidad que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles de IAM) que tengan esa política.

Para garantizar que esas entidades puedan seguir utilizando la consola de Billing Conductor, adjunte también la siguiente política AWS gestionada a las entidades. Para obtener más información, consulte Agregar permisos a un usuario en la Guía del usuario de IAM:

Además de los permisos de `billingconductor:*`, `pricing:DescribeServices` es necesario para crear reglas de precios y `organizations:ListAccounts` para enumerar las cuentas vinculadas que están vinculadas a la cuenta del pagador.

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

```
        }
    ]
}
```

No es necesario conceder permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

Concesión de acceso total a la API de Billing Conductor

En este ejemplo, concede a una entidad de IAM acceso total a la API de Billing Conductor.

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

Concesión de acceso de solo lectura a la consola de Billing Conductor

En este ejemplo, concede a una entidad de IAM acceso de solo lectura a la consola de Billing Conductor.

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

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

Concesión de acceso a Billing Conductor a través de la consola de facturación

En este ejemplo, las entidades de IAM pueden cambiar y ver los datos de facturación proforma en la página de facturas de su consola de facturación.

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

Otorgar a Billing Conductor acceso a través de los informes AWS de costos y uso

En este ejemplo, las entidades de IAM pueden cambiar y ver los datos de facturación proforma a través de la página de informes de costes y uso de su consola de facturación.

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

```
                "cur:DescribeReportDefinitions"
            ],
            "Resource": "*"
        }
    ]
}
```

Concesión de acceso a la característica de importación de unidades organizativas a Billing Conductor

En este ejemplo, las entidades de IAM tienen acceso de solo lectura a las operaciones de AWS Organizations API específicas que se requieren para importar las cuentas de las unidades organizativas (OU) al crear un grupo de facturación. La función de importación de unidades organizativas se encuentra en la consola de AWS Billing Conductor.

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

Denegar a Billing y Cost Explorer el acceso a servicios y funciones que no admiten costos pro forma

En este ejemplo, a las entidades de IAM se les niega el acceso a los servicios y funciones que no soportan los costes proforma. Esta política incluye una lista de las acciones que se pueden realizar en la cuenta de administración y en las cuentas individuales de los miembros.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "aws-portal:ModifyAccount",
```

```
            "aws-portal:ModifyBilling",
            "aws-portal:ModifyPaymentMethods",
            "aws-portal:ViewPaymentMethods",
            "aws-portal:ViewAccount",
            "cur:GetClassic*",
            "cur:Validate*",
            "tax:List*",
            "tax:Get*",
            "tax:Put*",
            "tax:ListTaxRegistrations",
            "tax:BatchPut*",
            "tax:UpdateExemptions",
            "freetier:Get*",
            "payments:Get*",
            "payments:List*",
            "payments:Update*",
            "payments:GetPaymentInstrument",
            "payments:GetPaymentStatus",
            "purchase-orders:ListPurchaseOrders",
            "purchase-orders:ListPurchaseOrderInvoices",
            "consolidatedbilling:GetAccountBillingRole",
            "consolidatedbilling:Get*",
            "consolidatedbilling:List*",
            "invoicing:List*",
            "invoicing:Get*",
            "account:Get*",
            "account:List*",
            "account:CloseAccount",
            "account:DisableRegion",
            "account:EnableRegion",
            "account:GetContactInformation",
            "account:GetAccountInformation",
            "account:PutContactInformation",
            "billing:GetBillingPreferences",
            "billing:GetContractInformation",
            "billing:GetCredits",
            "billing:RedeemCredits",
            "billing:Update*",
            "ce:GetPreferences",
            "ce:UpdatePreferences",
            "ce:GetReservationCoverage",
            "ce:GetReservationPurchaseRecommendation",
            "ce:GetReservationUtilization",
            "ce:GetSavingsPlansCoverage",
```

