Perfilador de costo de aplicación

Guía del usuario

Perfilador de costo de aplicación: Guía del usuario

Table of Contents

¿Qué es ?AWSPerfilador de costo de aplicación

AWSApplication Cost Profiler le ayuda a separar suAWSfacturación y costes por parte de los inquilinos de su servicio. UNAarrendatariopuede ser un usuario, un grupo de usuarios o un proyecto.

UNArecursoes una entidad con la que los usuarios pueden trabajar enAWS, como una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Asegúrese de que puede identificar el uso de recursos por parte del inquilino que elija.

TípicoAWSel uso de recursos incluye servicios compartidos que admiten varios inquilinos dentro de la organización. Algunos recursos utilizan dimensiones basadas en el tiempo. Para obtener información de costes y facturación por parte del arrendatario en lugar de por uso por hora del recurso, puede integrar sus recursos con Application Cost Profiler. Con este enfoque granular, puedes entender cómoAWSlos recursos se consumen en una solución de software compartida.

Los siguientes recursos que pueden utilizar dimensiones basadas en el tiempo o el uso por hora están habilitados para Application Cost Profiler:

- Instancias de Amazon EC2 (solo instancias bajo demanda y spot)
- Colas de Amazon Simple Queue Service (Amazon SQS)
- Temas de Amazon Simple Notification Service (Amazon SNS)
- Amazon DynamoDB lee y escribe

> **Note**
>
> El uso de Amazon SQS, Amazon SNS y DynamoDB no se cobra por tiempo, a diferencia de la mayoría de los recursos. En su caso, el uso durante una hora (por ejemplo, varias lecturas y escrituras en DynamoDB) se clasifica por el porcentaje de hora que asigna a diferentes inquilinos, independientemente de cuándo se produjeron las lecturas o escrituras durante la hora.

Integra sus servicios con Application Cost Profiler en tres pasos:

1. Habilite y configure un informe— Este paso define el aspecto que desea que tenga su resultado final.
2. Enviar datos de uso de inquilinos a Application Cost Profiler: este paso requiere código del servicio para crear datos de uso que asocien a los inquilinos con el tiempo que utilizan los recursos y, a continuación, envíen esos datos de uso a Application Cost Profiler.
3. Informes: Application Cost Profiler proporciona informes a la cadencia especificada en la configuración de informes. Los informes muestran el coste asociado al uso de cada inquilino, lo que le proporciona una vista detallada de su facturación.

Para obtener más información acerca de estos pasos, consulteIntroducción (p. 2).

Introducción al

AWSEl generador de perfiles de costos de aplicaciones le ayuda a obtener información sobre los costos de susAWS recursos al informar sobre el uso de los recursos por inquilino, en lugar de por el recurso en su conjunto. Un inquilino puede ser un usuario, un grupo de usuarios o un proyecto. Asegúrese de que el inquilino que elija puede identificar el uso de sus recursos. Para obtener informes de costos sobre el uso de los inquilinos, configure un informe y envíe los datos de uso a Application Cost Profiler. En esta sección se describen los requisitos previos que debe cumplir antes de utilizar Application Cost Profiler.

Temas

Registro en una Cuenta de AWS

Si no dispone de una Cuenta de AWS, siga los pasos que figuran a continuación para crear una.

Para registrarse en Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones en línea.

   Parte del procedimiento de inscripción consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Al registrase en una Cuenta de AWS, se crea un Usuario raíz de la cuenta de AWS. El usuario raíz tiene acceso a todos los recursos y Servicios de AWS de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario administrativo y utilice únicamente el usuario raíz para realizar la ejecución tareas que requieren acceso de usuario raíz.

AWS le enviará un email de confirmación luego de completar el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando My Account (Mi cuenta).

Crear un usuario administrativo

Después de registrarse para obtener una Cuenta de AWS, cree un usuario administrativo para que no utilice el usuario raíz en las tareas cotidianas.

Proteger su Usuario raíz de la cuenta de AWS

1. Inicie sesión en AWS Management Console como propietario de cuenta eligiendo Usuario raíz e ingrese el email de su Cuenta de AWS. En la siguiente página, escriba su contraseña.

Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Signing in as the root user (Iniciar sesión como usuario raíz) en la Guía del usuario de AWS Sign-In.

2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario raíz Cuenta de AWS (consola) en la Guía del usuario de IAM.

Crear un usuario administrativo

- Para las tareas administrativas diarias, conceda acceso administrativo a un usuario administrativo en AWS IAM Identity Center (successor to AWS Single Sign-On).

  Para obtener instrucciones, consulte Introducción en la Guía del usuario de AWS IAM Identity Center (successor to AWS Single Sign-On).

Iniciar sesión como usuario administrativo

- Para iniciar sesión con el usuario del Centro de identidades de IAM, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario del Centro de identidades de IAM.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de acceso de AWS en la Guía del usuario de AWS Sign-In.

Conceder acceso programático

Los usuarios necesitan acceso programático si desean interactuar con AWS fuera de la AWS Management Console. La forma de conceder el acceso programático depende del tipo de usuario que acceda a AWS:

Para conceder acceso programático a los usuarios, elija una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	B
Identidad del personal (Usuarios administrados en el IAM Identity Center)	Utilice credenciales a largo plazo para firmar las solicitudes programáticas a la AWS CLI, los SDK de AWS o las API de AWS.	Siga las instrucciones de la interfaz que desea utilizar: • Para elloAWS CLI, consulte Configuración delAWS CLI para su usoAWS IAM Identity Center (successor to AWS Single Sign-On) en la Guía delAWS Command Line Interface usuario. • Para verAWS los SDK, las herramientas y lasAWS API, consulte la autenticación de IAM Identity Center en la Guía de referencia deAWS SDK y herramientas.
IAM	Utilice credenciales a largo plazo para firmar las solicitudes	Siguiendo las instrucciones de Uso de credenciales temporales

¿Qué usuario necesita acceso programático?	Para	B
	programáticas a la AWS CLI, los SDK de AWS o las API de AWS.	con recursos de AWS de la Guía del usuario de IAM.
IAM	(No recomendado) Utilice credenciales a largo plazo para firmar las solicitudes programáticas a las API de AWS CLI o AWS (directamente o mediante los AWS SDK).	Siga las instrucciones de la interfaz que desea utilizar: • Para elloAWS CLI, consulte Autenticación mediante credenciales de usuario de IAM en la Guía delAWS Command Line Interface usuario. • Para verAWS los SDK y las herramientas, consulta Autenticar mediante credenciales a largo plazo en la Guía de referencia deAWS SDK y herramientas. • Consulte AWSAdministración de claves de acceso para usuarios de IAM en la Guía del usuario de IAM.

