aws

Manual do usuário

Application Cost Profiler

Application Cost Profiler: Manual do usuário

Table of Contents

AWS O Application Cost Profiler será descontinuado até 30 de setembro de 2024 e não está mais aceitando novos clientes.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.

O que é o Application Cost Profiler da AWS?

O Application Cost Profiler da AWS ajuda você a separar o faturamento e os custos da AWS pelos inquilinos do seu serviço. Um inquilino pode ser um usuário, um grupo de usuários ou um projeto.

Um recurso é uma entidade com a qual os usuários podem trabalhar na AWS, como uma instância do Amazon Elastic Compute Cloud (Amazon EC2). Certifique-se de que você possa identificar o uso dos recursos do inquilino que escolher.

O uso típico de recursos da AWS inclui serviços compartilhados que oferecem suporte a vários locatários em sua organização. Alguns recursos usam dimensões baseadas no tempo. Para obter informações de custo e cobrança por inquilino em vez de usar o recurso por hora, você pode integrar seus recursos ao Application Cost Profiler. Com essa abordagem granular, entenda como os recursos da AWS são consumidos em uma solução de software compartilhada.

Os seguintes recursos, que podem usar dimensões baseadas em tempo ou uso por hora, estão habilitados para o Application Cost Profiler:

- Instâncias do Amazon EC2 (apenas sob demanda e instâncias spot)
- Filas do Amazon Simple Queue Service (Amazon SQS)
- Amazon Simple Notification Service (Amazon SNS) topics
- O Amazon DynamoDB lê e grava

> **Note**
>
> O uso do Amazon SQS, Amazon SNS e DynamoDB não é cobrado por tempo, diferentemente da maioria dos recursos. No caso deles, o uso durante uma hora (por exemplo, várias leituras e gravações no DynamoDB) é categorizado pela porcentagem da hora que você aloca para diferentes inquilinos, independentemente de quando as leituras ou gravações aconteceram durante a hora.

Integre seus serviços ao Application Cost Profiler em três etapas:

1. Ative e configure um relatório: essa etapa define a aparência da saída final.

2. Envie dados de uso do inquilino para o Application Cost Profiler: essa etapa requer o código do seu serviço para criar dados de uso que associem os inquilinos com o tempo que eles usaram os recursos. Em seguida, envie esses dados de uso para o Application Cost Profiler.
3. Obtenha relatórios: o Application Cost Profiler fornece relatórios na cadência especificada na configuração do relatório. Os relatórios mostram o custo associado ao uso de cada inquilino, oferecendo uma visão granular do seu faturamento.

Para mais informações sobre essas etapas, consulte Conceitos básicos.

Conceitos básicos do Application Cost Profiler

AWS O Application Cost Profiler ajuda você a obter informações de custo sobre seus AWS recursos relatando o uso do recurso por locatário, e não pelo recurso como um todo. Um inquilino pode ser um usuário, um grupo de usuários ou um projeto. Certifique-se de que você possa identificar o uso dos recursos do inquilino que escolher. Para obter relatórios de custo sobre o uso do inquilino, configure um relatório e envie dados de uso para o Application Cost Profiler. Esta seção discute os pré-requisitos que devem ser preenchidos antes de usar o Application Cost Profiler.

Tópicos

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira sua senha.

   Para obter ajuda ao fazer login usando o usuário raiz, consulte Fazer login como usuário raiz no Guia do usuário do Início de Sessão da AWS .
2. Ative a autenticação multifator (MFA) para seu usuário root.

   Para obter instruções, consulte Habilitar um MFA dispositivo virtual para seu usuário Conta da AWS root (console) no Guia IAM do usuário.

Criar um usuário com acesso administrativo

1. Ative o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No IAM Identity Center, conceda acesso administrativo a um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para entrar com seu usuário do IAM Identity Center, use o login URL que foi enviado ao seu endereço de e-mail quando você criou o usuário do IAM Identity Center.

Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No IAM Identity Center, crie um conjunto de permissões que siga as melhores práticas de aplicação de permissões com privilégios mínimos.

   Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .
2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

Conceder acesso programático

Os usuários precisam de acesso programático se quiserem interagir com pessoas AWS fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando AWS.

Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

Qual usuário precisa de acesso programático?	Para	Por
Identificação da força de trabalho (Usuários gerenciados no IAM Identity Center)	Use credenciais temporárias para assinar solicitações programáticas para o AWS CLI AWS SDKs, ou. AWS APIs	Siga as instruções da interface que deseja utilizar. • Para o AWS CLI, consulte Configurando o AWS CLI para uso AWS IAM Identity Center no Guia do AWS Command Line Interface usuário. • Para AWS SDKs, ferramentas e AWS APIs, consulte Autenticação do IAM

Qual usuário precisa de acesso programático?	Para	Por
		Identity Center no AWS SDKsGuia de referência de ferramentas.
IAM	Use credenciais temporári as para assinar solicitações programáticas para o AWS CLI AWS SDKs, ou. AWS APIs	Siga as instruções em Uso de credenciais temporárias com AWS recursos no Guia do IAM usuário.
IAM	(Não recomendado) Use credenciais de longo prazo para assinar solicitaç ões programáticas para o AWS CLI, AWS SDKs, ou. AWS APIs	Siga as instruções da interface que deseja utilizar. • Para o AWS CLI, consulte Autenticação usando credenciais de IAM usuário no Guia do AWS Command Line Interface usuário. • Para ferramentas AWS SDKs e ferramentas, consulte Autenticar usando credenciais de longo prazo no Guia de referência de ferramentas AWS SDKs e ferramentas. • Para AWS APIs, consulte Gerenciamento de chaves de acesso para IAM usuários no Guia IAM do usuário.

Pré-requisitos específicos do Application Cost Profiler

Antes de começar com o Application Cost Profiler, conclua os seguintes pré-requisitos:

- Ative o Cost Explorer

  Ative AWS Cost Explorer para sua AWS conta. A configuração de uma conta no Cost Explorer pode demorar até 24 horas. Você deve concluir a configuração do Cost Explorer para que o Application Cost Profiler possa gerar relatórios diários e mensais.

  Para obter mais informações, consulte Ativar o Cost Explorer no Guia do usuário do AWS Billing and Cost Management .

- Crie buckets do S3

  Crie no mínimo dois buckets do Amazon Simple Storage Service (Amazon S3). O Application Cost Profiler usa um bucket do S3 para fornecer relatórios para você. Use o outro bucket do S3 para fazer upload de dados de uso no Application Cost Profiler. Em geral, é preciso apenas um bucket do S3 para fazer upload dos dados de uso. No entanto, talvez você queira ter mais de um bucket do S3 para poder manter o uso de diferentes serviços em buckets do S3 separados com permissões diferentes, se necessário para sua segurança. Você deve conceder permissões ao Application Cost Profiler para esses buckets do S3.

  Para obter mais informações sobre a configuração dos buckets do Amazon S3 para o Application Cost Profiler, consulte Configuração de buckets do Amazon S3 para o Application Cost Profiler.

