# Descreve Profiler

## Guia do usuário

# Descreve Profiler: Guia do usuário

# Table of Contents

# O que é oAWSApplication Cost Profiler?

AWSApplication Cost Profiler é um serviço que ajuda você a separar seuAWSfaturamento e custos pelos locatários do seu serviço. UMAinquilinaPode ser um usuário, um grupo de usuários ou um projeto. Certifique-se de que você possa identificar o uso do recurso pelo locatário que você escolher. TípicoAWSo uso de recursos inclui serviços compartilhados que suportam vários locatários em sua organização. Para obter informações de custo e faturamento por locatário em vez de usar por hora para o recurso, você pode integrar seus recursos ao Application Cost Profiler. Com essa abordagem granular, você pode entender comoAWSos recursos são consumidos em uma solução de software compartilhado.

Você integra seus serviços ao Application Cost Profiler em três etapas:

1. Habilitar e configurar um relatório— Esta etapa define como você quer que sua saída final seja parecida.
2. Enviar dados de uso do locatário para o Application Cost Pro— Esta etapa requer código em seu serviço para criar dados de uso que associam os locatários ao tempo em que usam seus recursos e, em seguida, envie esses dados de uso para o Application Cost Profiler.
3. Obter relatórios— Application Cost Profiler fornece relatórios na cadência especificada na configuração do relatório. Os relatórios mostram o custo associado ao uso de cada locatário, oferecendo uma visão granular do faturamento.

Para obter mais informações sobre essas etapas, consulteComeçar a usar (p. 2).

# Conceitos básicos do Application Cost Profiler

AWSO Application Cost Profiler ajuda você a obter informações de custo sobre seuAWSrecursos relatando o uso de recursos por locatário, em vez de para o recurso como um todo. UMAinquilinaPode ser um usuário, um grupo de usuários ou um projeto. Certifique-se de que você possa identificar o uso do recurso pelo locatário que você escolher. Para obter relatórios de custo sobre o uso do locatário, você configura um relatório e envia dados de uso para o Application Cost Profiler. Esta seção discute os pré-requisitos que você deve concluir antes de usar o Application Cost Profiler.

Tópicos



## Conseguir uma Conta da AWS e as credenciais do usuário raiz

Para acessar a AWS, você deve se cadastrar em uma conta da Conta da AWS.

Para se cadastrar em uma Conta da AWS

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

   Parte do procedimento de cadastro envolve uma chamada telefônica e a digitação de um código de verificação usando o teclado do telefone.

AWSA envia um e-mail de confirmação depois que o processo de cadastramento é concluído. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando My Account (Minha conta).

## Criar um usuário do IAM

Se sua conta já inclui umAWS Identity and Access ManagementUsuário (IAM) com totalAWSPermissões administrativas, você pode ignorar esta seção.

> Note
>
> Para obter mais informações sobre como usar o IAM com Application Cost Profiler, consulteIdentity and Access Management para oAWSCriador de custos do aplicativo (p. 21).

Ao criar uma conta da Amazon Web Services (AWS), você começa com uma única identidade de login. Essa identidade tem acesso completo a todos os Serviços da AWS e recursos na conta. Essa identidade é chamada de usuário raiz da Conta da AWS. Ao fazer login, insira o endereço de e-mail e a senha usados para criar a conta.

> **Important**
>
> Recomendamos que não use o usuário root para suas tarefas do dia a dia, nem mesmo as administrativas. Em vez disso, siga as práticas recomendadas sobre utilização de usuário raiz somente para criar seu primeiro usuário do IAM. Depois, armazene as credenciais do usuário root com segurança e use-as para executar somente algumas tarefas de gerenciamento de contas e de serviços. Para exibir as tarefas que exigem que você faça login como usuário root, consulte Tarefas que exigem credenciais do usuário root.

### Para criar um usuário administrador para você mesmo e adicionar o usuário a um grupo de administradores (console)

1. Faça login no console do IAM como proprietário da conta escolhendo Root user (Usuário root) e inserindo o endereço de e-mail da sua Conta da AWS. Na próxima página, insira sua senha.

   > **Note**
   >
   > Recomendamos seguir as práticas recomendadas para utilizar o usuário do IAM **`Administrator`** a seguir e armazenar as credenciais do usuário raiz com segurança. Cadastre-se como o usuário raiz apenas para executar algumas tarefas de gerenciamento de serviços e contas.

2. No painel de navegação, escolha Users (Usuários) e Add users (Adicionar usuários).
3. Em User name (Nome do usuário), digite **`Administrator`**.
4. Marque a caixa de seleção ao lado do acesso ao AWS Management Console. Então, selecione Custom password (Senha personalizada), e insira sua nova senha na caixa de texto.
5. (Opcional) Por padrão, a AWS exige que o novo usuário crie uma senha ao fazer login pela primeira vez. Você pode desmarcar a caixa de seleção próxima de User must create a new password at next sign-in (O usuário deve criar uma senha no próximo login) para permitir que o novo usuário redefina a senha depois de fazer login.
6. Selecione Next (Próximo): Permissions
7. Em Set permissions (Conceder permissões), escolha Add user to group (Adicionar usuário ao grupo).
8. Escolha Create group (Criar grupo).
9. Na caixa de diálogo Create group (Criar grupo), em Group name (Nome do grupo), digite **`Administrators`**.
10. Escolha Filter policies (Filtrar políticas) e, depois, selecione AWS managed — job function (Função de trabalho gerenciada da AWS) para filtrar o conteúdo da tabela.
11. Na lista de políticas, marque a caixa de seleção AdministratorAccess. A seguir escolha Criar grupo.

    > **Note**
    >
    > Você deve ativar o acesso de usuário do IAM e da função para Billing (Faturamento) antes de usar as permissões de `AdministratorAccess` para acessar o console do AWS Billing and Cost Management. Para fazer isso, siga as instruções na etapa 1 do tutorial sobre como delegar acesso ao console de faturamento.

12. Suporte a lista de grupos, selecione a caixa de seleção para seu novo grupo. Escolha Refresh (Atualizar) caso necessário, para ver o grupo na lista.
13. Selecione Next (Próximo): Tags.
14. (Opcional) Adicione metadados ao usuário anexando tags como pares de chave-valor. Para obter mais informações sobre como usar tags no IAM, consulte Marcar entidades do IAM no Manual do usuário do IAM.

15. Selecione Next (Próximo): Review (Revisar)Para ver uma lista de associações de grupos a serem adicionadas ao novo usuário. Quando você estiver pronto para continuar, escolha Create user (Criar usuário).

Você pode usar esse mesmo processo para criar mais grupos e usuários e conceder aos seus usuários acesso aos recursos da sua Conta da AWS. Para saber como usar políticas para restringir as permissões de usuário a recursos específicos da AWS, consulte Gerenciamento de acesso e Exemplos de políticas.

# Fazer login como usuário do IAM

Entre no console do IAM escolhendo IAM user (Usuário do IAM) e inserindo o ID da sua conta da Conta da AWS ou o alias da conta. Na próxima página, insira seu nome de usuário do IAM e sua senha.

Note

Para sua conveniência, a página de login da AWS usa um cookie de navegador para lembrar o nome de usuário do IAM e as informações da conta. Se você fez login anteriormente como outro usuário, escolha o link de login embaixo do botão para retornar à página principal de login. Daí, você pode inserir o ID da Conta da AWS ou o alias da conta para ser redirecionado para a página de login de usuário do IAM para sua conta.