```
            "ce:GetSavingsPlansPurchaseRecommendation",
            "ce:GetSavingsPlansUtilization",
            "ce:GetSavingsPlansUtilizationDetails",
            "ce:ListSavingsPlansPurchaseRecommendationGeneration",
            "ce:StartSavingsPlansPurchaseRecommendationGeneration",
            "ce:UpdateNotificationSubscription"
        ],
        "Resource": "*"
    }]
}
```

Para obtener más información, consulte Servicios de AWS que respaldan los costos pro forma.

AWS políticas gestionadas para AWS Billing Conductor

Para añadir permisos a usuarios, grupos y roles, es más fácil usar políticas AWS administradas que escribirlas tú mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puedes usar nuestras políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información sobre las políticas AWS administradas, consulte las políticas AWS administradas en la Guía del usuario de IAM.

AWS los servicios mantienen y AWS actualizan las políticas gestionadas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios agregan permisos adicionales a una política administrada por AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política administrada por AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política ReadOnlyAccess AWS gestionada proporciona acceso de solo lectura a todos los AWS servicios y recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

AWS política gestionada: AWSBillingConductorFullAccess

La política AWSBillingConductorFullAccess gestionada otorga acceso completo a la consola y a las API de AWS Billing Conductor. Los usuarios pueden enumerar, crear y eliminar los recursos AWS de Billing Conductor.

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

AWS política gestionada: AWSBillingConductorReadOnlyAccess

La política AWSBillingConductorReadOnlyAccess gestionada otorga acceso de solo lectura a la consola y a las API AWS de Billing Conductor. Los usuarios pueden ver y enumerar todos los recursos de AWS Billing Conductor. Estos usuarios no pueden crear, actualizar ni eliminar recursos.

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

```
}
```

AWS Billing Conductor actualiza las políticas AWS gestionadas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de AWS Billing Conductor desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial de documentos de AWS Billing Conductor.

Cambio	Descripción	Fecha
AWSBillingConductorReadOnlyAccess	Se agregó `GetBillingGroupCostReport` a la `AWSBillingConductorReadOnlyAccess` política.	8 de febrero de 2024
AWSBillingConductorFullAccess	Política creada	29 de marzo de 2022
AWSBillingConductorReadOnlyAccess	Política creada	29 de marzo de 2022
AWS Publicado el registro de cambios de Billing Conductor	AWS Billing Conductor comenzó a rastrear los cambios en sus políticas AWS gestionadas.	29 de marzo de 2022

Ejemplos de políticas basadas en recursos de AWS Billing Conductor

Temas

- Restricción del acceso del bucket Amazon S3 a direcciones IP específicas

Restricción del acceso del bucket Amazon S3 a direcciones IP específicas

En el siguiente ejemplo se conceden permisos a un usuario para que realice operaciones de Amazon S3 en objetos del bucket especificado. Sin embargo, la solicitud debe proceder del rango de direcciones IP especificado en la condición.

La condición en esta instrucción identifica el rango 54.240.143.* de direcciones IP permitidas en formato de Protocolo de Internet versión 4 (IPv4), con una excepción: 54.240.143.188.

El `Condition` bloque utiliza las `NotIpAddress` condiciones `IpAddress` y y la clave de `aws:SourceIp` condición, que es una clave de condición AWS amplia. Para obtener más información acerca de estas claves de condición, consulte Especificación de condiciones en una política. Los valores de IPv4 `aws:sourceIp` utilizan la notación CIDR estándar. Para obtener más información, consulte Operadores de condición de dirección IP en la guía del usuario de 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"}
      }
    }
  ]
}
```

Solución de problemas AWS Billing Conductor de identidad y acceso

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Billing Conductor e IAM.

Temas

- No tengo autorización para realizar una acción en Billing Conductor

- No estoy autorizado a realizar lo siguiente: PassRole
- Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis recursos de Billing Conductor

No tengo autorización para realizar una acción en Billing Conductor

Si AWS Management Console le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener ayuda. Su administrador es la persona que le facilitó su nombre de usuario y contraseña.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM de `mateojackson` intenta utilizar la consola para ver detalles sobre *`Billing Conductor`*, pero no tiene permisos `Billing Conductor:`*`GetWidget`*.

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

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso *`my-example-Billing Conductor`* mediante la acción `Billing Conductor:`*`GetWidget`*.