- Ativar tags

  Para relatar o uso por tag, em vez de por recurso, você deve habilitar essas tags no console do AWS Billing and Cost Management .

  Para obter mais informações sobre como ativar as tags AWS geradas, consulte Ativando as tags de alocação AWS de custos geradas no Guia do usuário.AWS Billing and Cost Management Para obter mais informações sobre tags definidas pelo usuário, consulte Tags de alocação de custos definidas pelo usuário no Guia do usuário do AWS Billing and Cost Management .

Próximas etapas

Após concluir os pré-requisitos, você pode:

- Configurar o relatório para enviar dados de uso ao Application Cost Profiler. Para obter mais informações, consulte Criar relatório.
- Obtenha e analise os relatórios gerados. Para obter mais informações, consulte Como usar os relatórios do Application Cost Profiler.

Configuração de buckets do Amazon S3 para o Application Cost Profiler

Para enviar dados de uso e receber relatórios do Application Cost Profiler da AWS, você deve ter pelo menos um bucket do Amazon Simple Storage Service (Amazon S3) no bucket da Conta da AWS para armazenar dados e um bucket S3 para receber os relatórios.

> **Note**
>
> Para usuários do AWS Organizations, os buckets do Amazon S3 podem estar na conta de gerenciamento ou em contas de membros individuais. Os dados nos buckets do S3 de propriedade da conta de gerenciamento podem ser usados para gerar relatórios para toda a organização. Em contas de membros individuais, os dados nos buckets do S3 só podem ser usados para gerar relatórios para essa conta membro.

Os buckets do S3 que você cria são de propriedade da Conta da AWS em que eles foram criados. Os buckets S3 são cobrados de acordo com as tarifas padrão do Amazon S3. Para obter mais informações sobre como criar um bucket do Amazon S3, consulte Criação de um bucket, no Guia do usuário do Amazon Simple Storage Service.

Para que o Application Cost Profiler use os buckets do S3, anexe uma política aos buckets que dá ao Application Cost Profiler permissões de leitura e/ou gravação no bucket. Se você modificar a política após a configuração dos relatórios, poderá impedir que o Application Cost Profiler possa ler os dados de uso ou entregar seus relatórios.

Os tópicos a seguir mostram como configurar permissões nos buckets do Amazon S3 depois de criá-los. Além da capacidade de ler e gravar objetos, se você criptografou os buckets, o Application Cost Profiler deverá ter acesso à chave AWS Key Management Service (AWS KMS) de cada bucket.

Tópicos

Fornecendo ao Application Cost Profiler acesso ao bucket S3 de entrega de relatórios

O bucket do S3 que você configura para que o Application Cost Profiler entregue os relatórios deve ter uma política anexada que permita que o Application Cost Profiler crie os objetos do relatório. Além disso, o bucket do S3 deve ser configurado para habilitar a criptografia.

> **Note**
>
> Ao criar o bucket, você deve optar por criptografá-lo. Você pode optar por criptografar o bucket com chaves gerenciadas pelo Amazon S3 (SSE-S3) ou com sua chave gerenciada pelo (SSE-KMS). AWS KMS Se você já criou o bucket sem criptografia, você deve editar o bucket para adicionar a criptografia.

Fornecendo ao Application Cost Profiler acesso ao bucket S3 de entrega de relatórios

1. Faça login no console do Amazon S3.
2. Selecione Buckets no painel de navegação à esquerda e escolha o bucket na lista.
3. Escolha Permissões e, em seguida, escolha Política de bucket e Editar.
4. Na seção Política, insira a política a seguir. Substitua *<bucket_name>* pelo nome do bucket e *<Conta da AWS>* pelo ID do seu Conta da 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": "<Conta da AWS>"
            },
            "ArnEquals": {
              "aws:SourceArn": "arn:aws:application-cost-profiler:us-east-1:<Conta
da AWS>:*"
            }
          }
        }
      ]
    }
```

Nessa política, você concede ao serviço principal (`application-cost-profiler.amazonaws.com`) do Application Cost Profiler acesso para entregar relatórios ao bucket especificado. Ele faz isso em seu nome e inclui um cabeçalho com a Conta da AWS e um ARN específico para o bucket de entrega de relatórios. Para garantir que o Application Cost Profiler esteja acessando o bucket somente quando estiver agindo em seu nome, a `Condition` verifica esses cabeçalhos.

5. Escolha Salvar alterações para salvar a política anexada ao seu bucket.

   Se você criou o bucket usando a criptografia SSE-S3, ele está pronto. Se usou a criptografia SSE-KMS, as etapas a seguir são necessárias para oferecer ao Application Cost Profiler acesso ao bucket.

6. (Opcional) Escolha a guia Propriedades do bucket e, em Criptografia padrão, selecione o nome do recurso da Amazon (ARN) para a chave do AWS KMS. Essa ação exibe o console do AWS Key Management Service e mostra sua chave.

7. (Opcional) Adicione a política para dar ao Application Cost Profiler acesso à chave do AWS KMS. Para obter instruções sobre como adicionar esse certificado, consulte Fornecendo ao Application Cost Profiler acesso a buckets S3 criptografados com SSE-KMS.

Fornecendo ao Application Cost Profiler acesso ao bucket S3 de entrega de relatórios

O bucket do S3 configurado para que o Application Cost Profiler entregue os relatórios deve ter uma política anexada que permita que o Application Cost Profiler crie os objetos do relatório.

> **Note**
>
> Ao conceder ao Application Cost Profiler acesso aos dados de uso, você concorda que podemos copiar temporariamente esses objetos de dados de uso para a Região da AWS Leste dos EUA (Norte da Virgínia) enquanto processamos relatórios. Esses objetos de dados serão mantidos na região Leste dos EUA (Norte da Virgínia) até que a geração do relatório mensal seja concluída.

Fornecendo ao Application Cost Profiler acesso ao bucket S3 de entrega de relatórios

1. Faça login no console do Amazon S3.
2. Selecione Buckets no painel de navegação à esquerda e escolha o bucket na lista.
3. Escolha Permissões e, em seguida, escolha Política de bucket e Editar.
4. Na seção Política, insira a política a seguir. Substitua *<bucket-name>* pelo nome do bucket e *<Conta da AWS>* pelo ID do seu Conta da 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": "<Conta da AWS>"
            },
            "ArnEquals": {
              "aws:SourceArn": "arn:aws:application-cost-profiler:us-east-1:<Conta
 da AWS>:*"
            }
```

```
            }
          }
        ]
      }
```

Nessa política, você concede ao serviço principal (`application-cost-profiler.amazonaws.com`) do Application Cost Profiler acesso para entregar relatórios ao bucket especificado. Ele faz isso em seu nome e inclui um cabeçalho com a Conta da AWS e um ARN específico para o bucket de uso. Para garantir que o Application Cost Profiler esteja acessando o bucket somente quando estiver agindo em seu nome, a `Condition` verifica esses cabeçalhos.