# Criar chaves de acesso para usuários do IAM

As chaves de acesso consistem em um ID da chave de acesso e uma chave de acesso secreta, que são usados para assinar solicitações programáticas feitas por você à AWS. Se você não tiver chaves de acesso, poderá criá-las usando o AWS Management Console. Como prática recomendada, não utilize as chaves de acesso do usuário raiz da Conta da AWS para realizar qualquer tarefa em que elas não sejam necessárias. Em vez disso, crie um novo usuário administrador do IAM com as chaves de acesso para você mesmo.

A única vez que você pode visualizar ou baixar a chave de acesso secreta é quando você a cria. Não será possível recuperá-la, posteriormente. No entanto, você pode criar novas chaves de acesso a qualquer momento. Você também deve ter permissões para executar as ações do IAM necessárias. Para obter mais informações, consulte Permissões necessárias para acessar recursos do IAM no Guia do usuário do IAM.

Para criar chaves de acesso para um usuário do IAM

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Usuários.
3. Escolha o nome do usuário cujas chaves de acesso você quer gerenciar, em seguida, escolha a guia Security credentials (Credenciais de segurança).
4. Na seção Access keys (Chaves de acesso), escolha Create access key (Criar chave de acesso).
5. Para ver o novo par de chaves de acesso, escolha Show (Mostrar). Você não terá mais acesso à chave de acesso secreta depois que essa caixa de diálogo for fechada. Suas credenciais terão a seguinte aparência:
   - ID de chave de acesso: AKIAIOSFODNN7EXAMPLE
   - Chave de acesso secreta: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
6. Para baixar o par de chaves, escolha Baixar arquivo .csv. Armazene as chaves em um lugar seguro. Você não terá mais acesso à chave de acesso secreta depois que essa caixa de diálogo for fechada.

   Mantenha a confidencialidade das chaves para proteger sua Conta da AWS e nunca as envie por e-mail. Não compartilhe as chaves fora da sua organização, mesmo se uma pesquisa parecer vir da

AWS ou da Amazon.com. Alguém que legitimamente represente a Amazon jamais pedirá a você sua chave secreta.

7. Depois de baixar o arquivo `.csv`, escolha Close (Fechar). Quando você cria uma chave de acesso, o par de chaves é ativo por padrão, e você pode usar o par imediatamente.

Tópicos relacionados

- O que é o IAM? no Guia do usuário do IAM
- Credenciais de segurança da AWS em Referência geral da AWS

# Pré-requisitos específicos do Application Cost Profiler

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

- Habilitar Cost Explorer

  Habilitar oAWS Cost ExplorerPara suas receitasAWSconta. A configuração de uma conta com o Cost Explorer pode levar até 24 horas. Você deve concluir a configuração do Cost Explorer antes que o Application Cost Profiler possa gerar relatórios diários e mensais.

  Para obter mais informações, consulteHabilitar o Cost Explorer.noAWS Billing and Cost ManagementGuia do usuário do.

- Crie buckets do S3

  Crie pelo menos dois buckets do Amazon Simple Storage Service (Amazon S3). O Application Cost Profiler usa um bucket do S3 para fornecer relatórios a você. Você usa o outro bucket do S3 para carregar dados de uso para o Application Cost Profiler. Normalmente, você só precisa de um bucket do S3 para carregar dados de uso. No entanto, talvez você queira ter mais de um bucket do S3 para que você possa manter o uso de serviços diferentes em buckets S3 separados com permissões diferentes, se necessário para sua segurança. Você deve dar permissões do Application Cost Profiler a esses buckets do S3.

  Para obter mais informações sobre como configurar os buckets do Amazon S3 para Application Cost Profiler, consulteConfigurar buckets do Amazon S3 para o Application Cost Profiler (p. 6).

- Ativar tags

  Para relatar o uso por tag, em vez de por recurso, você deve habilitar essas tags naAWS Billing and Cost Managementconsole do .

  Para obter mais informações sobre como ativar oAWSTags geradas, consulteComo ativar oAWSTags de alocação de custos geradas pelanoAWS Billing and Cost ManagementGuia do usuário do. Para obter mais informações sobre como ativar tags definidas pelo usuário, consulteComo ativar tags de alocação de custos definidas pelo usuárionoAWS Billing and Cost ManagementGuia do usuário do.

# Próximas etapas

Depois de concluir esses pré-requisitos, você poderá:

- Configure seu relatório e envie dados de uso para o Application Cost Profiler. Para obter mais informações, consulte Como criar seu relatório (p. 10).

- Obtenha e analise seus relatórios gerados. Para obter mais informações, consulte Usando relatórios Application Cost Profiler (p. 15).

# Configurar buckets do Amazon S3 para o Application Cost Profiler

Para enviar dados de uso e receber relatórios deAWSO Application Cost Profiler, você deve ter pelo menos um bucket do Amazon Simple Storage Service (Amazon S3) em seuConta da AWSPara armazenar dados e um bucket do S3 para receber seus relatórios.

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

Os buckets do S3 que você cria pertencem aoConta da AWSem que você os cria. Os buckets do S3 são cobrados de acordo com as taxas padrão do Amazon S3. Para obter mais informações sobre como criar um bucket do Amazon S3, consulteCriação de um bucketnoGuia do usuário do Amazon Simple Storage Service.

Para que o Application Cost Profiler use os buckets do S3, você deve anexar uma política aos buckets que dão permissões do Application Cost Profiler para ler e/ou gravações no bucket. Se você modificar a política após a configuração dos relatórios, poderá impedir que o Application Cost Profiler possa ler seus dados de uso ou entregar seus relatórios.

Os tópicos a seguir mostram como configurar permissões em seus 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 aoAWS Key Management Service(AWS KMS) chave para cada balde.

Tópicos

- Dando acesso ao Application Cost Profiler ao bucket S3 de entrega de relatórios (p. 6)
- Dando acesso ao Application Cost Profiler aos dados de uso do bucket S3 (p. 7)
- Dando acesso ao Application Cost Profiler a buckets S3 criptografados pelo SSE- (p. 9)

## Dando acesso ao Application Cost Profiler ao bucket S3 de entrega de relatórios

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

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

Para dar acesso ao Application Cost Profiler ao bucket S3 de entrega de relatórios