No estoy autorizado a realizar lo siguiente: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas se deben actualizar para permitirle pasar un rol a Billing Conductor.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Billing Conductor. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis recursos de Billing Conductor

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para obtener información acerca de si Billing Conductor admite estas características, consulte ¿Cómo AWS Billing Conductor funciona con IAM.
- Para obtener información sobre cómo proporcionar acceso a sus recursos a través de los Cuentas de AWS que es propietario, consulte Proporcionar acceso a un usuario de IAM en otro de su Cuenta de AWS propiedad en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Registro y supervisión en AWS Billing Conductor

El monitoreo es una parte importante para mantener la confiabilidad, la disponibilidad y el rendimiento de su AWS cuenta. Hay varias herramientas disponibles para monitorear su uso de AWS Billing Conductor.

AWS Informes de costos y uso

AWS Los informes de costos y AWS uso registran su consumo y proporcionan los cargos estimados asociados a su cuenta. Cada informe contiene partidas para cada combinación única de AWS productos, tipo de uso y operación que utilices en tu AWS cuenta. Puede personalizar los informes de AWS costos y uso para agregar la información por hora o por día.

Para obtener más información sobre los informes de AWS costos y uso, consulte la Guía de informes de costos y uso.

Registrar las llamadas a la AWS Billing Conductor API mediante AWS CloudTrail

AWS Billing Conductor está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en AWS Billing Conductor. CloudTrail captura todas las llamadas a la API de AWS Billing Conductor como eventos. Las llamadas capturadas incluyen llamadas desde la consola de AWS Billing Conductor y llamadas en código a las operaciones de la API de AWS Billing Conductor. Si crea un registro, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de AWS Billing Conductor. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por Billing Conductor CloudTrail, puede determinar la solicitud que se realizó a AWS Billing Conductor, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

AWS Billing Conductor CloudTrail eventos

En esta sección se muestra una lista completa de los CloudTrail eventos relacionados con Billing and Cost Management.

Nombre de evento	Definición
`AssociateAccounts`	Registra la asociación de cuentas a un grupo de facturación.
`Associate PricingRules`	Registra la asociación de las reglas de precios a un plan de precios.

Nombre de evento	Definición
`AutoAssociateAccount`	Registra la asociación automática de una cuenta a un grupo de facturación.
`AutoDisassociateAccount`	Registra la desasociación automática de una cuenta de un grupo de facturación en el siguiente período de facturación.
`BatchAssociateResourcesToCustomLineItem`	Registra la asociación por lotes de recursos a una partida porcentual personalizada.
`BatchDisassociateResourcesFromCustomLineItem`	Registra la disociación por lotes de los recursos de una partida porcentual personalizada.
`CreateBillingGroup`	Registra la creación de un grupo de facturación.
`CreateCustomLineItem`	Registra la creación de una partida personalizada.
`CreatePricingPlan`	Registra la creación de un plan de precios.
`CreatePricingRule`	Registra la creación de una regla de precios.
`DeleteBillingGroup`	Registra la eliminación de un grupo de facturación.
`DeleteCustomLineItem`	Registra la eliminación de una partida personalizada.
`DeletePricingPlan`	Registra la eliminación de un plan de precios.
`DeletePricingRule`	Registra la eliminación de una regla de precios.

Nombre de evento	Definición
`DisassociateAccounts`	Registra la disociación de las cuentas de un grupo de facturación.
`DisassociatePricingRules`	Registra la disociación de las reglas de precios de un plan de precios.
`ListAccountAssociations`	Registra el acceso a los identificadores de cuenta del grupo de facturación.
`ListBillingGroupCostReports`	Registra el acceso a los AWS cargos reales del grupo de facturación.
`ListBillingGroups`	Registra el acceso a los grupos de facturación en un período de facturación.
`ListCustomLineItems`	Registra el acceso a las partidas personalizadas en un período de facturación.
`ListCustomLineItemVersions`	Registra el acceso a las versiones de una partida personalizada.
`ListPricingPlans`	Registra el acceso a los planes de precios en un período de facturación.
`ListPricingPlansAssociatedWithPricingRule`	Registra el acceso a los planes de precios asociados a una regla de precios.
`ListPricingRules`	Registra el acceso a las reglas de precios en un período de facturación.