Application Cost Profiler specific prerequisites

Antes de la aplicación Cost, debe cumplir con los siguientes requisitos previos:

- Habilitar Cost Explorer

  HabilitaAWS Cost Explorer para tuAWS cuenta. La Debe completar la configuración de Cost Explorer antes de que Application Cost Profiler pueda generar sus informes diarios y mensuales.

  Para obtener más información, consulte Habilitar el Cost Explorer en la Guía delAWS Billing and Cost Management usuario.
- Crear cubos de S3

  Cree al menos dos buckets de Simple Storage Service (Amazon S3) Simal Application Cost Profiler utiliza un bucket de S3 para proporcionarle informes. Utiliza el otro bucket de S3 para cargar los datos de uso a Application Cost Profiler. Normalmente, solo necesitas un bucket de S3 para cargar los datos de uso. Sin embargo, es posible que desee tener más de un bucket de S3 para poder mantener el uso de diferentes servicios en cubos de S3 independientes con diferentes permisos, si es necesario por motivos de seguridad. Debe conceder permisos a Application Cost Profiler para estos buckets de S3.

  Para obtener más información acerca de los buckets de Amazon S3 paraConfiguración de buckets de Amazon S3 para Application Cost Profiler (p. 5)
- Habilitar etiquetas

  Para informar del uso por etiqueta, en lugar de por recurso, debe habilitar esas etiquetas en laAWS Billing and Cost Management consola.

  Para obtener más información sobre la activación de las etiquetasAWS generadas, consulte Activación de las etiquetasAWS de asignación de costos generadas en la Guía delAWS Billing and Cost Management usuario. Para obtener más información acerca de las etiquetas definidas por el usuario,

consulte Etiquetas de asignación de costos definidas por el usuario, en la Guía delAWS Billing and Cost Management usuario de.

Pasos siguientes

Después de los requisitos previos, puede:

- Configure su informe y envíe los datos de uso a Application Cost Profiler. Para obtener más información, consulte Crear informe (p. 9).
- Obtenga y analice los informes generados. Para obtener más información, consulte Uso de informes Application Cost Profiler (p. 14).

Configuración de buckets de Amazon S3 para Application Cost Profiler

Para enviar datos de uso y recibir informes deAWSApplication Cost Profiler, debe tener al menos un bucket de Amazon Simple Storage Service (Amazon S3) en suCuenta de AWSpara almacenar datos y un bucket de S3 para recibir sus informes.

> Note
>
> Para usuarios deAWS Organizations, los depósitos de Amazon S3 pueden estar en la cuenta de administración o en cuentas de miembro individuales. Los datos de los buckets de S3 propiedad de la cuenta de administración se pueden utilizar para generar informes para toda la organización. En cuentas de miembro individuales, los datos de los depósitos de S3 solo se pueden utilizar para generar informes para esa cuenta de miembro.

Los buckets de S3 que crea son propiedad de laCuenta de AWSen la que los creas. Los depósitos de S3 se facturan a las tarifas estándar de Amazon S3. Para obtener más información acerca de cómo crear un bucket de Amazon S3, consulteCrear un bucketen laGuía del usuario de Amazon Simple Storage Service.

Para que Application Cost Profiler use los bucket de S3, debe asociar una política a los bucket que otorgue permisos a Application Cost Profiler para leer y/o escribir en él. Si modifica la política después de configurar los informes, puede impedir que Application Cost Profiler pueda leer sus datos de uso o entregar los informes.

En los siguientes temas se muestra cómo configurar los permisos en los depósitos de Amazon S3 después de haberlos creado. Además de la capacidad de leer y escribir objetos, si ha cifrado los depósitos, Application Cost Profiler debe tener acceso alAWS Key Management Service(AWS KMS) para cada cubo.

Temas

Dar acceso a Application Cost Profiler al bucket de entrega de informes S3

El bucket de S3 que configura para Application Cost Profiler para entregar los informes debe tener adjunta una directiva que permita a Application Cost Profiler crear los objetos de informe. Además, el bucket de S3 debe configurarse para habilitar el cifrado.

Note

Al crear su bucket, debe optar por cifrar. Puede optar por cifrar su bucket con claves administradas por Amazon S3 (SSE-S3) o con su propia clave administrada porAWS KMS(SSE-KMS). Si ya ha creado el depósito sin cifrado, debe editar el depósito para agregar cifrado.

Para dar acceso a Application Cost Profiler al bucket de entrega de informes S3

1. Vaya aConsola de Amazon S3e iniciar sesión
2. SelectBucketsen la navegación de la izquierda y, a continuación, elija su bucket de la lista.
3. Elija el iconoPermisospestaña y, a continuación, junto aPolítica de bucket, eligeEditar.
4. En el navegadorPolítica de, inserte la siguiente política de. Reemplazar*<bucket_name>*por el nombre de su bucket de.*<Cuenta de AWS>*con el ID de suCuenta de AWS.

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

En esta política, está asignando el principal servicio Application Cost Profiler (`application-cost-profiler.amazonaws.com`) para entregar informes al bucket especificado. Lo hace en su nombre e incluye un encabezado con suCuenta de AWSy un ARN específico del depósito de entrega de informes. Para asegurarse de que Application Cost Profiler acceda a su depósito solo cuando actúa en su nombre, el`Condition`comprueba esos encabezados.

5. ElegirGuarde los cambiospara guardar tu póliza, adjunta a tu depósito.

Si ha creado su bucket utilizando el cifrado SSE-S3, ya está listo. Si ha utilizado el cifrado SSE-KMS, se necesitan los siguientes pasos para dar acceso a Application Cost Profiler a su bucket.

6. (Opcional) Seleccione elPropiedadespara su bucket y debajo deCifrado predeterminado, seleccione el Nombre de recurso de Amazon (ARN) para suAWS KMSClave. Esta acción muestra elAWS Key Management Serviceconsola y muestra tu llave.
7. (Opcional) Añada la política para dar acceso a Application Cost Profiler alAWS KMSClave. Para obtener instrucciones sobre cómo agregar esta política, consulteAcceso a Application Cost Profiler a depósitos S3 cifrados SSE-KMS (p. 8).

Dar acceso a Application Cost Profiler a los datos de uso del bucket S3

El bucket de S3 que configura para que Application Cost Profiler lea los datos de uso debe tener una directiva asociada para permitir que Application Cost Profiler lea los objetos de datos de uso.

> Note
>
> Al otorgar a Application Cost Profiler acceso a sus datos de uso, acepta que podamos copiar temporalmente dichos objetos de datos de uso en EE. UU. Este (N. Virginia)Región de AWSmientras se procesan los informes. Estos objetos de datos se conservarán en la región US East (N. Virginia) hasta que se complete la generación mensual de informes.