1. Vá para oConsole do Amazon S3e faça login.

2. SelectBucketsNa navegação à esquerda e, em seguida, selecione seu bucket na lista.
3. Selecione oPermissõesguia, em seguida, ao lado dePolítica de bucket, escolhaEdite.
4. NoPolíticaseção, insira a seguinte política do. Substituir*<bucket_name>*pelo nome do bucket do.*<Conta da AWS>*pelo ID do seuConta 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>:*"
            }
          }
        }
      ]
    }
```

   Nesta política, você está fornecendo o principal de serviço Application Cost Profiler (`application-cost-profiler.amazonaws.com`) Acesso para entregar relatórios ao bucket especificado. Ele faz isso em seu nome e inclui um cabeçalho com seuConta da AWSe um ARN específico para o intervalo de entrega do relatório. Para garantir que o Application Cost Profiler esteja acessando seu bucket somente ao agir em seu nome, o`Condition`verifica esses cabeçalhos.
5. SelecioneSalve as alteraçõespara salvar sua política, anexada ao seu bucket.

   Se você criou seu bucket usando criptografia SSE-S3, então você está pronto. Se você usou a criptografia SSE-KMS, as etapas a seguir serão necessárias para dar acesso ao Application Cost Profiler ao seu bucket.
6. (Opcional) Escolha oPropertiesguia para o bucket e abaixoCriptografia padrão, selecione o Nome de recurso da Amazon (ARN) para seuAWS KMSchave. Esta ação exibe oAWS Key Management Serviceconsole e mostra sua chave.
7. (Opcional) Adicione a política para dar acesso ao Application Cost Profiler aoAWS KMSchave. Para obter instruções sobre como adicionar essa política, consulteDando acesso ao Application Cost Profiler a buckets S3 criptografados pelo SSE- (p. 9).

# Dando acesso ao Application Cost Profiler aos dados de uso do bucket S3

O bucket do S3 que você configura para o Application Cost Profiler para ler seus dados de uso deve ter uma política anexada para permitir que o Application Cost Profiler leia os objetos de dados de uso.

Note

Ao dar acesso ao Application Cost Profiler aos seus dados de uso, você concorda que podemos copiar temporariamente esses objetos de dados de uso para o Leste dos EUA (Norte da Virgínia)Região da AWSdurante o processamento de relatórios. Esses objetos de dados serão mantidos na região Leste dos EUA (Norte da Virgínia) até que a geração de relatórios mensal seja concluída.

Para dar acesso ao Application Cost Profiler aos dados de uso do bucket S3

1. Vá para oConsole do Amazon S3e faça login.
2. SelectBucketsNa navegação à esquerda e, em seguida, selecione seu bucket na lista.
3. Selecione oPermissõesguia, em seguida, ao lado dePolítica de bucket, escolhaEdite.
4. NoPolíticaseção, insira a seguinte política do. Substituir*<bucket-name>*pelo nome do bucket do.*<Conta da AWS>*pelo ID do seuConta 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>:*"
            }
          }
        }
      ]
    }
```

Nesta política, você está fornecendo o principal de serviço Application Cost Profiler (`application-cost-profiler.amazonaws.com`) acesso para obter dados do bucket especificado. Ele faz isso em seu nome e inclui um cabeçalho com seuConta da AWSe um ARN específico para seu intervalo de uso. Para garantir que o Application Cost Profiler esteja acessando seu bucket somente ao agir em seu nome, o`Condition`verifica esses cabeçalhos.

5. SelecioneSalve as alteraçõespara salvar sua política, anexada ao seu bucket.

Se o bucket estiver criptografado comAWS KMSchaves gerenciadas, então você deve dar acesso ao Application Cost Profiler ao seu bucket seguindo o procedimento na próxima seção.

# Dando acesso ao Application Cost Profiler a buckets S3 criptografados pelo SSE-

Se você criptografar os buckets do S3 configurados para o Application Cost Profiler (necessário para buckets de relatório) com chaves armazenadas emAWS KMS(SSE-KMS), você também deve conceder permissões ao Application Cost Profiler para descriptografá-los. Você faz isso dando acesso aoAWS KMSchaves usadas para criptografar os dados.

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

Para dar acesso ao Application Cost Profiler aoAWS KMSPara buckets do S3 criptografados pelo SSE-KMS