5. Escolha Salvar alterações para salvar a política anexada ao seu bucket.

Se o bucket estiver criptografado com chaves gerenciadas do AWS KMS, você deverá conceder ao Application Cost Profiler acesso ao bucket seguindo o procedimento na próxima seção.

Fornecendo ao Application Cost Profiler acesso a buckets S3 criptografados com SSE-KMS

Se você criptografar os buckets do S3 configurados para o Application Cost Profiler (necessários para buckets de relatórios) com as chaves armazenadas no AWS KMS (SSE-KMS), conceda permissões também ao Application Cost Profiler para descriptografá-los. Você faz isso dando acesso às chaves do AWS KMS usadas para criptografar os dados.

> **Note**
>
> Se o bucket estiver criptografado com chaves gerenciadas do Amazon S3, você não precisará concluir esse procedimento.

Fornecendo ao Application Cost Profiler acesso ao AWS KMS para buckets S3 criptografados com SSE-KMS

1. Acesse o console do AWS KMS para entrar.
2. Selecione Chaves gerenciadas pelo cliente no painel de navegação à esquerda e, em seguida, escolha a chave usada para criptografar o bucket na lista.
3. Selecione Alternar para exibição de política e, em seguida, escolha Editar.

4. Na seção Política, insira a instrução de política a seguir.

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

5. Escolha Salvar alterações para salvar a política anexada à chave.
6. Repita o procedimento para cada chave que criptografa um bucket do S3 que o Application Cost Profiler precisa acessar.

> **Note**
>
> Os dados são copiados do bucket do S3 na importação para os buckets gerenciados do Application Cost Profiler (que são criptografados). Se revogar o acesso às chaves, o Application Cost Profiler não poderá recuperar nenhum objeto novo do bucket. No entanto, todos os dados já importados ainda podem ser usados para gerar relatórios.

Criar relatório

Depois de cumprir os pré-requisitos, você estará pronto para configurar o relatório da Conta da AWS e enviar os dados de uso para o Application Cost Profiler da AWS. Esta seção descreve como configurar o relatório e enviar dados de uso ao Application Cost Profiler.

Configurar seu relatório do Application Cost Profiler

O procedimento a seguir mostra como configurar o relatório que você deseja gerar com base na data de uso. Você configura detalhes como a frequência com que o relatório é gerado.

> **Note**
>
> Se sua Conta da AWS faz parte de uma organização AWS, configure o relatório usando a conta de gerenciamento ou uma conta de membro individual. Os relatórios configurados para contas individuais contêm apenas dados dessa conta. Os relatórios configurados usando a conta de gerenciamento podem incluir dados de toda a organização.
> O bucket do Amazon S3 usado para a saída do relatório deve pertencer à conta que cria a configuração do relatório.

Configurar o relatório do Application Cost Profiler

1. Abra um navegador da Web e faça login no console do Application Cost Profiler.
2. Escolha Começar agora para configurar ou modificar um relatório.
3. Insira um Nome do relatório e uma Descrição do relatório para o relatório.
4. Insira o nome do bucket do S3 no campo Inserir nome do bucket S3 e insira o prefixo do S3 no campo Inserir prefixo do S3. Para obter mais informações sobre como criar buckets do S3 e conceder permissões ao Application Cost Profiler, consulte Configuração de buckets do Amazon S3 para o Application Cost Profiler.
5. Selecione as opções que você deseja que o relatório tenha:

   - Frequência de tempo: escolha se o relatório é gerado em uma cadência diária, mensal ou nas duas.
   - Formato de saída do relatório: escolha o tipo de arquivo a ser criado em no bucket do Amazon S3. Se você escolher CSV, o Application Cost Profiler criará um arquivo de texto de valores

separados por vírgula com compactação gzip para os relatórios. Se escolher Parquet, um arquivo Parquet será gerado para os relatórios.

6. Escolha Configurar para salvar as configurações do relatório.

> **Note**
>
> Você também pode usar a API da AWS Application Cost Profiler para configurar relatórios.

Verifique as configurações do relatório escolhendo Começar agora para ver a configuração atual do relatório.

> **Note**
>
> Você só pode ter um relatório configurado. Retornar à página de configuração editará o relatório existente.

Depois de configurar o relatório, a ingestão de dados é ativada. Integre os serviços com o Application Cost Profiler para fornecer dados de uso dos recursos.

Relatar dados de uso de inquilinos dos serviços

Depois de configurar o relatório, você estará pronto para enviar dados de uso do inquilino dos recursos ou serviços da conta. Você deve informar o Application Cost Profiler quando o recurso estiver sendo usado por um inquilino específico. Por exemplo, se o serviço aceita chamadas de API de diferentes inquilinos, registre um horário de início e término para cada inquilino ao iniciar e encerrar uma chamada de API desse inquilino. O Application Cost Profiler usa esses dados para gerar relatórios sobre o custo do serviço, de acordo com a quantidade de tempo gasto no trabalho de cada inquilino.

Para fornecer ao Application Cost Profiler os dados de uso, faça o seguinte:

- Preparar dados de uso de recursos: crie tabelas que descrevam quando um recurso é usado por um inquilino específico.
- Carregar dados de uso: faça upload das tabelas em um bucket do Amazon S3 que você concedeu permissão ao Application Cost Profiler para acessar.

- Importar dados de uso: chame a operação da API `ImportApplicationUsage` para que o Application Cost Profiler saiba que os dados estão prontos para serem processados.

As seções a seguir descrevem essas etapas em detalhes.

Tópicos

Etapa 1: preparando os dados de uso de recursos

À medida que um recurso está sendo usado no serviço, você rastreia qual inquilino o está usando. Registre esses dados em uma tabela que você pode carregar posteriormente para ser importada pelo Application Cost Profiler. Cada linha na tabela descreve um recurso, o inquilino que está usando o recurso e os horários de início e término desse uso. Um exemplo de recurso é uma instância do Amazon Elastic Compute Cloud (Amazon EC2) que está sendo usada.

Essa etapa exige que você integre o código ao serviço para gerar as informações corretas sobre o uso.

Os possíveis valores de alocação de custos estão indicados na tabela a seguir.

Campo	Descrição
ApplicationId	Identifica o aplicativo ou produto no sistema que está sendo usado. Define o escopo dos metadados do inquilino.
TenantId	Um identificador no sistema para o inquilino que está consumindo o recurso especificado. O Application Cost Profiler agrega esse nível no ApplicationId.
TenantDesc	(Opcional) Dados adicionais sobre o inquilino para seus relatórios adicionais.