Para dar acceso a Application Cost Profiler a los datos de uso del bucket S3

1. Vaya aConsola de Amazon S3e iniciar sesión
2. SelectBucketsen la navegación de la izquierda y, a continuación, elija su bucket de la lista.
3. Elija el iconoPermisospestaña y, a continuación, junto aPolítica de bucket, eligeEditar.
4. En el navegadorPolítica de, inserte la siguiente política de. Reemplazar*<bucket-name>*por el nombre de su bucket de.*<Cuenta de AWS>*con el ID de suCuenta de AWS.

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

   En esta política, está asignando el principal servicio Application Cost Profiler (`application-cost-profiler.amazonaws.com`) para obtener datos del bucket especificado. Lo hace en su nombre e incluye un encabezado con suCuenta de AWSy un ARN específico de su depósito de uso. Para asegurarse de que Application Cost Profiler acceda a su depósito solo cuando actúa en su nombre, el`Condition`comprueba esos encabezados.
5. ElegirGuarde los cambiospara guardar tu póliza, adjunta a tu depósito.

Si tu depósito está encriptado conAWS KMSclaves administradas y, a continuación, debe dar acceso a Application Cost Profiler a su bucket siguiendo el procedimiento de la siguiente sección.

Acceso a Application Cost Profiler a depósitos S3 cifrados SSE-KMS

Si cifra los buckets de S3 que configura para Application Cost Profiler (necesario para los depósitos de informes) con claves almacenadas enAWS KMS(SSE-KMS), también debe otorgar permisos a Application Cost Profiler para descifrarlos. Esto lo hace dando acceso a laAWS KMSclaves utilizadas para cifrar los datos.

> **Note**
>
> Si el bucket está cifrado con claves administradas de Amazon S3, no es necesario que complete este procedimiento.

Para dar acceso a Application Cost Profiler aAWS KMSpara bucket de S3 cifrados por SSE-KMS

1. Vaya aAWS KMSconsolae iniciar sesión
2. SelectClaves administradas por el clienteen la navegación de la izquierda y, a continuación, elija la clave que se utiliza para cifrar el bucket de la lista.
3. SelectCambiar a la vista de políticasy, a continuación, elijaEditar.
4. En el navegadorPolítica de, inserte la siguiente instrucción de política.

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

5. ElegirGuarde los cambiospara guardar tu póliza, adjunta a tu clave.
6. Repita el procedimiento para cada clave que cifra un bucket de S3 al que necesita acceder Application Cost Profiler.

> **Note**
>
> Los datos se copian del bucket de S3 al importarlos a los depósitos administrados de Application Cost Profiler (que están cifrados). Si revoca el acceso a las claves, Application Cost Profiler no puede recuperar ningún objeto nuevo del depósito. Sin embargo, los datos ya importados se pueden utilizar para generar informes.

Crear informe

Tras cumplir los requisitos previos, estará listo para configurar el informe para ustedCuenta de AWS y enviar sus datos de uso aAWS Application Cost Profiler. En esta sección, se describe cómo configurar el informe y cómo enviar los datos de uso en Application Cost Cost Cost Profiler costo de uso.

Configure el informe de costo de costo de costo de costo de costo de

El siguiente procedimiento muestra cómo configurar el informe que desea generar en función de la fecha de uso. Configura detalles como la frecuencia con la que se genera el informe.

> Note
>
> SiCuenta de AWS forma parte de unaAWS organización, puede configurar el informe mediante la cuenta de administración o una cuenta de miembro individual. Los informes configurados para cuentas individuales solo contienen datos de esa cuenta. Los informes configurados mediante la cuenta de administración pueden incluir datos de toda la organización.
> El bucket de Amazon S3 utilizado para la producción de informes debe pertenecer a la cuenta que crea la configuración del informe.

Para configurar su informe de Application Cost Profiler

1. Abra un navegador web e inicie sesión en la consola de Application Cost Profiler.
2. Elija Comenzar ahora para configurar o modificar un informe.
3. Introduzca un nombre y una descripción para el informe.
4. Introduzca el nombre de su bucket de S3 en el campo Introduzca el nombre del bucket de S3 e introduzca el prefijo S3 en el campo Introduzca el prefijo de S3. Para obtener más información sobre la creación de buckets de S3 y la concesión de permisos a Application Cost Profiler, consulteConfiguración de buckets de Amazon S3 para Application Cost Profiler (p. 5).
5. Selecciona las opciones que quieres que tenga tu informe:
   - Frecuencia horaria: elija si el informe se genera en una cadencia diaria o mensual, o ambas.
   - Formato de salida del informe: elija el tipo de archivo que desea crear en su bucket de Amazon S3. Si elige CSV, Application Cost Profiler crea un archivo de texto de valores separados por comas con compresión gzip para los informes. Si elige Parquet, se generará un archivo Parquet para los informes.
6. Elija Configurar para guardar la configuración del informe.

> Note
>
> También puede utilizar la APIAWS Application Cost Profiler para configurar los informes.

Compruebe la configuración del informe seleccionando Comenzar ahora para ver la configuración actual del informe.

Note

Solo puede configurar un único informe. Al volver a la página de configuración, se editará el informe existente.

Después de configurar el informe, se habilita la ingesta de datos. Puede integrar sus servicios con Application Cost Profiler para proporcionar datos de uso de sus recursos.

Reportar los datos de uso de los inquilinos desde sus servicios

Una vez que haya configurado el informe, estará listo para enviar los datos de uso de los inquilinos desde los recursos o servicios de su cuenta. Debe informar a Application Cost Profiler cuando su recurso se utilice para un inquilino específico. Por ejemplo, si tu servicio acepta llamadas a la API de diferentes inquilinos, registras una hora de inicio y finalización para cada inquilino al iniciar y finalizar una llamada a la API de ese inquilino. Application Cost Profiler utiliza esos datos para generar informes sobre el costo de su servicio, según la cantidad de tiempo dedicado al trabajo de cada inquilino.

Para proporcionar los datos de uso, haga lo siguiente:

- Prepare los datos de uso de los recursos: cree tablas que describan cuándo se usa un recurso para un inquilino específico.
- Cargar datos de uso: suba las tablas a un bucket de Amazon S3 al que haya autorizado el acceso a Application Cost Profiler.
- Importar datos de uso: llame a la operación de`ImportApplicationUsage` API para que Application Cost Profiler sepa que los datos están listos para procesarse.

En las siguientes secciones se describen cada uno de estos pasos de manera más detallada.

Temas

Paso 1: Preparar los datos de uso de los recursos

A medida que se utiliza un recurso en su servicio, realiza un seguimiento del inquilino que lo está utilizando. Registre estos datos en una tabla que pueda cargar posteriormente para que Application Cost Profiler los importe. Cada fila de la tabla describe un recurso, el arrendatario que lo usa y las horas de inicio y finalización de ese uso. Un ejemplo de recurso es una instancia de Amazon Elastic Compute Cloud (Amazon EC2) que se está utilizando.