1. Vá para oAWS KMSconsolee faça login.
2. SelectChaves gerenciadas pelo clienteNa navegação à esquerda e, em seguida, escolha a chave que é usada para criptografar o bucket da lista.
3. SelectAlternar para visualização de políticaEm seguida, escolhaEdite.
4. NoPolíticaseção, insira a seguinte declaração de política.

```
 {
   "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. SelecioneSalve as alteraçõespara salvar sua política, anexada à sua chave.
6. Repita 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 buckets gerenciados do Application Cost Profiler (criptografados). Se você 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.

# Como criar seu relatório

Depois de cumprir opré-requisitos, você está pronto para configurar o relatórioConta da AWSe envie seus dados de uso paraAWSApplication Cost Profiler. Esta seção descreve como configurar o relatório e como enviar os dados de uso para o Application Cost Profiler.

## Configurar o relatório 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 em que o relatório é gerado.

> Note
>
> Se suas receitasConta da AWSFaz parte de umAWSorganização, você pode configurar o relatório usando a conta de gerenciamento ou uma conta de membro individual. Os relatórios configurados para contas individuais só contêm dados dessa conta. Os relatórios configurados usando a conta de gerenciamento podem incluir dados para toda a organização.
> O bucket do Amazon S3 usado para saída de relatório deve pertencer à conta que cria a configuração do relatório.

Para configurar o relatório Application Cost Profiler

1. Abra um navegador da Web e faça login noApplication Cost Profiler.
2. SelecioneComece a usar agorapara configurar ou modificar um relatório.
3. Digite umNome do relatórioeDescrição do relatórioPara o relatório.
4. Digite o nome do bucket do S3 noDigite o nome do bucket do S3e insira o prefixo S3 naDigite o prefixo do S3campo. Para obter mais informações sobre como criar buckets do S3 e fornecer permissões Application Cost Profiler, consulteConfigurar buckets do Amazon S3 para o Application Cost Profiler (p. 6).
5. Selecione as opções que você deseja que seu relatório tenha:
   - Time Frequency— Escolha se o relatório é gerado em umDiariamenteouMensalmentecadência, ouAmbos.
   - Formato de saída— Escolha o tipo de arquivo a ser criado no bucket do Amazon S3. Se escolherCSV, Application Cost Profiler cria um arquivo de texto de valores separados por vírgula com compactação gzip para os relatórios. Se escolherParquet, um arquivo Parquet é gerado para os relatórios.
6. SelecioneConfigurePara salvar a configuração do relatório.

> Note
>
> Você também pode usar oAWSApplication Cost Profilerpara configurar relatórios.

Verifique as configurações do relatório escolhendoComece a usar agorapara exibir a configuração do relatório atual.

> Note
>
> Apenas é possível configurar um único relatório. Retornar à página de configuração editará seu relatório existente.

Depois de configurar seu relatório, a ingestão de dados será ativada. Você pode integrar seus serviços ao Application Cost Profiler para fornecer dados de uso para seus recursos.

# Relatar dados de uso do locatário de seus serviços

Depois de configurar o relatório, você estará pronto para enviar dados de uso do locatário dos recursos ou serviços em sua conta. Você deve informar o Application Cost Profiler quando seu recurso estiver sendo usado para um locatário específico. Por exemplo, se o serviço aceitar chamadas de API de diferentes locatários, você registrará uma hora de início e término para cada locatário ao iniciar e finalizar uma chamada de API desse locatário. O Application Cost Profiler usa esses dados para gerar relatórios sobre o custo do seu serviço, pela quantidade de tempo gasto no trabalho para cada locatário.

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

- Preparar dados de uso de recursos— Crie tabelas que descrevem quando um recurso é usado para um locatário específico.
- Fazer upload de dados— Carregue as tabelas para um bucket do Amazon S3 que você deu permissão para acessar o Application Cost Profiler.
- Importar dados— Chame o`ImportApplicationUsage`Operação da API para permitir que o Application Cost Profiler saiba que os dados estão prontos para serem processados.

As seções a seguir descrevem cada uma dessas etapas com mais detalhes.

Tópicos



## Etapa 1: Preparando seus dados de uso de recursos

Como um recurso está sendo usado em seu serviço, você rastreia qual locatário o está usando. Registre esses dados em uma tabela que você pode carregar posteriormente para importar o Application Cost Profiler. Cada linha na tabela descreve um recurso, o locatário que está usando o recurso e os horários de início e término desse uso. Um exemplo de um recurso é uma instância do Amazon Elastic Compute Cloud (Amazon EC2) que está sendo usada.

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

Os campos que estão em uma tabela de uso de recursos estão listados na tabela a seguir.

| Campo | Descrição |
|---|---|
| ApplicationId | Identifica o aplicativo ou o produto em seu sistema que está sendo usado. Define o escopo dos metadados do locatário. |
| Tenantid | Um identificador em seu sistema para o locatário que está consumindo o recurso especificado. O Application Cost Profiler se agrega a esse nível dentro doApplicationId. |
| TenantDesc | (Opcional) Dados adicionais sobre o locatário para seus próprios relatórios adicionais. |
| UsageAccountId | A conta em que o recurso é executado (importante para contas que fazem parte de uma organização). |

| Campo | Descrição |
| --- | --- |
| StartTime | Timestamp (em milissegundos e microssegundos) da Epoch, em UTC. Indica a hora de início do período para o uso pelo locatário especificado. |
| EndTime | Timestamp (em milissegundos e microssegundos) da Epoch, em UTC. Indica a hora final do período para o uso pelo locatário especificado. |
| ResourceId | Nome de recurso da Amazon (ARN) para recurso que está sendo usado. |
| Name (Nome) | (Opcional) Como alternativa à especificação de umResourceId, é possível especificar umName (Nome)tag de recurso para atribuir custos a um conjunto de recursos (o campo deve incluir o valor que você deseja usar para oName (Nome)tag). As tags de recursos estão ativadas como parte do Relatório de custos e uso. Para obter mais informações sobre tags de recursos, consulteDetalhes de tags de recursosnoGuia do usuário do Relatório de custos e uso. |

A saída deve estar em um arquivo de valores separados por vírgulas (.csv) que inclui uma linha de cabeçalho, 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 compactado com gzip). Quando você carrega esses dados para o Application Cost Profiler, cada fatia de tempo é atribuída ao locatário associado. Neste exemplo, o relatório inclui a fatia de tempo do custo da instância do Amazon EC2 para esse locatário. Somente para instâncias do EC2, fatias que não estão associadas a um locatário específico são adicionadas a umnão atribuídoLocatário. Fatias de tempo sobrepostas são contadas várias vezes. É sua responsabilidade garantir que os dados na tabela de uso sejam precisos.

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

Por exemplo, a tabela a seguir mostra como o Application Cost Profiler calcula o uso de três locatários, ao longo de uma hora (3.600.000 milissegundos), com base nas fatias de tempo fornecidas.

| Locatário | Fatias de tempo fornecidas | Porcentagem calculada do custo por hora |
|---|---|---|
| Inquilato1 | 1.200.000 ms | 33,34% |
| Inquilato2 | 600.000 ms | 16,66% |
| <unattributed> | | 50,00% |

Neste exemplo, o Tenant1 recebe um terço da hora e o Tenant2 recebe um sexto da hora. A meia hora restante (1.800.000 ms) não é atribuída a nenhum dos clientes, o que é de 50% da hora.

Note

Atualmente, os seguintes recursos estão habilitados para o Application Cost Profiler: Instâncias do Amazon EC2, funções do Lambda, instâncias do Amazon Elastic Container Service (Amazon ECS), filas do Amazon Simple Queue Service (Amazon SQS), tópicos do Amazon Simple Notification Service (Amazon SNS) e leituras e gravações do Amazon DynamoDB.
O uso do Amazon SQS, Amazon SNS e DynamoDB não é cobrado pelo tempo, ao contrário 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 alocada para diferentes locatários, independentemente de quando as leituras ou gravações ocorreram durante a hora.

# Etapa 2: Fazer upload do uso de recursos

Depois de ter um arquivo de uso pelo locatário, carregue seu 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 um bucket do S3, consultePré-requisitos específicos do Application Cost Profiler (p. 5).

Certifique-se de 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 carregar vários arquivos de uso). Para obter informações sobre como dar acesso ao bucket, consulteDando acesso ao Application Cost Profiler aos dados de uso do bucket S3 (p. 7). Se o bucket estiver criptografado, consulteDando acesso ao Application Cost Profiler a buckets S3 criptografados pelo SSE- (p. 9).

Note

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

Carregue seus dados para o bucket do S3 como um arquivo, com uma extensão.csv (ou .csv.gzip se compactado com gzip), em intervalos de hora. Depois de carregar um novo arquivo, você deve informar o Application Cost Profiler que o enviou para que o arquivo possa ser importado para o relatório.

Note

Ao dar acesso ao Application Cost Profiler aos seus dados de uso, você concorda que podemos copiar temporariamente esses objetos de dados de uso para o Leste dos EUA (Norte da Virgínia)Região da AWSdurante o processamento de relatórios. Esses objetos de dados serão mantidos na região Leste dos EUA (Norte da Virgínia) até que a geração mensal do relatório esteja concluída.

# Etapa 3: Importando dados de uso para o Application Cost Profiler

Depois de carregar os dados de uso em um bucket do Amazon S3 ao qual o Application Cost Profiler tem acesso, informe o Application Cost Profiler que os dados existem e importá-los para o relatório final. Para isso, você pode usar o`ImportApplicationUsage`operação na API Application Cost Profiler.

Para obter informações sobreAWSAPI Application Cost Profiler, incluindo a`ImportApplicationUsage`operação, veja aAWSReferência da API Application Cost Profiler.

O exemplo a seguir mostra como chamar`ImportApplicationUsage`. Substitua o*`texto de entrada entre colchetes`*com os 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`region`parâmetro só é necessário se o bucket estiver em umRegião da AWSO que está desativado por padrão. Para obter mais informações, consulteGerenciar oRegiões da AWSnoAWSReferência geral.

O Application Cost Profiler gera um novo relatório na frequência solicitada quandoConfigurar seu relatório (p. 10), usando os dados que você importou 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 relatóriosUsando relatórios Application Cost Profiler (p. 15).

# Usando relatórios Application Cost Profiler

Depois de integrar seus dados de uso comAWSApplication Cost Profiler e estão enviando os dados por hora, o Application Cost Profiler gera automaticamente seu relatório.

Os relatórios são gerados diariamente ou mensalmente, com base na opção selecionada quandoComo configurar seu relatório (p. 10). 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 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 doAWS Organizations. |
| UsageAccountId | O ID da conta da conta com uso. |
| LineItemType | O tipo de registro. Sempre `Usage`. |
| UsageStartTime | Carimbo de data/hora (em milissegundos) de Epoch, em UTC. Indica a hora de início do período para o uso pelo locatário especificado. |
| UsageEndTime | Carimbo de data/hora (em milissegundos) de Epoch, em UTC. Indica a hora de término do período para o uso pelo locatário especificado. |
| ApplicationIdentifier | OApplicationIdespecificado nos dados de uso enviados ao Application Cost Profiler. |
| TenantiDentificador | OTenantidespecificado nos dados de uso enviados ao Application Cost Profiler. Dados sem registro nos dados de uso são coletados em`unattributed`. |
| Descrição do inquilino | O`TenantDesc`especificado nos dados de uso enviados ao Application Cost Profiler. |
| ProductCode | OAWSproduto sendo faturado (por exemplo,`AmazonEC2`). |
| UsageType | O tipo de uso que está sendo cobrado (por exemplo,`BoxUsage:c5.large`). |

| Nome da coluna | Descrição |
| --- | --- |
| Operação | A operação que está sendo cobrada (por exemplo,`RunInstances`). |
| ResourceId | O ID do recurso ou Nome de recurso da Amazon (ARN) do recurso que está sendo faturado. |
| ScaleFactor | Se um recurso estiver sobrealocado por uma hora, por exemplo, os dados de uso relatados são iguais a 2 horas em vez de 1 hora, um fator de escala será aplicado para tornar o total igual ao valor faturado real (nesse caso, 0,5). Esta coluna relata o fator de escala usado para o recurso específico para essa hora. O fator de escala é sempre maior que zero (0) e menor ou igual a 1. |
| TenantAttributionPercent | A porcentagem do uso atribuída ao locatário especificado (entre zero (0) e 1). |
| UsageAmount | A quantidade de uso atribuída ao locatário especificado. |
| CurrencyCode | A moeda em que a taxa e o custo estão (por exemplo,`USD`). |
| Rate (Taxa) | A taxa de faturamento para o uso, por unidade. |
| TenantCost | O custo total desse recurso para o locatário especificado. |
| Região | OAWSRegião do recurso. |
| Name (Nome) | Se você criou tags de recurso para seus recursos no relatório Custo e Uso, ou por meio dos dados de uso do recurso, oName (Nome)A tag é mostrada aqui. Para obter mais informações sobre tags de recurso, consulteDetalhes de tags de recursosnoGuia do usuário do relatório de custos e uso da. |

Veja a seguir um exemplo do relatório de saída de um recurso por duas 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
```