Campo	Descrição
UsageAccountId	A conta na qual o recurso é executado (importante para contas que fazem parte de uma organização).
startTime	Registro de data e hora (em milissegundos e microssegundos) da Epoch, em UTC. Indica a hora de início do período de uso pelo inquilino especificado.
EndTime	Registro de data e hora (em milissegundos e microssegundos) da Epoch, em UTC. Indica a hora final do período de uso pelo inquilino especificado.
ResourceId	O nome do recurso da Amazon (ARN) do recurso usado.
Nome	(Opcional) Como alternativa à especificação de um resourceID, você pode especificar um Nome de tag de recurso para atribuir custos a um conjunto de recursos (o campo deve incluir o valor que você deseja usar para o Nome da tag. As tags de recursos são habilitadas como parte do relatório de custo e uso. Para obter mais informações sobre as tags de recursos, consulte os Detalhes das tags de recursos no Guia do usuário do relatório de custo e uso.

A saída deve estar em um arquivo de valores separados por vírgula (.csv) que inclua uma linha de título, conforme mostrado no exemplo a seguir.

```
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
```

Salve os dados como um arquivo com uma extensão.csv (ou .csv.gzip se ele for compactado com gzip). Quando você carrega esses dados para o Application Cost Profiler, cada fatia de tempo é atribuída ao inquilino associado. Neste exemplo, o relatório inclui o intervalo temporal do custo da instância do Amazon EC2 para esse inquilino. Somente para instâncias do Amazon EC2, fatias que não estão associadas a um locatário específico são adicionadas a um inquilino não atribuído. Os intervalos de tempo sobrepostos são contados várias vezes. É sua responsabilidade garantir que os dados na tabela de uso sejam precisos.

> **Note**
>
> O arquivo deve representar uma hora de tempo. Se um recurso for usado por várias horas, encerre o uso na hora e tenha um novo registro no próximo arquivo que comece ao mesmo tempo.
>
> Você deve enviar um único arquivo contendo os dados de uma hora inteira. Se vários arquivos forem enviados para os dados da mesma hora, o Application Cost Profiler considerará somente os dados no arquivo mais recente.

Por exemplo, a tabela a seguir mostra como o Application Cost Profiler calcula o uso de três inquilinos, em uma hora (3.600.000 milissegundos), com base nos intervalos de tempo fornecidos.

Inquilino	Fatias de tempo fornecidas	Porcentagem calculada do custo por hora
Inquilino 1	1.200.000 ms	33,34%
Inquilino 2	600.000 m	16.66%
<unattributed>		50,00%

Neste exemplo, o Inquilino 1 recebe um terço da hora e o Inquilino 2 recebe um sexto da hora. A meia hora restante (1.800.000 ms) não é atribuída a nenhum dos clientes, o que representa 50% da hora.

Atualmente, os seguintes recursos estão habilitados para o Application Cost Profiler:

- Instâncias do Amazon EC2 (apenas sob demanda e instâncias spot)
- Funções do Lambda (se você estiver enviando dados para uma função do Lambda, deverá enviar o ARN do recurso não qualificado como `ResourceId`).
- Instâncias do Amazon Elastic Container Service (Amazon ECS)
- Filas do Amazon Simple Queue Service (Amazon SQS)
- Amazon Simple Notification Service (Amazon SNS) topics
- O Amazon DynamoDB lê e grava

> **Note**
>
> O uso do Amazon SQS, Amazon SNS e DynamoDB não é cobrado por tempo, diferentemente da maioria dos recursos. No caso deles, o uso durante uma hora (por exemplo, várias leituras e gravações no DynamoDB) é categorizado pela porcentagem da hora que você aloca para diferentes inquilinos, independentemente de quando as leituras ou gravações aconteceram durante a hora.

Etapa 2: fazer o upload do uso do recurso

Depois de ter um arquivo de uso pelo inquilino, faça o upload do arquivo de dados para o Amazon S3 e certifique-se de que o Application Cost Profiler tenha permissão para acessá-lo.

Para saber mais sobre como criar funções para o bucket do S3, consulte Pré-requisitos específicos do Application Cost Profiler.

Você deve garantir que o Application Cost Profiler tenha acesso ao bucket do S3. Isso só precisa ser feito uma vez por bucket do S3 (você pode reutilizar o mesmo bucket para fazer upload de vários arquivos de uso). Para obter mais informações sobre o acesso ao bucket, consulte Fornecendo ao Application Cost Profiler acesso ao bucket S3 de entrega de relatórios. Se o bucket estiver criptografado, consulte Fornecendo ao Application Cost Profiler acesso a buckets S3 criptografados com SSE-KMS.

> **Note**
>
> Não é necessário criptografar os buckets do S3 que você usa para dados de uso.

Faça upload dos dados para o bucket do S3 como um arquivo, com uma extensão.csv (ou .csv.gzip se compactado com gzip) e em intervalos de hora em hora. Depois de carregar um novo arquivo, informe ao Application Cost Profiler que o upload foi realizado para que o arquivo possa ser importado para o relatório.

> **Note**
>
> Ao conceder ao Application Cost Profiler acesso aos dados de uso, você concorda que podemos copiar temporariamente esses objetos de dados de uso para a Região da AWS Leste dos EUA (Norte da Virgínia) enquanto processamos relatórios. Esses objetos de dados serão mantidos na região Leste dos EUA (Norte da Virgínia) até que a geração do relatório mensal seja concluída.

Etapa 3: importar dados de uso para o Application Cost Profiler

Depois de fazer o upload dos dados de uso em um bucket do Amazon S3 ao qual o Application Cost Profiler tem acesso, informe ao Application Cost Profiler que os dados existem e importe-os para o relatório final. Você faz isso usando a operação `ImportApplicationUsage` no API Application Cost Profiler.

Para obter informações sobre a API da AWS Application Cost Profiler, incluindo a operação `ImportApplicationUsage`, consulte a API da AWS do Application Cost Profiler.

O exemplo a seguir mostra como chamar `ImportApplicationUsage`. Substitua o *`texto de entrada entre colchetes`* pelos valores do bucket do S3 e do objeto carregado.

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

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

```
        "region": "<region-id>"
    }
}
```

> **Note**
>
> O parâmetro `region` só é necessário se o bucket estiver em uma Região da AWS que esteja desativado por padrão. Para obter mais informações, consulte Gerenciar as Regiões da AWS no Referência geral da AWS.

O Application Cost Profiler gera um novo relatório na frequência solicitada ao configurar seu relatório, usando os dados importados com `ImportApplicationUsage`.

Depois de configurar o relatório e automatizar a importação dos dados de uso para o Application Cost Profiler, você estará pronto para visualizar os relatórios gerados. Para obter mais informações sobre os relatórios, consulte Como usar os relatórios do Application Cost Profiler.

Como usar os relatórios do Application Cost Profiler

Depois de integrar os dados de uso ao Application Cost Profiler da AWS e enviar os dados de hora em hora, o Application Cost Profiler gera automaticamente o relatório.

Os relatórios são gerados diariamente ou mensalmente, com base na opção selecionada ao configurar o relatório. Os relatórios são entregues ao bucket do Amazon Simple Storage Service (Amazon S3) que você selecionou ao configurar o relatório.

Relatórios diários gerados no primeiro dia do mês têm os dados do mês anterior.

Dados disponíveis em um relatório do Application Cost Profiler

As colunas que são criadas em um relatório de uso são mostradas na tabela a seguir.