Este paso requiere que integre el código en su servicio para generar la información correcta sobre el uso.

Los campos que se encuentran en una tabla de uso de recursos se indican en la siguiente tabla.

Campo	Descripción
ApplicationId	Identifica la aplicación o el producto del sistema que se está utilizando. Define el alcance de los metadatos del inquilino.

Campo	Descripción
TenantId	Un identificador del sistema para el inquilino que consume el recurso especificado. El generador de perfiles de costos de aplicaciones se agrega a este nivel dentro del ApplicationId.
TenantDesc	(Opcional) Datos adicionales sobre el inquilino para sus propios informes adicionales.
UsageAccountId	La cuenta en la que se ejecuta el recurso (importante para las cuentas que forman parte de una organización).
StartTime	Marca de tiempo (en milisegundos y microsegundos) de Epoch, en UTC. Indica la hora de inicio del período de uso por parte del inquilino especificado.
EndTime	Marca de tiempo (en milisegundos y microsegundos) de Epoch, en UTC. Indica la hora de finalización del período de uso por parte del inquilino especificado.
ResourceId	Nombre de recurso de Amazon (ARN) del recurso que se está utilizando.
Nombre	(Opcional) Como alternativa a especificar una ResourceId, puede especificar una etiqueta de recurso Name para atribuir los costos a un conjunto de recursos (el campo debe incluir el valor que desea utilizar para la etiqueta de nombre). Las etiquetas de recursos se habilitan como parte del informe de uso y costo de uso. Para obtener más información sobre las etiquetas de recursos, consulte los detalles de las etiquetas de recursos en la Guía del usuario de los informes de costes y uso.

El resultado debe estar en un archivo de valores separados por comas (.csv) que incluya una fila de encabezado, como se muestra en el siguiente ejemplo.

```
ApplicationId,TenantId,TenantDesc,UsageAccountId,StartTime,EndTime,ResourceId
MyApp,Tenant1,,123456789012,1613681437032.9001,1613681437041.5312,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant2,,123456789012,1613681245531.4426,1613681245551.1323,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant1,,123456789012,1613681904815.3381,1613681904930.0972,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant2,,123456789012,1613681904765.1956,1613681904946.574,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
```

Guarda los datos como un archivo, con la extensión.csv (o .csv.gzip si está comprimido con gzip). Al cargar estos datos en Application Cost Profiler, cada intervalo de tiempo se asigna al inquilino asociado. En este ejemplo, el informe incluye el intervalo de tiempo del coste de la instancia de Amazon EC2 para ese inquilino. Solo para las instancias de Amazon EC2, los segmentos que no están asociados a un inquilino específico se agregan a un inquilino no atribuido. Los intervalos de tiempo superpuestos se cuentan varias veces. Es tu responsabilidad asegurarte de que los datos de tu tabla de uso sean precisos.

> **Note**
>
> Su archivo debe representar una hora de tiempo. Si un recurso se utiliza durante varias horas, finalice el uso esa hora y cree un registro nuevo en el siguiente archivo que comience a la misma hora.
> Debe enviar un único archivo que contenga los datos de toda una hora. Si se envían varios archivos para los datos de la misma hora, Application Cost Profiler solo tendrá en cuenta los datos del último archivo.

Por ejemplo, la siguiente tabla muestra cómo Application Cost Profiler calcula el uso de tres inquilinos durante una hora (3 600 000 milisegundos), en función de los intervalos de tiempo proporcionados.

Inquilino	Intervalos de tiempo proporcionados	Porcentaje calculado del costo por hora
Inquilino 1	1.200.000 ms	33,34%
Inquilino 2	600.000 ms	16,66%
<unattributed>		50,00%

En este ejemplo, al inquilino 1 se le asigna un tercio de la hora y al inquilino 2 se le asigna una sexta parte de la hora. La media hora restante (1.800.000 ms) no se atribuye a ninguno de los clientes, lo que representa el 50% de la hora.

Actualmente, los siguientes recursos están habilitados para Application Cost Profiler:

- Instancias de Amazon EC2 (solo instancias puntuales y bajo demanda)
- Funciones lambda (si envía datos para una función Lambda, debe enviar el ARN del recurso no calificado como`ResourceId`.)
- Instancias de Amazon Elastic Container Service (Amazon ECS)
- Colas de Amazon Simple Queue Service (Amazon SQS)
- Temas de Amazon Simple Notification Service (Amazon SNS)
- Amazon DynamoDB lee y escribe

> **Note**
>
> El uso de Amazon SQS, Amazon SNS y DynamoDB no se cobra por tiempo, a diferencia de la mayoría de los recursos. En su caso, el uso durante una hora (por ejemplo, el número de lecturas y escrituras en DynamoDB) se clasifica según el porcentaje de la hora que se asigna a los distintos inquilinos, independientemente de cuándo se hayan producido las lecturas o escrituras durante la hora.

Paso 2: Subir el uso de tus recursos

Cuando tenga un archivo de uso por inquilino, cargue el archivo de datos en Amazon S3 y asegúrese de que Application Cost Profiler tenga permiso para acceder a él.

Para obtener más información acerca de cómo crear un bucket de S3, consulteApplication Cost Profiler specific prerequisites (p. 4).

Debe asegurarse de que Application Cost Profiler tenga acceso a su bucket de S3. Esto solo debe hacerse una vez por depósito de S3 (puede reutilizar el mismo depósito para cargar varios archivos de uso). Para obtener información sobre cómo dar acceso al bucket, consulteDar acceso a Application Cost Profiler a los

datos de uso del bucket S3 (p. 7). Si el bucket está cifrado, consulteAcceso a Application Cost Profiler a depósitos S3 cifrados SSE-KMS (p. 8).

> Note
>
> No es necesario cifrar los buckets de S3 que utiliza para los datos de uso.

Sube tus datos al bucket de S3 como un archivo, con la extensión.csv (o .csv.gzip si está comprimido con gzip), a intervalos de una hora. Después de cargar un archivo nuevo, debe informar a Application Cost Profiler de que lo ha subido para poder importarlo a su informe.

> Note
>
> Al permitir que Application Cost Profiler acceda a sus datos de uso, usted acepta que podamos copiar temporalmente dichos objetos de datos de uso en el este de EE. UU. (Virginia del Norte)Región de AWS mientras procesamos los informes. Estos objetos de datos se mantendrán en la región Este de EE. UU. (Norte de Virginia) hasta que se complete la generación del informe mensual.

Paso 3: Importación de datos de uso a Application Cost Profiler

Tras subir los datos de uso a un bucket de Amazon S3 al que tenga acceso Application Cost Profiler, informe a Application Cost Profiler de que los datos existen e importarlos a su informe final. Para ello, utilice la`ImportApplicationUsage` operación de la API Application Cost Profiler.