Neste exemplo, a primeira hora é alocada para`Tenant1`por metade do tempo. Uma meia hora permanece como`unattributed`. Na segunda hora, quatro inquilinos recebem todos a hora completa. Nesse caso, o

fator de escala dimensiona todos eles em 0,25, e todos eles são alocados um quarto da hora. Você pode ver o custo final no`TenantCost`coluna.

# AWSCotas e endpoints do Application Cost Profiler

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 éAWSEspecífico da região. Você pode solicitar aumentos para algumas cotas e outras cotas não podem ser aumentadas.

As seguintes tabelas listam as cotas de serviço por conta e oAWSPontos finais de região para o Application Cost Profiler.

## Cotas de serviço

| Recurso | Valor padrão | Descrição |
|---|---|---|
| Taxa de`PutReportDefinition`pedidos | 5 | O número máximo de`PutReportDefinition`Solicitações de solicitação por segundo por conta. |
| Taxa de`UpdateReportDefinition`pedidos | 5 | O número máximo de`UpdateReportDefinition`Solicitações de solicitação por segundo por conta. |
| Taxa de`GetReportDefinition`pedidos | 5 | O número máximo de`GetReportDefinition`Solicitações de solicitação por segundo por conta. |
| Taxa de`DeleteReportDefinition`pedidos | 5 | O número máximo de`DeleteReportDefinition`Solicitações de solicitação por segundo por conta. |
| Taxa de`ListReportDefinitions`pedidos | 5 | O número máximo de`ListReportDefinitions`Solicitações de solicitação por segundo por conta. |
| Taxa de`ImportApplicationUsage`pedidos | 5 | O número máximo de`ImportApplicationUsage`Solicitações de solicitação por segundo por conta. |
| Tamanho máximo do arquivo de dados de uso | 10 MB | O tamanho máximo de um arquivo de dados de uso por hora. |

# Service endpoints (Endpoints de serviço)

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

- US East (N. Virginia) – `application-cost-profiler.us-east-1.amazonaws.com`

# Segurança emAWSApplication Cost Profil

A segurança da nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se 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, consulteServiços da AWS no escopo pelo programa de conformidade.
- Segurança da 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 usarAWSApplication Cost Profiler. Ela mostra como configurar o Application Cost Profiler para atender aos objetivos de segurança e conformidade. Você também aprende a usar outrosAWSServiços da que ajudam a monitorar e proteger os recursos do Application Cost Profiler.

Índice



# Proteção de dados noAWSApplication Cost Profil

OAWS Modelo de responsabilidade compartilhadaAplica-se à proteção de dados noAWSApplication Cost Profiler. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Esse conteúdo inclui as tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que você usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja as credenciais da conta da Conta da AWS e configure as contas de usuário individuais com o 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 uma autenticação multifator (MFA) com cada conta.

- Use SSL/TLS para se comunicar com os recursos da AWS. Recomendamos TLS 1.2 ou posterior.
- Configure o registro em log das atividades da API e do usuário com o AWS CloudTrail.
- Use as soluções de criptografia da AWS, juntamente com todos os controles de segurança padrão nos serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados pessoais armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por meio de uma interface de linha de comando ou uma API, use um endpoint do FIPS. Para obter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que você nunca coloque informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Name (Nome). Isso inclui quando você trabalha com Application Cost Profiler ou outrosAWSserviços usando o console, a API,AWS CLI, ouAWSSDKs. Quaisquer dados inseridos em marcações ou campos de formato livre usados para nomes podem ser usados para logs de cobrança ou diagnóstico. Se fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

## Criptografia em repouso

AWSO 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 buckets do Amazon S3 que você fornece, você deve criptografar o bucket de relatório e criptografar o bucket de dados de uso e dar acesso ao Application Cost Profiler. Para obter mais informações, consulte Configurar buckets do Amazon S3 para o Application Cost Profiler (p. 6).

## Criptografia em trânsito

AWSO Application Cost Profiler usa Transport Layer Security (TLS) e criptografia no lado do cliente para a criptografia em trânsito. A comunicação com o Application Cost Profiler é sempre feita por HTTPS para que seus dados sejam sempre criptografados em trânsito. Essa criptografia é configurada por padrão quando você usa Application Cost Profiler.

# Identity and Access Management para oAWSCriador de custos do aplicativo

O AWS Identity and Access Management (IAM) é um serviço da AWS service (Serviço da AWS) que ajuda a controlar o acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode serautenticada(assinado) eautorizada(tem permissões) para usar os recursos do Application Cost Profiler. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

Tópicos

# Público

Como você usa oAWS Identity and Access ManagementO (IAM) varia dependendo do trabalho que é realizado no Application Cost Profiler.

Usuário do serviço— se você usar o serviço Application Cost Profiler para fazer sua tarefa, o administrador fornecerá as credenciais e as permissões de que você precisa. 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 você não conseguir acessar um recurso no Application Cost Profiler, consulteSolução de problemasAWSIdentidade e acesso ao Application Cost Pro (p. 31).

Administrador de serviços— se você for o responsável pelos recursos do Application Cost Profiler em sua empresa, você provavelmente terá acesso total ao Application Cost Profiler. Seu trabalho é determinar quais recursos do Application Cost Profiler seus funcionários devem acessar. Assim, é necessário enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os conceitos básicos do IAM. Para saber mais sobre como a empresa pode usar o IAM com o Application Cost Profiler, consulteComoAWSApplication Cost Profiler (p. 26).

Administrador do IAM— se você é um administrador do IAM, talvez queira saber detalhes sobre como pode escrever políticas para gerenciar o acesso ao Application Cost Profiler. Para visualizar exemplos de políticas baseadas em identidade do Application Cost Profiler que podem ser usadas no IAM, consulteAWSExemplos de políticas baseadas em identidade do Application Cost Profiler (p. 28).