Nome da coluna	Descrição
PayerAccountId	O ID da conta de gerenciamento em uma organização ou o ID da conta se a conta não fizer parte do AWS Organizations.
UsageAccountId	O ID da conta em uso.
LineItemType	O tipo de registro. Sempre `Usage`.
UsageStartTime	Registro de data e hora (em milissegundos e microssegundos) da Epoch, em UTC. Indica a hora de início do período de uso pelo inquilino especificado.
UsageEndTime	Registro de data e hora (em milissegundos e microssegundos) da Epoch, em UTC. Indica a hora final do período de uso pelo inquilino especificado.
ApplicationIdentifier	O ApplicationID especificado nos dados de uso enviados ao Application Cost Profiler.

Nome da coluna	Descrição
TenantIdentifier	O ApplicationID especificado nos dados de uso enviados ao Application Cost Profiler. Dados sem registro nos dados de uso são coletados em `unattributed` .
TenantDescription	O `TenantDesc` especificado nos dados de uso enviados ao Application Cost Profiler.
ProductCode	O produto da AWS que está sendo cobrado (por exemplo, `AmazonEC2`).
UsageType	O tipo de uso que está sendo cobrado (por exemplo ,`BoxUsage:c5.large`).
Operation	A operação que está sendo cobrada (por exemplo,`RunInstances`).
ResourceId	O ID do recurso ou o nome do recurso da Amazon (ARN) do recurso que está sendo cobrado.
ScaleFactor	Se um recurso for superalocado por uma hora, por exemplo, os dados de uso relatados forem iguais a 2 horas em vez de 1 hora, um fator de escala será aplicado para tornar o total igual ao valor real faturado (nesse caso, 0,5). Essa coluna relata o fator de escala usado para o recurso específico naquela hora. O fator de escala é sempre maior que zero (0) e menor ou igual a 1.
TenantAttributionPercent	A porcentagem do uso atribuído ao inquilino especificado (entre zero (0) e 1).
UsageAmount	A quantidade de uso atribuída ao inquilino especificado.

Nome da coluna	Descrição
CurrencyCode	A moeda em que a taxa e o custo estão (por exemplo,USD).
Rate	A taxa de cobrança pelo uso, por unidade.
TenantCost	O custo total desse recurso para o inquilino especificado.
Region	A região da AWS dos recursos.
Nome	Se você criou tags de recursos para seus recursos no relatório de custo e uso ou por meio dos dados de uso do recurso, a tag Nome é mostrada aqui. Para obter mais informaçõ es sobre as tags de recursos, consulte os Detalhes das tags de recursos no Guia do usuário do relatório de custo e uso.

Veja a seguir um exemplo de um relatório de saída para um recurso por duas horas.

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

Neste exemplo, a primeira hora é alocada para `Tenant1` por metade do tempo. Meia-hora permanece com o`unattributed`. Na segunda hora, quatro inquilinos recebem a hora inteira. Nesse

caso, o fator de escala reduz todos eles para 0,25 e todos são alocados em um quarto da hora. Você pode ver o custo final na coluna `TenantCost`.

Cotas e endpoints do Application Cost Profiler da AWS

Sua conta da AWS possui cotas padrão, anteriormente chamadas de limites, para cada produto da AWS. A menos que especificado de outra forma, cada cota é específica da região AWS. Você pode solicitar aumentos para algumas cotas e outras cotas não podem ser aumentadas.

As tabelas a seguir listam as Service Quotas por conta e os endpoints da região AWS para o Application Cost Profiler.

Service Quotas

Recurso	Valor padrão	Descrição
Taxa de solicitações de `PutReportDefinition`	5	O número máximo de solicitações de `PutReportDefinition` por segundo e por conta.
Taxa de solicitações de `UpdateReportDefinition`	5	O número máximo de solicitações de `UpdateReportDefinition` por segundo e por conta.
Taxa de solicitações de `GetReportDefinition`	5	O número máximo de solicitações de `GetReportDefinition` por segundo e por conta.
Taxa de solicitações de `DeleteReportDefinition`	5	O número máximo de solicitações de `DeleteReportDefinition` por segundo e por conta.
Taxa de solicitações de `ListReportDefinitions`	5	O número máximo de solicitações de `ListReportDefinitions` por segundo e por conta.

Recurso	Valor padrão	Descrição
Taxa de solicitações de `ImportApplicationUsage`	5	O número máximo de solicitações de `ImportApplicationUsage` por segundo e por conta.
Tamanho máximo de um arquivo de dados de uso	10 MB	O tamanho máximo de um arquivo de dados de uso por hora.

Service endpoints (Endpoints de serviço)

O Application Cost Profiler é um serviço global. Todas as chamadas de API devem ser feitas para o endpoint Leste dos EUA (Norte da Virgínia).

- Leste dos EUA (Norte da Virgínia): `application-cost-profiler.us-east-1.amazonaws.com`

Segurança no Application Cost Profiler da AWS

A segurança para com a nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você contará com um datacenter e uma arquitetura de rede criados para atender aos requisitos das organizações com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isso como a segurança da nuvem e a segurança na nuvem:

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao Application Cost Profiler, consulte Serviços da AWS em escopo por programa de conformidade
- Segurança na nuvem: sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade dos dados, os requisitos da empresa e as leis e os regulamentos aplicáveis

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Application Cost Profiler da AWS. Ela mostra como configurar o Application Cost Profiler para atender aos objetivos de segurança e conformidade. Saiba também como usar outros serviços da AWS que ajudam a monitorar e proteger os recursos do Application Cost Profiler.

Índice

Proteção de dados no AWS Application Cost Profiler

O modelo de responsabilidade AWS compartilhada O modelo se aplica à proteção de dados no AWS Application Cost Profiler. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre privacidade de dados, consulte Privacidade de dados FAQ. Para obter informações sobre proteção de dados na Europa, consulte o Modelo de Responsabilidade AWS Compartilhada e GDPR a postagem no blog AWS de segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use a autenticação multifator (MFA) com cada conta.
- UseSSL/TLSpara se comunicar com AWS os recursos. Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Configure API e registre as atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de FIPS 140-3 módulos criptográficos validados ao acessar AWS por meio de uma interface de linha de comando ou umaAPI, use um endpoint. FIPS Para obter mais informações sobre os FIPS endpoints disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Application Cost Profiler ou outro Serviços da AWS usando o console,API, AWS CLI, ou AWS SDKs. Quaisquer dados inseridos em tags ou

campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é altamente recomendável que você não inclua informações de credenciais no URL para validar sua solicitação para esse servidor.

Criptografia em repouso

AWS O Application Cost Profiler sempre criptografa todos os dados armazenados no serviço em repouso sem exigir nenhuma configuração adicional. Essa criptografia é automática quando você usa o Application Cost Profiler.

Para os buckets do Amazon S3 fornecidos, criptografe o bucket de relatórios e o bucket de dados de uso e ofereça acesso ao Application Cost Profiler. Para obter mais informações, consulte Configuração de buckets do Amazon S3 para o Application Cost Profiler.