Para obtener información sobre la API del generador de perfiles de costos de laAWS aplicación, incluida la`ImportApplicationUsage` operación, consulte la referencia de la API del generador de perfiles de costos de laAWS aplicación.

En el siguiente ejemplo se muestra cómo realizar una llamada`ImportApplicationUsage`. Sustituya el *`texto de entrada entre corchetes`* por los valores del bucket de S3 y del objeto cargado.

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

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

> Note
>
> El`region` parámetro solo es obligatorio si el bucket se encuentra en una opciónRegión de AWS que está deshabilitada de forma predeterminada. Para obtener más información, consulte Administración de Regiones de AWS en la Referencia general de AWS.

Application Cost Profiler genera un nuevo informe con la frecuencia que solicitó al configurar el informe (p. 9), utilizando los datos con los que lo importó`ImportApplicationUsage`.

Después de configurar el informe y de importar automáticamente los datos de uso a Application Cost Profiler, estará listo para ver los informes generados. Para obtener más información acerca de los informes, consulteUso de informes Application Cost Profiler (p. 14).

Uso de informes Application Cost Profiler

Después de integrar los datos de uso conAWSApplication Cost Profiler y envía los datos por hora, Application Cost Profiler genera automáticamente su informe.

Los informes se generan diariamente o mensualmente, según la opción que seleccionó cuandoconfigurar el informe (p. 9). Los informes se entregan al bucket de Amazon Simple Storage Service (Amazon S3) que seleccionó al configurar el informe.

Los informes diarios generados el primer día del mes tienen los datos del mes anterior.

Datos disponibles en un informe del generador de perfiles de costes de aplicaciones

Las columnas que se crean en un informe de uso se muestran en la siguiente tabla.

Nombre de la columna	Descripción
PayerAccountId	El ID de cuenta de administración de una organización o el ID de cuenta si la cuenta no forma parte deAWS Organizations.
UsageAccountId	El ID de cuenta de la cuenta con uso.
LineItemType	Tipo de registro. Siempre `Usage`.
Hora de inicio de uso	Marca de hora (en milisegundos) de Epoch, en UTC. Indica la hora de inicio del período de uso por el arrendatario especificado.
Hora de finalización de uso	Marca de hora (en milisegundos) de Epoch, en UTC. Indica la hora de finalización del período de uso por el arrendatario especificado.
Identificador de aplicación	LaApplicationIdespecificados en los datos de uso enviados a Application Cost Profiler.
Identificador de tenant	LaID de inquilinoespecificados en los datos de uso enviados a Application Cost Profiler. Los datos sin registro en los datos de uso se recopilan en`unattributed`.
Descripción del inquilino	La`TenantDesc`especificados en los datos de uso enviados a Application Cost Profiler.
ProductCode	LaAWSproducto facturado (por ejemplo,`AmazonEC2`).

Nombre de la columna	Descripción
UsageType	El tipo de uso que se factura (por ejemplo,`BoxUsage:c5.large`).
Operación	La operación que se está facturando (por ejemplo,`RunInstances`).
ResourceId	El ID de recurso o el nombre de recurso de Amazon (ARN) para el recurso que se está facturando.
Factor de escala	Si un recurso está sobreasignado durante una hora, por ejemplo, los datos de uso notificados equivalen a 2 horas en lugar de 1 hora, se aplica un factor de escala para que el total sea igual al importe facturado real (en este caso, 0,5). En esta columna se informa del factor de escala utilizado para el recurso específico durante esa hora. El factor de escala es siempre mayor que cero (0) e menor o igual que 1.
porcentaje de atribución de inquilinos	Porcentaje del uso atribuido al arrendatario especificado (entre cero (0) y 1).
UsageAmount	Cantidad de uso atribuida al arrendatario especificado.
CurrencyCode	La moneda en la que se encuentran el tipo y el costo (por ejemplo,`USD`).
Tasa	La tarifa de facturación del uso, por unidad.
Costo del inquilino	El coste total de ese recurso para el arrendatario especificado.
Región	LaAWSRegión del recurso.
Nombre	Si ha creado etiquetas de recursos para los recursos en el informe Costo y uso, o mediante los datos de uso de recursos, elNombreLa etiqueta se muestra aquí. Para obtener más información acerca de las etiquetas de recursos, consulteDetalles de las etiquetas de recursosen laGuía del usuario del informe de costo y uso.

A continuación se muestra un ejemplo del informe de salida para un recurso durante dos horas.

```
PayerAccountId,UsageAccountId,LineItemType,UsageStartTime,UsageEndTime,ApplicationIdentifier,TenantIden
123456789012,123456789012,Usage,2021-02-01T00:00:00.000Z,2021-02-01T00:30:00.000Z,Canary,unattributed,,
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T00:30:00.000Z,2021-02-01T01:00:00.000Z,Canary,Tenant1,exampl
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant4,exampl
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant3,exampl
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant2,exampl
east-1,test-tag
```

```
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant1,exampl
east-1,test-tag
```

En este ejemplo, la primera hora se asigna a`Tenant1`durante la mitad del tiempo. Queda media hora como`unattributed`. En la segunda hora, a cuatro inquilinos se les asigna la hora completa. En este caso, el factor de escala los reduce todos en 0,25, y a todos se les asigna un cuarto de hora. Puedes ver el coste final en el`TenantCost`column.

AWSCuotas y puntos finales de Application Cost Profiler

La cuenta de AWS tiene cuotas predeterminadas para cada servicio de AWS (estas cuotas anteriormente se denominaban "límites"). A menos que se indique otra cosa, cada cuota esAWSEspecífico de la región. Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

En las siguientes tablas, se indican las cuotas de servicio por cuenta y elAWSPuntos finales de región para Application Cost Profiler.

Service Quotas

Recurso	Valor predeterminado	Descripción
Tasa de`PutReportDefinition`requests	5	El número máximo de`PutReportDefinition`solicitudes por segundo por cuenta.
Tasa de`UpdateReportDefinition`requests	5	El número máximo de`UpdateReportDefinition`solicitudes por segundo por cuenta.
Tasa de`GetReportDefinition`requests	5	El número máximo de`GetReportDefinition`solicitudes por segundo por cuenta.
Tasa de`DeleteReportDefinition`requests	5	El número máximo de`DeleteReportDefinition`solicitudes por segundo por cuenta.
Tasa de`ListReportDefinitions`requests	5	El número máximo de`ListReportDefinitions`solicitudes por segundo por cuenta.
Tasa de`ImportApplicationUsage`requests	5	El número máximo de`ImportApplicationUsage`solicitudes por segundo por cuenta.
Tamaño máximo del archivo de datos de uso	10 MB	Tamaño máximo de un archivo de datos de uso por hora.

Service endpoints

Application Cost Profiler es un servicio global. Todas las llamadas a la API deben realizarse al extremo EE. UU. Este (Norte de Virginia).