# Autenticar com identidades

A autenticação é a forma como você faz login na AWS usando suas credenciais de identidade. Para obter mais informações sobre como fazer login usando o AWS Management Console, consulte Login no AWS Management Console como usuário do IAM ou usuário root no Manual do usuário do IAM.

É necessário estar autenticado (conectado à AWS) como o usuário root da Conta da AWS ou um usuário do IAM, ou ainda assumindo uma função do IAM. Também é possível usar a autenticação de logon único da sua empresa ou até mesmo fazer login usando o Google ou o Facebook. Nesses casos, o administrador configurou anteriormente federação de identidades usando funções do IAM. Ao acessar a AWS usando credenciais de outra empresa, você estará assumindo uma função indiretamente.

Para fazer login diretamente no AWS Management Console, use sua senha com o e-mail do usuário root ou seu nome de usuário do IAM. É possível acessar a AWS de maneira programática usando chaves de acesso do seu usuário root ou dos usuários do IAM. AWS fornece ferramentas SDK e de linha de comando para assinar de forma criptográfica a sua solicitação usando suas credenciais. Se você não utilizar as ferramentas AWS, você deverá assinar a solicitação por conta própria. Faça isso usando o Signature versão 4, um protocolo para autenticação de solicitações de API de entrada. Para obter mais informações sobre solicitações de autenticação, consulte Processo de assinatura do Signature Version 4 na Referência geral da AWS.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte Uso da autenticação multifator (MFA) AWS no Guia do usuário do IAM.

## Usuário root da Conta da AWS

Ao criar uma Conta da AWS, você começa com uma única identidade de login que tenha acesso total a todos os recursos e Serviços da AWS na conta. Essa identidade é denominada Conta da AWSusuário root da  e é acessada pelo login com o endereço de e-mail e a senha que você usou para criar a conta. Recomendamos que não use o usuário raiz para suas tarefas do dia a dia, nem mesmo as administrativas.

Em vez disso, siga as práticas recomendadas para o uso do usuário root somente a fim de criar seu primeiro usuário do IAM. Depois, armazene as credenciais do usuário raiz com segurança e use-as para executar somente algumas tarefas de gerenciamento de contas e de serviços.

## Grupos e usuários do IAM

Um usuário do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas para uma única pessoa ou aplicação. Um usuário do IAM pode ter credenciais de longo prazo, como um nome de usuário e uma senha ou um conjunto de chaves de acesso. Para saber como gerar chaves de acesso, consulte Gerenciar chaves de acesso para usuários do IAM no Manual do usuário do IAM. Ao gerar chaves de acesso para um usuário do IAM, visualize e salve o par de chaves de maneira segura. Não será possível recuperar a chave de acesso secreta futuramente. Em vez disso, você deverá gerar outro par de chaves de acesso.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. 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 IAMAdmins e atribuir a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de funções. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas uma função pode ser assumida por qualquer pessoa que precisar dela. Os usuários têm credenciais permanentes de longo prazo, mas as funções fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de uma função) no Manual do usuário do IAM.

## Funções do IAM

Uma função do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas. Ela é semelhante a um usuário do IAM, mas não está associada a uma pessoa específica. É possível assumir temporariamente uma função do IAM no AWS Management Console alternando funções. É possível assumir uma função chamando uma operação de API da AWS CLI ou da AWS, ou usando um URL personalizado. Para mais informações sobre métodos para o uso de funções, consulte Usar funções do IAM no Manual do usuário do IAM.

As funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Permissões temporárias para usuários do IAM: um usuário do IAM pode assumir uma função do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso de usuário federado: em vez de criar um usuário do IAM, você poderá usar identidades de usuários existentes no AWS Directory Service, em seu diretório de usuários corporativos ou em um provedor de identidades da Web. Estes são conhecidos como usuários federados. A AWS atribui uma função a um usuário federado quando o acesso é solicitado por meio de um provedor de identidades. Para obter mais informações sobre usuários federados, consulte Usuários federados e funções no Manual do usuário do IAM.
- Acesso entre contas: é possível usar uma função do IAM para permitir que alguém (um principal confiável) em outra conta acesse recursos em sua conta. As funções são a principal forma de conceder acesso entre contas. No entanto, alguns Serviços da AWS permitem que você anexe uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recurso para acesso entre contas, consulte Como as funções do IAM diferem das políticas baseadas em recurso no Manual do usuário do IAM.
- 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 aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando uma função de serviço ou uma função vinculada ao serviço.
  - Permissões de principal: ao usar um usuário ou uma função do IAM para executar ações na AWS, você é considerado um principal. As políticas concedem permissões a uma entidade principal. Quando

você usa alguns serviços, pode executar uma ação que, em seguida, aciona outra ação em outro serviço. Nesse caso, você deve ter permissões para executar ambas as ações. Para ver se uma ação requer ações dependentes adicionais em uma política, consulteAções, recursos e chaves de condição para oAWSserviçosnoReferência de autorização do serviço.

- Função de serviço: uma função de serviço é uma função do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir uma função de serviço do IAM. Para obter mais informações, consulte Criar uma função para delegar permissões a AWS service (Serviço da AWS) no Guia do usuário do IAM.
- Função vinculada a serviço: uma função vinculada a serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode assumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em sua conta do IAM e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas ao serviço.

- Aplicações em execução no Amazon EC2: é possível usar uma função do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso do que armazenar chaves de acesso na instância do EC2. Para atribuir uma função da AWS a uma instância do EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado à instância. Um perfil de instância contém a função e permite que programas que estão em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar uma função do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Manual do usuário do IAM.

Para saber se deseja usar as funções do IAM, consulte Quando criar uma função do IAM (em vez de um usuário) no Manual do usuário do IAM.

# Gerenciamento do acesso usando políticas

Você controla o acesso na AWS criando e anexando políticas às identidades do IAM ou aos recursos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou recurso, define suas permissões. Você pode fazer login como o usuário raiz ou um usuário do IAM ou assumir uma função do IAM. Quando você faz uma solicitação, a AWS avalia as políticas relacionadas baseadas em identidade ou baseadas em recursos. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas são armazenadas na AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Manual do usuário do IAM.

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

Cada entidade do IAM (usuário ou função) começa sem permissões. Em outras palavras, por padrão, os usuários não podem fazer nada, nem mesmo alterar sua própria senha. Para dar permissão a um usuário para fazer algo, um administrador deve anexar uma política de permissões ao usuário. Ou o administrador pode adicionar o usuário a um grupo que tenha as permissões pretendidas. Quando um administrador concede permissões a um grupo, todos os usuários desse grupo recebem essas permissões.

As políticas do IAM definem permissões para uma ação, independentemente do método usado para executar 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 funções do AWS Management Console, da AWS CLI ou da API da AWS.

## Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou função do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber

como criar uma política baseada em identidade, consulte Criar políticas do IAM no Manual do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou função. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e funções na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Manual do usuário do IAM.

## Políticas baseadas em recursos

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de função do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com 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 um principal em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, funções, usuários federados ou Serviços da AWS.

Políticas baseadas em recursos são políticas em linha que estão localizadas nesse serviço. Não é possível usar as políticas gerenciadas da AWS do IAM em uma política baseada em recursos.