Nombre de evento	Definición
`ListPricingRulesAssociatedToPricingPlan`	Registra el acceso a las reglas de precios asociadas a un plan de precios.
`ListResourcesAssociatedToCustomLineItem`	Registra el acceso a los recursos asociados a una partida personalizada.
`ListTagsForResource`	Registra el acceso a las etiquetas de un recurso.
`TagResource`	Registra la asociación de etiquetas en un recurso.
`UpdateBillingGroup`	Registra la actualización de un grupo de facturación.
`UpdateCustomLineItem`	Registra la actualización de una línea de pedido personalizada.
`UpdatePricingPlan`	Registra la actualización de un plan de precios.
`UpdatePricingRule`	Registra la actualización de una regla de precios.

AWS La información del conductor de facturación en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en AWS Billing Conductor, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los eventos de AWS Billing Conductor, crea un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de

todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas las acciones AWS de Billing Conductor las registra CloudTrail y se documentan en la Referencia de la API AWS de Billing Conductor.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento CloudTrail UserIdentity.

Descripción de las entradas del archivo AWS de registro de Billing Conductor

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

Temas

- AutoAssociateAccount
- CreateBillingGroup

AutoAssociateAccount

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `AutoAssociateAccount` acción.


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "billingconductor.amazonaws.com"
    },
    "eventTime": "2024-02-23T00:22:08Z",
    "eventSource": "billingconductor.amazonaws.com",
    "eventName": "AutoAssociateAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "billingconductor.amazonaws.com",
    "userAgent": "billingconductor.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "1v14d239-fe63-4d2b-b3cd-450905b6c33",
    "eventID": "14536982-geff-4fe8-bh18-f18jde35218d0",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
        "requestParameters": {
            "Arn": "arn:aws:billingconductor::111122223333:billinggroup/444455556666",
            "AccountIds": [
                "333333333333"
            ]
        },
        "responseElements": {
            "Arn": "arn:aws:billingconductor::111122223333:billinggroup/444455556666"
        }
    },
    "eventCategory": "Management"
}
```


CreateBillingGroup

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `CreateBillingGroup` acción.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId":"111122223333",
        "accessKeyId":"ASIAIOSFODNN7EXAMPLE"
    },
    "eventTime": "2024-01-24T20:30:03Z",
    "eventSource": "billingconductor.amazonaws.com",
    "eventName": "CreateBillingGroup",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "100.100.10.10",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "PrimaryAccountId": "444455556666",
        "ComputationPreference": {
            "PricingPlanArn": "arn:aws:billingconductor::111122223333:pricingplan/
TqeITi5Bgh"
        },
        "X-Amzn-Client-Token": "32aafb5s-e5b6-47f5-9795-3a69935e9da4",
        "AccountGrouping": {
            "LinkedAccountIds": [
                "444455556666",
                "111122223333"
            ]
        },
        "Name": "***"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "Arn": "arn:aws:billingconductor::111122223333:billinggroup/444455556666"
    },
    "requestID": "fb26ae47-3510-a833-98fe-3dc0f602gb49",
    "eventID": "3ab70d86-c63e-46fd8d-a33s-ce2970441a8",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Validación de conformidad para AWS Billing Conductor

Los auditores externos evalúan la seguridad y el cumplimiento de AWS los servicios como parte de varios programas de AWS cumplimiento. AWS Billing Conductor no está incluido en el ámbito de ningún programa de conformidad de AWS.

Para ver una lista de AWS los servicios incluidos en el ámbito de los programas de conformidad específicos, consulte Servicios de AWS incluidos . Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Su responsabilidad de cumplimiento al utilizar AWS Billing Conductor viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Security and Compliance Quick Start Guides (Guías de inicio rápido de seguridad y conformidad) (Guías de inicio rápido de seguridad y conformidad): Estas guías de implementación analizan las consideraciones en materia de arquitectura y proporcionan los pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su sector y ubicación.