- EE.UU. Este (Norte de Virginia) – `application-cost-profiler.us-east-1.amazonaws.com`

Seguridad enAWSPerfilador de costo de aplicación

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos que se han diseñado para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre 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 los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWSProgramas de conformidad de . Para obtener más información acerca de los programas de conformidad que se aplican a Application Cost Profiler, consulteServicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el servicio de AWS que utilice. 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 lo ayuda a comprender cómo puede aplicar el modelo de responsabilidad compartida cuando se utilizaAWSPerfilador de costo de aplicación. Muestra cómo configurar Application Cost Profiler para satisfacer sus objetivos de seguridad y conformidad. También puedes aprender a utilizar otrosAWSque le ayudan a supervisar y proteger los recursos de Application Cost Profiler de.

Contenido

Protección de datos enAWS Application Cost Profiler

El modelo de responsabilidadAWS compartida modelo se aplica a la protección de datos enAWS Application Cost Profiler. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Este contenido incluye la configuración de seguridad y las tareas de administración para el que utiliza Servicios de AWS. 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 AWSShared Responsibility Model and GDPR en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center (successor to AWS Single Sign-On) o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir con sus obligaciones laborales. También recomendamos proteger sus datos de las siguientes formas:

- Utilice la autenticación multifactor (MFA) con cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. Nosotros exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad del usuario con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de 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 FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de conexión de 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 ingresar 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 Applicliclication licliclication liclication liclication Cost Profiler u otros aServicios de AWS través de la consola, la APIAWS CLI, la oAWS los SDK de. Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se pueden 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.

Cifrado en reposo

AWSApplication Cost Profiler siempre cifra todos los datos almacenados en el servicio en reposo sin requerir ninguna configuración adicional. Este cifrado es automático cuando se utiliza Application Cost Profiler.

Para los cubos de Amazon S3 que proporcione, debe cifrar el depósito de informes y puede cifrar el depósito de datos de uso y dar acceso a Application Cost Profiler. Para obtener más información, consulte Configuración de buckets de Amazon S3 para Application Cost Profiler (p. 5).

Cifrado en tránsito

AWSApplication Cost Profiler utiliza la seguridad de la capa de transporte (TLS) y el cifrado del lado del cliente para el cifrado en tránsito. La comunicación con Application Cost Profiler siempre se realiza a través de HTTPS, por lo que sus datos siempre se cifran en tránsito. Este cifrado se configura de forma predeterminada cuando se utiliza Application Cost Profiler.

Administración de identidades y accesos paraAWS Application CoProService Profiler Service

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Application Cost Profiler. IAM es un Servicio de AWS que se puede utilizar sin cargo adicional.

Temas

Público

La forma en que utiliceAWS Identity and Access Management (IAM) difiere en función del trabajo que realice en Application CoProService Profiler Service.

Usuario de servicio: si utiliza el servicio Application CoProer Service para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. Es posible que a medida que utilice más características de Application CoProer Service, necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos a su administrador. Si no puede acceder a una característica de Application CoProer Service, consulteSolución de problemas de identidad y acceso aAWS Application Cost Profiler (p. 29).

Administrador de servicio: si está a cargo de los recursos de Application Cost Profiler Service. Su trabajo consiste en determinar a qué características y recursos de Application CoProService. 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 Application CoProService Profiler Service, consulteCómo funcionaAWS Application Cost Profiler con IAM (p. 24).

Administrador de IAM: si es un administrador de IAM, es posible que desee obtener información sobre cómo escribir políticas para administrar el acceso a Application CoProService Service. Para consultar ejemplos de políticas basadas en identidades de Application CoProService, consulteAWSEjemplos de políticas basadas en identidades de Application CoProService Profiler Service (p. 26).

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe estar autenticado (haber iniciado sesión en AWS) como el Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Puede iniciar sesión en AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center (successor to AWS Single Sign-On) Los usuarios (IAM Identity Center), 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 identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accede a AWS mediante la federación, está asumiendo un rol de forma indirecta.

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

Si accede a 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 usa las herramientas de AWS, debe firmar usted mismo las solicitudes. Para obtener más información sobre cómo utilizar el método recomendado para firmar las solicitudes usted mismo, consulte Proceso de firma de Signature Version 4 en Referencia general de AWS.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de 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 (successor to AWS Single Sign-On) y Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Usuario raíz de Cuenta de AWS

Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos y Servicios de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con el email y la contraseña que utilizó para crear la cuenta. Recomendamos que no utilice el usuario raíz para las tareas cotidianas. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que este pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tasks that require root user credentials (Tareas que requieren credenciales de usuario raíz) en la Guía de referencia de AWS Account Management.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad de la Cuenta de AWS que dispone de 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 obtener 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 obtener más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

IAM roles

Un rol de IAM es una identidad de la Cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un rol de IAM en la AWS Management Consolecambiando de roles. Puede asumir un rol llamando a una operación de la AWS CLI o de la API de AWS, o utilizando una URL personalizada. Para obtener más información acerca de 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 permisos para este. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos que están definidos en este. 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 el Centro de identidades de IAM, debe configurar un conjunto de permisos. El Centro de identidades de IAM 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 IAM Identity Center (successor to 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. No obstante, con algunos Servicios de AWS se puede adjuntar una política directamente a un recurso (en lugar de utilizar un rol como representante). 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 características de 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 a servicios.
  - Permisos principales: cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se lo considera una entidad principal. Las políticas conceden permisos a una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. En este caso, debe tener permisos para realizar ambas acciones. Para ver si una acción requiere acciones dependientes adicionales en una política, consulte Acciones, recursos y claves de condición para losAWS servicios en la Referencia de autorizaciones de servicio.
  - 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.
  - Rol vinculado a servicio: un rol vinculado a servicio es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la 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 utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia de EC2 y realizan solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia adjuntado 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 obtener 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

Para controlar el acceso en AWS, se crean políticas y se asocian a identidades o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal (sesión de rol, usuario o usuario raíz) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. Las mayoría de las políticas se almacenan en 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 utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede agregar las políticas de IAM a los 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 dicha política puede obtener información del usuario de la AWS Management Console, la AWS CLI o la API de AWS.

Políticas basadas en identidad

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y bajo 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 identidad 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. Las políticas administradas incluyen las políticas administradas por AWS y las políticas administradas por el cliente. Para obtener más información acerca de 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 adjuntan 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 adjunta 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 basada en recursos. Las entidades 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 se puede utilizar políticas de IAM administradas por AWS 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 política JSON.

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL. 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 otros tipos de políticas adicionales menos frecuentes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le otorgan.