Criptografia em trânsito

AWS O Application Cost Profiler usa Transport Layer Security (TLS) e criptografia do lado do cliente para criptografia em trânsito. A comunicação com o Application Cost Profiler é sempre refeita HTTPS para que seus dados sejam sempre criptografados em trânsito. Essa criptografia é automática quando você usa o Application Cost Profiler.

Gerenciamento de identidade e acesso para o AWS Application Cost Profiler

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. IAMos administradores controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar os recursos do Application Cost Profiler. IAMé um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Público
- Autenticando com identidades
- Gerenciando acesso usando políticas
- Como o AWS Application Cost Profiler funciona com IAM

- AWS Exemplos de políticas baseadas em identidade do Application Cost Profiler
- Solução de problemas de identidade e acesso do AWS Application Cost Profiler

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Application Cost Profiler.

Usuário do serviço: se você usa o serviço do Application Cost Profiler para fazer o trabalho, o administrador fornece as credenciais e as permissões necessárias. À medida que usar mais recursos do Application Cost Profiler para fazer seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um atributo no Application Cost Profiler, consulte Solução de problemas de identidade e acesso do AWS Application Cost Profiler.

Administrador do serviço: se você for responsável pelos recursos do Application Cost Profiler na empresa, provavelmente terá acesso total ao Application Cost Profiler. Cabe a você determinar quais funcionalidades e recursos do Application Cost Profiler os usuários do serviço devem acessar. Em seguida, você deve enviar solicitações ao IAM administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos doIAM. Para saber mais sobre como sua empresa pode usar IAM o Application Cost Profiler, consulteComo o AWS Application Cost Profiler funciona com IAM.

IAMadministrador — Se você for IAM administrador, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao Application Cost Profiler. Para ver exemplos de políticas baseadas em identidade do Application Cost Profiler que você pode usar, consulte. IAM AWS Exemplos de políticas baseadas em identidade do Application Cost Profiler

Autenticando com identidades

A autenticação é como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como IAM usuário ou assumindo uma IAM função. Usuário raiz da conta da AWS

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Os usuários (do IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você entra como uma identidade federada, seu

administrador configurou previamente a federação de identidades usando IAM funções. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para você mesmo assinar solicitações, consulte AWS Signature versão 4 para API solicitações no Guia IAM do usuário.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia do AWS IAM Identity Center usuário e Autenticação AWS multifator IAM no Guia do IAMusuário.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para ver a lista completa de tarefas que exigem que você faça login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do IAM usuário.

Grupos e usuários do IAM

Um IAMusuário é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos confiar em credenciais temporárias em vez de criar IAM usuários com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com IAM os usuários, recomendamos que você alterne as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exigem credenciais de longo prazo no Guia do IAMusuário.

Um IAMgrupo é uma identidade que especifica uma coleção de IAM usuários. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar IAM recursos.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Casos de uso para IAM usuários no Guia IAM do usuário.

IAMfunções

Uma IAMfunção é uma identidade dentro da sua Conta da AWS que tem permissões específicas. É semelhante a um IAM usuário, mas não está associado a uma pessoa específica. Para assumir temporariamente uma IAM função no AWS Management Console, você pode alternar de usuário para IAM função (console). Você pode assumir uma função chamando uma AWS API operação AWS CLI or ou usando uma personalizadaURL. Para obter mais informações sobre métodos de uso de funções, consulte Métodos para assumir uma função no Guia IAM do usuário.

IAMfunções com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter informações sobre funções para federação, consulte Criação de uma função para um provedor de identidade terceirizado no Guia IAM do usuário. Se você usa o IAM Identity Center, configura um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a uma função em. IAM Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .
- Permissões temporárias IAM de IAM usuário — Um usuário ou função pode assumir uma IAM função para assumir temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas — Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a

diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. FASas solicitações são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte Encaminhar sessões de acesso.
  - Função de serviço — Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma AWS service (Serviço da AWS) no Guia do IAM usuário.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.
- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo AWS CLI AWS API solicitações. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Como usar uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia IAM do usuário.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como JSON documentos. Para obter mais informações sobre a estrutura e o conteúdo dos documentos de JSON política, consulte Visão geral das JSON políticas no Guia IAM do usuário.

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

IAMas políticas definem permissões para uma ação, independentemente do método usado para realizar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função do AWS Management Console AWS CLI, do ou do AWS API.

Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir IAM permissões personalizadas com políticas gerenciadas pelo cliente no Guia do IAMusuário.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolha entre políticas gerenciadas e políticas em linha no Guia do IAMusuário.

Políticas baseadas no recurso

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas de uma política baseada IAM em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLssão semelhantes às políticas baseadas em recursos, embora não usem o formato de documento JSON de política.

Amazon S3, AWS WAF, e Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber maisACLs, consulte a visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões — Um limite de permissões é um recurso avançado no qual você define as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (IAMusuário ou função). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para IAM entidades no Guia IAM do usuário.

- Políticas de controle de serviço (SCPs) — SCPs são JSON políticas que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. Os SCP limites de permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations eSCPs, consulte Políticas de controle de serviços no Guia AWS Organizations do Usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia IAM do usuário.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de política estão envolvidos, consulte Lógica de avaliação de políticas no Guia IAM do usuário.

Como o AWS Application Cost Profiler funciona com IAM

Antes de usar IAM para gerenciar o acesso ao Application Cost Profiler, você deve entender quais IAM recursos estão disponíveis para uso com o Application Cost Profiler. Para obter uma visão geral de como o Application Cost Profiler e outros AWS serviços funcionam comIAM, consulte AWS Serviços que funcionam com IAM no Guia do IAMusuário.

Tópicos

- Políticas baseadas em identidade do Application Cost Profiler
- Políticas baseadas em recursos do Application Cost Profiler
- Autorização baseada em tags do Application Cost Profiler
- Funções do Application Cost Profiler IAM

Políticas baseadas em identidade do Application Cost Profiler

Com políticas IAM baseadas em identidade, você pode especificar ações e recursos permitidos ou negados, além das condições sob as quais as ações são permitidas ou negadas. O Application Cost Profiler suporta ações específicas. Para saber mais sobre todos os elementos que você usa em uma JSON política, consulte Referência IAM JSON de elementos de política no Guia do IAM usuário.

Ações

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O `Action` elemento de uma JSON política descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da AWS API operação associada. Há algumas exceções, como ações somente com permissão que não têm uma operação correspondente. API Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

As ações de política no Application Cost Profiler usam o seguinte prefixo antes da ação: `application-cost-profiler:`. Por exemplo, para conceder permissão para alguém visualizar os detalhes da definição do Application Cost Profiler, inclua a ação `application-cost-profiler:GetReportDefinition` na política da pessoa. As instruções de política devem incluir um elemento `Action` ou `NotAction`. O Application Cost Profiler define seu próprio conjunto de ações que descrevem as tarefas que você pode executar com esse serviço.