- Evaluación de los recursos con las reglas de la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Este AWS servicio proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar su conformidad con los estándares y las mejores prácticas del sector de la seguridad.

La resiliencia en la AWS facturación, Conductor

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor

disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura global.AWS

Seguridad de la infraestructura en AWS Billing Conductor

Como servicio gestionado, AWS Billing Conductor está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a Billing Conductor a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Cuotas y limitaciones

En la siguiente tabla se describen las cuotas y restricciones actuales de AWS.

Cuotas

Número de grupos de facturación por cuenta de pagador	5 000
Número de cuentas por grupo de facturación	1 000
Número de planes de precios	5 000
Número de reglas de precios	50 000
Número de reglas de precios que se pueden asociar a un plan de precios	500
Número de planes de precios que se pueden asociar a una regla de precios	1 000
Número de partidas personalizadas	50 000
Número de valores de origen que se pueden asociar a un porcentaje de partida personali zada	100
Número de porcentajes personalizados que se pueden asociar a una partida fija personalizada	100

Restricciones

No se pueden aumentar otras restricciones de la siguiente tabla.

Número de informes de coste y uso del grupo de facturación por grupo de facturación	10

Nombre del grupo de facturación	• Debe tener un máximo de 128 caracteres • No puede contener un `space` • No puede contener caracteres especiales
La descripción del grupo de facturación	Debe tener un máximo de 1024 caracteres
Nombre del plan de precios	• Debe tener un máximo de 128 caracteres • No puede contener un `space` • No puede contener caracteres especiales
La descripción del plan de precios	Debe tener un máximo de 1024 caracteres
Nombre de partida personalizada	• Debe tener un máximo de 128 caracteres • No puede contener un `space` • No puede contener caracteres especiales

Historial del documento

En la siguiente tabla se describe la documentación de esta versión de AWS Billing Conductor.

Cambio	Descripción	Fecha
Documentación actualizada	Se actualizó la sección ¿Qué es AWS Billing Conductor? tema.	7 de marzo de 2024
Documentación actualizada para las políticas AWS gestionadas	Se agregó `GetBillingGroupCostReport` a la `AWSBillingConductorReadOnlyAccess` política. Consulte las políticas AWS gestionadas para AWS Billing Conductor.	8 de febrero de 2024
Se agregó documentación para el resumen de los márgenes	Puedes ver los detalles de tus márgenes Servicio de AWS por grupo de facturación. Consulta Análisis de los márgenes por grupo de facturación.	14 de diciembre de 2023
Se agregó documentación sobre las líneas de pedido personalizadas	Puedes aplicar una partida personalizada a una cuenta vinculada específica de tu grupo de facturación. Consulte Crear partidas personalizadas por grupo de facturación.	4 de diciembre de 2023
Documentación añadida sobre la cuenta principal	Comprenda cómo la elección de una cuenta principal puede afectar a los costos proforma de sus grupos de facturación. Consulte Comprensión de	26 de octubre de 2023

	la importancia de la fecha de registro de la cuenta principal.	
Soporte añadido para filtros de partidas personalizadas	Ahora puede especificar filtros de partidas para sus partidas personalizadas. Para obtener más información, consulte Creación de una partida personalizada con cargo porcentual.	5 de septiembre de 2023
Se agregó documentación sobre los costos pro forma	Consulte los siguientes temas: • Realizar un análisis ad hoc de los costos pro forma en AWS Cost Explorer • Servicios de AWS que respalden los costos pro forma • Ejemplo de política de IAM: denegar el acceso a los costes pro forma	22 de agosto de 2023
Soporte añadido para la asociación automática de cuentas	Ahora puede habilitar un grupo de facturación para la asociación automática de cuentas. Para obtener más información, consulte Creación de grupos de facturación, configuraciones de precios y partidas personalizadas.	26 de julio de 2023

Soporte añadido para la descarga de CSV	Ahora puede descargar un archivo CSV para la tabla de análisis de márgenes de su grupo de facturación. Para obtener más información, consulte Análisis de los márgenes por grupo de facturación.	6 de junio de 2023
Versión inicial	Publicación inicial de la guía del usuario y la referencia de la API de AWS Billing Conductor.	16 de marzo de 2022

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.