- 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 identidad. Los permisos resultantes son la intersección de las políticas basadas en 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 servicio (SCP): las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa en AWS Organizations. AWS Organizations

es un servicio que le permite agrupar y administrar de manera centralizada varias Cuentas de AWS que posea su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada 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 identidad del rol y las políticas de la sesión. Los permisos también pueden proceder de una política basada en recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener 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 obtener información acerca de cómo AWS decide si permitir o no una solicitud cuando hay varios tipos de políticas implicados, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funcionaAWS Application Cost Profiler con IAM

Antes de utilizar IAM para administrar el acceso a Application CoProService, debe entender qué características de IAM están disponibles para su uso con Application CoProService Service. Para obtener una perspectiva general sobre cómo Application CoProService Profiler Service, consulte AWSServicios de que funcionan con IAM en la Guía del usuario de IAM.AWS

Temas

Políticas basadas en identidades de Application CoProService Profiler Service

Con las políticas basadas en identidades de IAM, puede especificar las acciones y recursos permitidos o denegados, además de las condiciones en las que se permiten o deniegan las acciones. Application Cost Profiler admite acciones específicas. 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 utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS 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 Application CoProService Profiler Service, utilizan el siguiente prefijo antes de la acción:`application-cost-profiler:`. Por ejemplo, para conceder a alguien permiso para ver los detalles de la definición del informe de CoProService Profiler Service, incluya la`application-cost-profiler:GetReportDefinition` acción en su política. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. Application CoProer Service 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": [
      "application-cost-profiler:ListReportDefinitions",
      "application-cost-profiler:GetReportDefinition"
```

Las siguientes son las acciones disponibles en Application Cost Profiler. Cada una de ellas permite la acción de la API del mismo nombre. Para obtener más información sobre la API de Application Cost Profiler, consulte AWSla referencia de la API de Application Cost Profiler.

- `application-cost-profiler:ListReportDefinitions`— Permite incluir la definición del informe de suAWS cuenta, si la hubiera.
- `application-cost-profiler:GetReportDefinition`— Permite obtener los detalles de la definición del informe de Application Cost Profiler.
- `application-cost-profiler:PutReportDefinition`— Permite crear una nueva definición de informe.
- `application-cost-profiler:UpdateReportDefinition`— Permite actualizar la definición de un informe.
- `application-cost-profiler:DeleteReportDefinition`— Permite eliminar un informe (solo disponible a través de la API Application Cost Profiler).
- `application-cost-profiler:ImportApplicationUsage`— Permite solicitar a Application Cost Profiler la importación de datos de uso de un bucket de Amazon S3 específico.

Recursos

Application Cost Profiler no admite la especificación de nombres de recursos de Amazon (ARN) de recursos en una política.

Claves de condición

Application CoProer Service no proporciona ninguna clave de condición específica del servicio, pero sí admite el uso de algunas claves de condición globales. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Ejemplos

Para ver ejemplos de políticas basadas en identidades de Application CoProService Profiler Service, consulteAWSEjemplos de políticas basadas en identidades de Application CoProService Profiler Service (p. 26).

Políticas basadas en recursos de Application CoProService Profiler Service

Application CoProer Service no soporta políticas basadas en recursos.

Autorización basada en etiquetas del CoProService Service Profiler Service

Application CoProer Service no soporta el etiquetado de recursos ni el control de acceso basado en etiquetas.

Funciones de IAM de Application CoProService Profiler Service

Un rol de IAM es una entidad de la cuenta de AWS que dispone de permisos específicos.

Uso de credenciales temporales con Application CoProer Service

Puede utilizar credenciales temporales para iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Las credenciales de seguridad temporales se obtienen mediante una llamada a operaciones de laAWS STS API tales como AssumeRoleo GetFederationToken.

Application CoProer Profiler Service

Roles vinculados a servicios

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

Application CoProer Service no es compatible con 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 puede cambiar los permisos de este rol. Sin embargo, hacerlo podría deteriorar la funcionalidad del servicio.

Application Cost Profiler no admite funciones de servicio.

AWSEjemplos de políticas basadas en identidades de Application CoProService Profiler Service

De forma predeterminada, los usuarios y roles de IAM no tienen permisos para crear, ver ni modificar recursos deAWS Application CoProProer Service. Tampoco pueden realizar tareas mediante la APIAWS Management Console,AWS Command Line Interface (AWS CLI) o laAWS API. Un administrador debe crear políticas de IAM que concedan permisos a los usuarios y a los roles para realizar las operaciones de API concretas 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

- Permitir a los usuarios consultar sus propios permisos (p. 28)
- Acceso a un bucket de Amazon S3 (p. 29)

Prácticas recomendadas relativas a políticas

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

- Comience con las políticas administradas por AWS y continúe con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de trabajo, utilice las políticas administradas por AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en la Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para sus casos de uso a fin de reducir aún más los permisos. 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 de usuario de IAM.
- Use 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 política para especificar que todas las solicitudes deben enviarse utilizando SSL. También puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado, como por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política JSON de IAM: condición en la Guía del usuario de IAM.
- Use 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. IAM Access Analyzer proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para obtener más información, consulte la política de validación del Analizador de acceso de IAM en la Guía de usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de MFA a sus políticas. Para obtener más información, consulte Configuración de acceso a una API protegida 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 de usuario de IAM.

Uso de la consola de CoProService Service

Para acceder a laAWS consola de CoProService Service Profiler Service, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle mostrar y consultar los detalles sobre los detalles sobre los detalles sobre los detalles sobre los recursos de Application CoProer Service Profiler Service en laAWS cuenta. 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 utilizar la consola de Application Cost Profiler para ver la definición del informe de Application Cost Profiler de suAWS cuenta, adjunte los siguientes permisos a las entidades.

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

Por ejemplo, podría crear la siguiente política para los usuarios de solo lectura.

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

Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM.

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

Permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se adjuntan a la identidad de sus usuarios. Esta política incluye permisos para llevar a cabo esta acción en la consola o mediante programación con la AWS CLI o la API de AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

Acceso a un bucket de Amazon S3

En este ejemplo, desea conceder acceso a un usuario de IAM de suAWS cuenta de a uno de sus bucket de Amazon S3`examplebucket`. También desea permitir al usuario añadir, actualizar o eliminar objetos.

Además de conceder los permisos `s3:PutObject`, `s3:GetObject` y `s3:DeleteObject` al usuario, la política también concede los permisos `s3:ListAllMyBuckets`, `s3:GetBucketLocation` y `s3:ListBucket`. Estos son los permisos adicionales que requiere la consola. Las acciones `s3:PutObjectAcl` y `s3:GetObjectAcl` también son necesarias para poder copiar, cortar y pegar objetos en la consola. Para ver un tutorial de ejemplo en el que se conceden permisos a los usuarios y se prueban con la consola, consulte Tutorial de ejemplo: uso de las políticas del usuario para controlar el acceso al bucket.