Para especificar várias ações em uma única declaração, separe-as com vírgulas, conforme a seguir.

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

A seguir estão as ações disponíveis no Application Cost Profiler. Cada um permite a API ação com o mesmo nome. Para obter mais informações sobre o Application Cost ProfilerAPI, consulte AWS Application Cost Profiler Reference. API

- `application-cost-profiler:ListReportDefinitions`— Permite listar a definição do relatório para sua AWS conta, se houver.

- `application-cost-profiler:GetReportDefinition`: permite obter os detalhes da definição do relatório para o relatório do Application Cost Profiler.
- `application-cost-profiler:PutReportDefinition`: permite criar uma nova definição de relatório.
- `application-cost-profiler:UpdateReportDefinition`: permite atualizar a definição de um relatório.
- `application-cost-profiler:DeleteReportDefinition`— Permite excluir um relatório (disponível somente por meio do Application Cost ProfilerAPI).
- `application-cost-profiler:ImportApplicationUsage`: permite solicitar que o Application Cost Profiler importe dados de uso de um bucket específico do Amazon S3.

Recursos

O Application Cost Profiler não suporta a especificação do recurso Amazon Resource Names (ARNs) em uma política.

Chaves de condição

O Application Cost Profiler não fornece nenhuma chave de condição específica ao serviço, mas é compatível com o uso de algumas chaves de condição globais. Para ver todas as chaves de condição AWS globais, consulte Chaves de contexto de condição AWS global no Guia IAM do usuário.

Exemplos

Para visualizar exemplos de políticas baseadas em identidade do Application Cost Profiler, consulte AWS Exemplos de políticas baseadas em identidade do Application Cost Profiler.

Políticas baseadas em recursos do Application Cost Profiler

O Application Cost Profiler não suporta políticas baseadas em recursos.

Autorização baseada em tags do Application Cost Profiler

O Application Cost Profiler não é compatível com recursos de marcação ou de controle de acesso com base em tags.

Funções do Application Cost Profiler IAM

Uma IAMfunção é uma entidade dentro da sua AWS conta que tem permissões específicas.

Usar credenciais temporárias com o Application Cost Profiler

Você pode usar credenciais temporárias para entrar com a federação, assumir uma IAM função ou assumir uma função entre contas. Você obtém credenciais de segurança temporárias ligando para AWS STS API operações como AssumeRoleou GetFederationToken.

Usar credenciais temporárias com o Application Cost Profiler.

Funções vinculadas a serviço

As funções vinculadas ao serviço permitem que AWS os serviços acessem recursos em outros serviços para concluir uma ação em seu nome. As funções vinculadas ao serviço aparecem em sua IAM conta e são de propriedade do serviço. Um administrador do pode visualizar, mas não pode editar as permissões para funções vinculadas ao serviço.

O Application Cost Profiler não é compatível com funções vinculadas ao serviço.

Perfis de serviço

Esse atributo permite que um serviço assuma um perfil de serviço em seu nome. O perfil permite que o serviço acesse recursos em outros serviços para concluir uma ação em seu nome. As funções de serviço aparecem na sua IAM conta e são de propriedade da conta. Isso significa que um administrador do pode alterar as permissões para essa função. Porém, fazer isso pode alterar a funcionalidade do serviço.

O Application Cost Profiler não oferece suporte a perfis de serviço.

AWS Exemplos de políticas baseadas em identidade do Application Cost Profiler

Por padrão, IAM usuários e funções não têm permissões para criar ou modificar recursos do AWS Application Cost Profiler. Eles também não podem realizar tarefas usando o AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Um administrador deve criar IAM políticas que concedam aos usuários e funções permissão para realizar as API operações específicas de que precisam. O administrador deve então anexar essas políticas aos IAM usuários ou grupos que exigem essas permissões.

Para saber como criar uma política IAM baseada em identidade usando esses exemplos de documentos JSON de política, consulte Criação de políticas na JSON guia do IAMusuário.

Tópicos

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Application Cost Profiler em sua conta. Essas ações podem incorrer em custos para seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte políticas AWS gerenciadas ou políticas AWS gerenciadas para funções de trabalho no Guia IAM do usuário.
- Aplique permissões com privilégios mínimos — Ao definir permissões com IAM políticas, conceda somente as permissões necessárias para realizar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre IAM como usar para aplicar permissões, consulte Políticas e permissões IAM no Guia IAM do usuário.
- Use condições nas IAM políticas para restringir ainda mais o acesso — Você pode adicionar uma condição às suas políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usandoSSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte elementos IAM JSON da política: Condição no Guia IAM do usuário.
- Use o IAM Access Analyzer para validar suas IAM políticas e garantir permissões seguras e funcionais — o IAM Access Analyzer valida políticas novas e existentes para que as políticas

sigam a linguagem da IAM política (JSON) e as melhores práticas. IAM IAMO Access Analyzer fornece mais de 100 verificações de políticas e recomendações práticas para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validar políticas com o IAM Access Analyzer no Guia do IAMUsuário.

- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija IAM usuários ou um usuário root Conta da AWS, ative MFA para obter segurança adicional. Para exigir MFA quando API as operações são chamadas, adicione MFA condições às suas políticas. Para obter mais informações, consulte APIAcesso seguro MFA no Guia do IAM usuário.

Para obter mais informações sobre as melhores práticas emIAM, consulte as melhores práticas de segurança IAM no Guia IAM do usuário.

Como usar o console do Application Cost Profiler

Para acessar o console do AWS Application Cost Profiler, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do Application Cost Profiler em sua AWS conta. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas exigidas, o console não funcionará conforme planejado para entidades (IAMusuários ou funções) com essa política.

Para garantir que essas entidades possam usar o console do Application Cost Profiler para visualizar a definição do relatório do Application Cost Profiler para sua AWS conta, anexe as seguintes permissões às entidades.

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

Por exemplo, é possível criar a política a seguir para os usuários somente para leitura.

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

```
      }
   ]
}
```

Para obter mais informações, consulte Adicionar permissões a um usuário no Guia do IAM usuário.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para AWS CLI o. ou AWS API o. Em vez disso, permita o acesso somente às ações que correspondam à API operação que você está tentando realizar.

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permita IAM aos usuários visualizar as políticas embutidas e gerenciadas que estão anexadas à identidade do usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando o AWS CLI ou. AWS API

```
{
    "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": "*"
        }
    ]
}
```

Acessar um bucket do Amazon S3

Neste exemplo, você deseja conceder a um IAM usuário da sua AWS conta acesso a um dos seus buckets do Amazon S3,. `examplebucket` Você também deseja permitir que o usuário adicione, atualize e exclua objetos.

Além de conceder as permissões `s3:PutObject`, `s3:GetObject` e `s3:DeleteObject` ao usuário, a política também concede as permissões `s3:ListAllMyBuckets`, `s3:GetBucketLocation` e `s3:ListBucket`. Estas são permissões adicionais, exigidas pelo console. As ações `s3:PutObjectAcl` e `s3:GetObjectAcl` também são necessárias para copiar, recortar e colar objetos no console. Para obter uma demonstração de exemplo que concede permissões aos usuários e testa-os ao usar o console, consulte Demonstração de exemplo: Usar políticas de usuário para controlar o acesso a seu 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/*"
      }
   ]
}
```

Solução de problemas de identidade e acesso do AWS Application Cost Profiler

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o AWS Application Cost Profiler e AWS Identity and Access Management ()IAM.

Tópicos

- Não tenho autorização para executar uma ação no Application Cost Profiler
- Não estou autorizado a realizar o meu pedido: PassRole
- Quero permitir que pessoas fora da minha AWS conta acessem meus recursos do Application Cost Profiler

Não tenho autorização para executar uma ação no Application Cost Profiler

Se isso AWS Management Console indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. Caso seu administrador seja a pessoa que forneceu suas credenciais de início de sessão.

O exemplo de erro a seguir ocorre quando o `mateojackson` IAM usuário tenta usar o console para visualizar detalhes sobre o relatório do Application Cost Profiler, mas não tem `application-cost-profiler:ListReportDefinitions` permissão.

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

Nesse caso, Mateo pede ao administrador para atualizar suas políticas para que ele acesse o recurso de definição de relatório usando a ação `application-cost-profiler:ListReportDefinitions`.

Não estou autorizado a realizar o meu pedido: PassRole

Se você receber uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, as suas políticas deverão ser atualizadas para permitir a passagem de um perfil para o Application Cost Profiler.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um IAM usuário chamado `marymajor` tenta usar o console para realizar uma ação no Application Cost Profiler. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha AWS conta acessem meus recursos do Application Cost Profiler

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Application Cost Profiler é compatível com esses recursos, consulte Como o AWS Application Cost Profiler funciona com IAM.

- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Fornecer acesso a um IAM usuário em outro Conta da AWS de sua propriedade no Guia do IAM usuário.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Fornecer Contas da AWS acesso a terceiros no Guia do IAM usuário.
- Para saber como fornecer acesso por meio da federação de identidades, consulte Fornecendo acesso a usuários autenticados externamente (federação de identidades) no Guia do IAMusuário.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

Validação de conformidade para o AWS Application Cost Profiler

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para HIPAA segurança e conformidade na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar HIPAA aplicativos qualificados.

> **Note**
>
> Nem todos Serviços da AWS são HIPAA elegíveis. Para obter mais informações, consulte a Referência de serviços HIPAA elegíveis.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.

- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização ()). ISO
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, por exemplo PCIDSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência do Application Cost Profiler da AWS

A infraestrutura global da AWS é criada com base em regiões e zonas de disponibilidade da AWS. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, alta throughput e redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Para obter mais informações sobre regiões e zonas de disponibilidade da AWS, consulte Infraestrutura global da AWS.

Segurança da infraestrutura no AWS Application Cost Profiler

Como um serviço gerenciado, o AWS Application Cost Profiler é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa API chamadas AWS publicadas para acessar o Application Cost Profiler pela rede. Os clientes devem oferecer suporte para:

- Segurança da camada de transporte (TLS). Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Suítes de criptografia com sigilo direto perfeito (), como (Ephemeral PFS Diffie-Hellman) ou DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando uma ID de chave de acesso e uma chave de acesso secreta associada a um IAM principal. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Monitorando eventos do Application Cost Profiler no EventBridge

O Amazon EventBridge pode ser usado para automatizar seus serviços da AWS e responder automaticamente a eventos do sistema, como problemas de disponibilidade de aplicações ou alterações de recursos. Os eventos dos serviços da AWS são entregues ao EventBridge quase em tempo real. Você pode escrever regras simples para indicar quais eventos são do seu interesse, e as ações automatizadas a serem tomadas quando um evento corresponder à regra. Para obter mais informações, consulte o Guia do usuário do Amazon EventBridge.

Monitorando eventos do Application Cost Profiler da AWS no EventBridge. O EventBridge encaminha esses dados para destinos como AWS Lambda e o Amazon Simple Notification Service (Amazon SNS). Esses eventos são iguais aos que aparecem no Amazon CloudWatch Events, que oferece um fluxo quase em tempo real de eventos do sistema que descrevem as mudanças nos recursosAWS.

Monitorar a geração de relatórios com o EventBridge

Com o EventBridge, você pode criar regras que definem ações a serem executadas quando o Application Cost Profiler envia uma notificação de geração de um relatório. Por exemplo, você pode criar uma regra que envia uma mensagem de e-mail sempre que um relatório for gerado.

Para monitorar a geração de relatórios

1. Faça login na AWS usando uma conta que tenha permissões para usar o EventBridge e o Application Cost Profiler.
2. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
3. Usando os valores a seguir, crie uma regra do EventBridge que monitore os eventos criados quando um relatório é gerado:

   - Em Tipo de regra, escolha Regra com um padrão de evento.
   - Em Origem do evento, escolha Outra.
   - Em Padrão de evento, escolha Padrões personalizados (editor JSON) e cole um dos seguintes exemplos de padrão de evento na área de texto:

```
{
  "source": ["aws.application-cost-profiler"],
```

```
  "detail-type": ["Application Cost Profiler Report Generated"]
}
```

- Em Tipos de destino, escolha o serviço da AWS e, em Selecionar um destino, escolha o serviço da AWS que você deseja utilizar quando o EventBridge detectar um evento do tipo selecionado. O destino é acionado quando é recebido um evento que corresponde ao padrão de evento definido na regra.

Para obter informações sobre como criar regras, consulte Criar regras do Amazon EventBridge que reagem a eventos no Guia do usuário do Amazon EventBridge.

Exemplo de um evento gerado por relatório

Esse evento informa quando um relatório é gerado e está pronto para ser recuperado. O campo `message` fornece o bucket e a chave do Amazon Simple Storage Service (Amazon S3) para o objeto do Amazon S3 em que o relatório está armazenado.

```
{
   "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"
   }
}
```

Histórico do documento

A tabela a seguir descreve as versões da documentação do Application Cost Profiler da AWS.

Alteração	Descrição	Data
Notificação de suspensão de serviço	O Application Cost Profiler da AWS será descontinuado até 30 de setembro de 2024 e não está mais aceitando novos clientes.	11 de agosto de 2023
Eventos de monitoramento	Devido às mudanças no console do EventBridge, a forma como as regras para monitorar os eventos do Application Cost Profiler mudou. Para obter mais informações, consulte Monitorando eventos do Application Cost Profiler no EventBridge.	5 de julho de 2022
Atualizações em exemplos de políticas de bucket do S3	Atualização somente com documentação dos exemplos de políticas de bucket do S3. Para obter mais informações, consulte Configuração dos buckets do Amazon S3 para o Application Cost Profiler.	6 de dezembro de 2021
Disponibilidade geral	O lançamento público inicial do Application Cost Profiler.	13 de maio de 2021