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

Solución de problemas de identidad y acceso aAWS Application Cost Profiler

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje conAWS Application CoProServiceAWS Identity and Access Management Profiler Service.

Temas

No tengo autorización para realizar una acción en Application CoProService Profiler Service

Si la AWS Management Console le indica que no está autorizado para llevar a cabo una acción, debe ponerse en contacto con su administrador para recibir ayuda. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

En el siguiente ejemplo, el error se produce cuando el usuario de`mateojackson` IAM intenta utilizar la consola para ver detalles sobre el informe de CoProService Profiler Service, pero no tiene`application-cost-profiler:ListReportDefinitions` permiso.

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

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso de definición de informe mediante la`application-cost-profiler:ListReportDefinitions` acción.

No tengo autorización para realizar iam:PassRole

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

Algunos servicios de Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al 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 Application Cost Profiler Service. Sin embargo, la acción requiere que el servicio cuente con permisos que otorga 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 de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a miAWS cuenta de accedan a los recursos de CoProService Profiler Service

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 obtener más información, consulte lo siguiente:

- Para saber si Application CoProService Profiler Service es compatible con estas características, consulteCómo funcionaAWS Application Cost Profiler con IAM (p. 24).
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte Proporcionar acceso a un usuario de IAM a otra Cuenta de AWS de la que es propietario en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos a Cuentas de AWS de terceros, consulte Proporcionar acceso a Cuentas de AWS que son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una identidad federada, 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.

Validación de cumplimiento paraAWS Application Cost Profiler

Para saber si un Servicio de AWS está incluido en el ámbito de programas de conformidad específicos, consulte Servicios de AWS en el ámbito del programa de conformidad y escoja el programa de conformidad que le interese. Para obtener información general, consulte Programas de conformidad de AWS.

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

Su responsabilidad de conformidad al utilizar Servicios de AWS se determina en función de la sensibilidad de los datos, los objetivos de cumplimiento de su empresa y la legislación y los reglamentos correspondientes. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- Guías de inicio rápido de seguridad y conformidad: estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Architecting for HIPAA Security and Compliance on Amazon Web Services (Arquitectura para la seguridad y el cumplimiento de la HIPAA en Amazon Web Services): en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones aptas para HIPAA.

  Note

  No todos los Servicios de AWS son aptos para HIPAA. Para obtener más información, consulte la Referencia de servicios aptos para HIPAA.
- Recursos de conformidad de AWS: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub— EstoServicio de AWS proporciona una visión completa de su estado de seguridad internoAWS. Security Hub le permite comprobar susAWS recursos y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la referencia de controles de Security Hub.
- AWS Audit Manager: este Servicio de AWS le ayuda a auditar continuamente el uso de AWS con el fin de simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector.

Resiliencia enAWSPerfilador de costo de aplicación

La infraestructura global de AWS está conformada por regiones y zonas de disponibilidad de AWS. Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. 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 centros de datos únicos o múltiples.

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

Seguridad de la infraestructura enAWSPerfilador de costo de aplicación

Al tratarse de un servicio administrado, Application Cost Profiler está protegido porAWSprocedimientos de seguridad de red globales de que se describen enAmazon Web Services: Información general de procesos de seguridaddocumento técnico.

UsaAWSpublicadas en para obtener acceso a Application Cost Profiler a través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.0 o una versión posterior. Recomendamos TLS 1.2 o una versión posterior. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). 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 unaAWS Identity and Access Management(IAM) principal. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Monitorización de costo de costo de costo de aplicación en EventBridge

Puedes usar Amazon EventBridge para automatizarAWSy responder automáticamente a eventos del sistema, como problemas de disponibilidad de aplicaciones o cambios de recursos. Eventos deAWSlos servicios se entregan a EventBridge casi en tiempo real. Puede crear reglas sencillas para indicar qué eventos le resultan de interés, así como qué acciones automatizadas se van a realizar cuando un evento cumple una de las reglas. Para obtener más información, consulteAmazon EventBridge Guía del usuario de.

Puede monitorizarAWSeventos de costo de costo de costo de aplicación EventBridge. EventBridge dirige esos datos a los objetivos, como:AWS Lambday Amazon Simple Notification Service (Amazon SNS) Estos eventos son los mismos que los que aparecen en Amazon. CloudWatch Events, que ofrece near-real-time flujo de eventos del sistema que describen los cambios enAWSde AWS.

Supervise la generación de informes EventBridge

con EventBridge, puede crear reglas que definan las acciones que se deben realizar cuando Perfiler er er er er er er er er er er er er er er Por ejemplo, puede crear una regla que le envíe un mensaje de correo electrónico cada vez que se genera un informe.

Para supervisar la generación de informes

1. Inicia sesión enAWSusar una cuenta que tenga permisos para usar ambos EventBridge y Perfilador de costo de aplicación.
2. Abrir la Amazonía EventBridge Consola de:https://console.aws.amazon.com/events/.
3. Con los siguientes valores, cree un EventBridge regla que supervisa los eventos creados cuando se genera un informe:
   - En Rule type (Tipo de regla), elija Rule with an event pattern (Regla con un patrón de evento).
   - ParaOrigen del evento, eligeOtro.
   - En el navegadorPatrón de eventos, elija.Patrones personalizados (editor JSON)y, a continuación, pegue el siguiente patrón de eventos en el área de texto:

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

   - ParaTipos de objetivo, eligeAWSServicio de, y paraSeleccione un objetivo, elige laAWSservicio que desea actuar cuando EventBridge detecta un evento del tipo seleccionado. El destino se activa cuando se recibe un evento que coincide con el patrón de eventos definido en la regla.

Para obtener más información sobre la creación de reglas, consulteCreación de Amazon EventBridge reglas que reaccionan a los eventosen laAmazon EventBridge Guía del usuario de.

Ejemplo de un evento generado por informe

Este evento le informa cuando se genera un informe y está listo para que lo recupere. La`message`le proporciona el bucket de Amazon Simple Storage Service (Amazon S3) y la clave para el objeto de Amazon S3 en el que se almacena el informe.

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

Historial de documentos

En la siguiente tabla se describen las versiones de la documentación deAWSPerfilador de costo de aplicación.

Cambio	Descripción	Fecha
Monitoreo de eventos (p. 35)	Debido a cambios en el EventBridge consola, la forma en que se crean reglas para monitorear los eventos de Application Cost Profiler cambió. Para obtener más información, consulteApplication Cost Profiler events in EventBridge.	5 de julio de 2022
Actualizaciones de ejemplos de políticas de bucket de S3 (p. 35)	Actualización de los ejemplos de la política de bucket de S3 únicamente con documentación. Para obtener más información, consulteConfiguración de bucket de Amazon S3 para Application Cost Profiler.	6 de diciembre de 2021
Disponibilidad general (p. 35)	La versión pública inicial de Application Cost Profiler.	13 de mayo de 2021

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.