## Listas de controle de acesso (ACLs)

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

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

## Outros tipos de política

A AWS oferece suporte a tipos de política 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 o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou função do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade da entidade e seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou a função 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 identidades do IAM no Manual do usuário do IAM.
- Políticas de controle de serviço (SCPs): SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (UO) no AWS Organizations. O AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS pertencentes à sua empresa. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades em contas-membro, incluindo cadaConta da AWSusuário raiz. Para obter mais informações sobre o Organizations e SCPs, consulte Como os SCPs funcionam no Manual do usuário do AWS Organizations.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para uma função ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou da função e

das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recurso. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Manual do usuário do IAM.

## Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como a AWS determina se deve permitir uma solicitação quando há vários tipos de política envolvidos, consulte Lógica da avaliação de políticas no Manual do usuário do IAM.

# ComoAWSApplication Cost Profiler

Antes de usar o IAM para gerenciar o acesso ao Application Cost Profiler, você deve entender quais recursos do IAM estão disponíveis para uso com o Application Cost Profiler. Para obter uma visão de alto nível de como Application Cost Profiler e outrosAWSOs serviços da funcionam com o IAM, consulteAWSServiços compatíveis com o IAMnoManual do usuário do IAM.

Tópicos



## Políticas baseadas em identidade do Application Cost Profiler

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, além das condições sob as quais as ações são permitidas ou negadas. O Application Cost Profiler suporta ações específicas. Para conhecer todos os elementos usados em uma política JSON, consulte Referência de elementos de política JSON do IAM no Manual do usuário do IAM.

### Ações

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

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

Inclua 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 a alguém permissão para visualizar os detalhes da definição do relatório Application Cost Profiler, inclua a`application-cost-profiler:GetReportDefinitionação` em sua política. 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 o seguinte.

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

```
    "application-cost-profiler:GetReportDefinition"
```

A seguir estão as ações disponíveis no Application Cost Profiler. Cada um permite a ação da API com o mesmo nome. Para obter mais informações sobre o Application Cost Profiler API, consulteAWSReferência do Application Cost Profiler.

- `application-cost-profiler:ListReportDefinitions`— Permite listar a definição do relatório para oAWSConta, se houver.
- `application-cost-profiler:GetReportDefinition`— Permite obter os detalhes da definição do relatório do Application Cost Profiler.
- `application-cost-profiler:PutReportDefinition`— Permite criar uma nova definição de relatório.
- `application-cost-profiler:UpdateReportDefinition`— Permite atualizar uma definição de relatório.
- `application-cost-profiler:DeleteReportDefinition`— Permite excluir um relatório (disponível somente por meio da API Application Cost Profiler).
- `application-cost-profiler:ImportApplicationUsage`— Permite solicitar dados de uso da importação do Application Cost Profiler de um bucket do Amazon S3 especificado.

### Recursos

O Application Cost Profiler não oferece suporte à especificação de nomes de recurso da Amazon (ARNs) em uma política.

### Chaves de condição

O Application Cost Profiler não fornece nenhuma chave de condição específica ao serviço, mas oferece suporte ao uso de algumas chaves de condição globais. Para ver todas as chaves de condição globais da AWS, consulte Chaves de contexto de condição globais da AWS no Manual do usuário do IAM.

### Exemplos

Para visualizar exemplos de políticas baseadas em identidade do Application Cost Profiler, consulteAWSExemplos de políticas baseadas em identidade do Application Cost Profiler (p. 28).

## Políticas baseadas em recurso Application Cost Profiler

O Application Cost Profiler não oferece suporte a políticas baseadas em recurso.

## Autorização baseada em tags Application Cost Profiler

O Application Cost Profiler não oferece suporte à marcação de recursos nem ao controle de acesso com base em tags.

## Funções IAM

Uma função do IAM é uma entidade dentro da sua AWS conta da que tem permissões específicas.

### Usar credenciais temporárias com o Application Cost Pro

É possível usar credenciais temporárias para fazer login com federação, assumir uma função do IAM ou assumir uma função entre contas. Você obtém credenciais de segurança temporárias chamandoAWS STSOperações de API, comoAssumeRoleouGetFederationFicha.

Application Cost Profiler oferece suporte ao uso de credenciais

### Funções vinculadas ao serviço

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

Application Cost Profiler não oferece suporte a funções vinculadas ao serviço.

### Funções de serviço

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

Application Cost Profiler não oferece suporte às funções de serviço.

# AWSExemplos de políticas baseadas em identidade do Application Cost Profiler

Por padrão,AWS Identity and Access ManagementUsuários e funções do (IAM) não têm permissões para criar ou modificarAWSRecursos do Application Cost Profiler Eles também não podem executar tarefas usando oAWS Management Console,AWS Command Line Interface(AWS CLI), ouAWSAPI. Um administrador do IAM deve criar políticas do IAM que concedam aos usuários e funções permissão para executar as operações de API específicas de que precisam. O administrador deve anexar essas políticas aos usuários ou grupos do IAM que exigem essas permissões.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documentos de política JSON, consulte Criar políticas na guia JSON no Manual do usuário do IAM.

Tópicos



## Práticas recomendadas de políticas

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

- Comece a usar oAWSpolíticas gerenciadas— Para começar a usar o Application Cost Profiler rapidamente, useAWSPolíticas gerenciadas pela para conceder aos funcionários as permissões de que precisam. Essas políticas já estão disponíveis em sua conta e são mantidas e atualizadas pela AWS. Para obter mais informações, consulte Começar a usar permissões com políticas gerenciadas da AWS no Manual do usuário do IAM.
- Conceder privilégio mínimo: ao criar políticas personalizadas, conceda apenas as permissões necessárias para executar uma tarefa. Comece com um conjunto mínimo de permissões e conceda permissões adicionais conforme necessário. Fazer isso é mais seguro do que começar com permissões

que são muito lenientes e tentar restringi-las superiormente. Para obter mais informações, consulte Conceder privilégio mínimo no Manual do usuário do IAM.

- Habilitar MFA para operações confidenciais: para aumentar a segurança, exija que os usuários do IAM usem Multi-Factor Authentication (MFA) para acessar recursos ou operações de API confidenciais. Para obter mais informações, consulte Usar autenticação multifator (MFA) AWS no Guia do usuário do IAM.
- Usar condições de política para segurança adicional: na medida do possível, defina as condições sob as quais suas políticas baseadas em identidade permitem o acesso a um recurso. Por exemplo, você pode gravar condições para especificar um intervalo de endereços IP permitidos do qual a solicitação deve partir. Você também pode escrever condições para permitir somente solicitações em uma data especificada ou período ou para exigir o uso de SSL ou MFA. Para obter mais informações, consulteElementos de política JSON do IAM: CondiçãonoManual do usuário do IAM.

## Usar o console Application Cost Profiler

Para acessar oAWSConsole Application Cost Profiler, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes dos recursos do Application Cost Profiler noAWSconta. Se você criar uma política baseada em identidade que seja mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou funções do IAM) com essa política.

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

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

Por exemplo, você pode criar a política a seguir para seus usuários somente 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 usuário do IAM:

Não é necessário conceder permissões mínimas do console para usuários que fazem chamadas somente à AWS CLI ou à API do AWS. Em vez disso, permita o acesso somente às ações que correspondem à operação da API que você está tentando executar.

## Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou de forma programática usando a AWS CLI ou a API da 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": "*"
        }
    ]
}
```

## Acesso a um bucket do Amazon S3

Neste exemplo, você deseja conceder a um usuário do IAM noAWSAcesso à conta da para um de 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 um exemplo de demonstração que concede permissões aos usuários e testa-as usando o console, consulteUm exemplo de demonstração: Usar políticas de usuário para controlar o acesso ao 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 problemasAWSIdentidade e acesso ao Application Cost Pro

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com oAWSApplication Cost Profiler eAWS Identity and Access Management(IAM).

Tópicos

- Não tenho autorização para executar uma ação no Application Cost Profiler (p. 31)
- Não tenho autorização para executar o IAM:PassRole (p. 31)
- Quero visualizar minhas chaves de acesso (p. 32)
- Sou administrador e quero permitir que outros usuários tenham acesso ao Application Cost Profiler (p. 32)
- Quero permitir que as pessoas fora do meuAWSConta para acessar os recursos do My Application Cost Profiler (p. 32)

## Não tenho autorização para executar uma ação no Application Cost Profiler

Se o AWS Management Console informar que você não está autorizado a executar uma ação, você deverá entrar em contato com o administrador para obter assistência. O administrador é a pessoa que forneceu a você o seu nome de usuário e senha.

O exemplo a seguir ocorre quando o`mateojackson`O usuário do IAM tenta usar o console para visualizar detalhes do relatório 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
```

Neste caso, Mateo pede ao administrador para atualizar suas políticas a fim de conceder a ele o acesso ao recurso de definição de relatório usando a`application-cost-profiler:ListReportDefinitions`Ação .

## Não tenho autorização para executar o IAM:PassRole

Se você receber uma mensagem de erro informando que você não está autorizado a executar a ação `iam:PassRole`, entre em contato com o administrador para obter assistência. O administrador é a pessoa

que forneceu a você o seu nome de usuário e senha. Peça a essa pessoa para atualizar suas políticas para permitir que você passe uma função para o Application Cost Profiler.

AlgunsServiços da AWSPara permitir que você passe uma função existente para o serviço, em vez de criar uma nova função de serviço ou função vinculada ao serviço. Para fazer isso, um usuário deve ter permissões para passar a função para o serviço.

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

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

Neste caso, Mary pede ao administrador para atualizar suas políticas para permitir que ela execute a ação `iam:PassRole`.

## Quero visualizar minhas chaves de acesso

Depois de criar suas chaves de acesso de usuário do IAM, é possível visualizar seu ID da chave de acesso a qualquer momento. No entanto, você não pode visualizar sua chave de acesso secreta novamente. Se você perder sua chave secreta, crie um novo par de chaves de acesso.

As chaves de acesso consistem em duas partes: um ID de chave de acesso (por exemplo, `AKIAIOSFODNN7EXAMPLE`) e uma chave de acesso secreta (por exemplo, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Como um nome de usuário e uma senha, você deve usar o ID da chave de acesso e a chave de acesso secreta em conjunto para autenticar suas solicitações. Gerencie suas chaves de acesso de forma tão segura quanto você gerencia seu nome de usuário e sua senha.

> **Important**
>
> Não forneça as chaves de acesso a terceiros, mesmo que seja para ajudar a encontrar o ID de usuário canônico. Ao fazer isso, você pode dar a alguém acesso permanente à sua conta.

Ao criar um par de chaves de acesso, você é solicitado a guardar o ID da chave de acesso e a chave de acesso secreta em um local seguro. A chave de acesso secreta só está disponível no momento em que é criada. Se você perder sua chave de acesso secreta, será necessário adicionar novas chaves de acesso para seu usuário do IAM. Você pode ter no máximo duas chaves de acesso. Se você já tiver duas, você deverá excluir um par de chaves para poder criar um novo. Para visualizar as instruções, consulte Gerenciar chaves de acesso no Manual do usuário do IAM.

## Sou administrador e quero permitir que outros usuários tenham acesso ao Application Cost Profiler

Para permitir que outros usuários acessem o Application Cost Profiler, é necessário criar uma entidade do IAM (usuário ou função) para a pessoa ou a aplicação que precisa do acesso. Elas usarão as credenciais dessa entidade para acessar a AWS. Você deve anexar uma política à entidade que concede a eles as permissões corretas no Application Cost Profiler.

Para começar a usar imediatamente, consulte Criar os primeiros usuário e grupo delegados do IAM no Manual do usuário do IAM.

## Quero permitir que as pessoas fora do meuAWSConta para acessar os recursos do My Application Cost Profiler

Você pode criar uma função 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 a função. 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 o seguinte:

- Para saber se o Application Cost Profiler oferece suporte a esses recursos, consulteComoAWSApplication Cost Profiler (p. 26).
- Para saber como conceder acesso a seus recursos em todas as Contas da AWS pertencentes a você, consulte Fornecimento de acesso a um usuário do IAM em outra Conta da AWS pertencente a você no Guia de usuário do IAM.
- Para saber como conceder acesso a seus recursos para terceiros Contas da AWS, consulte Fornecimento de acesso a Contas da AWS pertencentes a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Manual do usuário do IAM.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Como as funções do IAM diferem de políticas baseadas em recursos no Manual do usuário do IAM.

# Validação de conformidade doAWSAplicativo Cost Profiler

Auditores terceirizados avaliam a segurança e a conformidade dos Serviços da AWS como parte de vários programas de conformidade da AWS, p. ex., SOC, PCI, FedRAMP e HIPAA.

Para saber se Application Cost Profiler ou outroServiços da AWSda estão no escopo de programas de conformidade específicos, consulteAWSServiços da no escopo pelo programa de conformidade. Para obter informações gerais, consulte Programas de conformidade da AWS.

Você pode fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Downloading Reports in AWS Artifact.

Sua responsabilidade de conformidade ao usar o Serviços da AWS é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes recursos para ajudar com a conformidade:

- Guias de referência rápida de conformidade e segurança: esses guias de implantação abordam as considerações de arquitetura e fornecem etapas para implantação de ambientes de lista de referência na AWS concentrados em conformidade e segurança.
- Whitepaper Architecting for HIPAA Security and Compliance (Elaboração de arquitetura para segurança e conformidade com HIPAA): esse whitepaper descreve como as empresas podem usar a AWS para criar aplicações adequadas aos padrões HIPAA.

  Note

  Nem todos os Serviços da AWS são aptos aos padrões HIPAA. Para mais informações, consulte a Referência dos serviços qualificados pela HIPAA.
- Recursos de conformidade da AWS: essa coleção de manuais e guias pode ser aplicada a seu setor e local.
- Avaliar recursos com regras no AWS Config Developer Guide (Guia do desenvolvedor do CCI): o serviço AWS Config avalia como as configurações de recursos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub: esse AWS service (Serviço da AWS) fornece uma visão abrangente do estado de sua segurança na AWS que ajuda você a conferir sua conformidade com padrões e práticas recomendadas de segurança do setor.

- AWS Audit Manager: esse AWS service (Serviço da AWS) ajuda a auditar continuamente seu uso da AWS para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

# Resiliência noAWSApplication Cost Profil

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, altas taxas de transferência e redes altamente redundantes. Com as zonas de disponibilidade, você pode 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 data center tradicionais.

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

# Segurança da infraestrutura noAWSApplication Cost Profil

Como um serviço gerenciado, o Application Cost Profiler é protegido peloAWSprocedimentos de segurança de rede global da descritos noAmazon Web Services: Visão geral dos processos de segurançawhitepaper.

Você usaAWSPublicadas chamadas de API para acessar o Application Cost Profiler pela rede. Os clientes devem oferecer suporte a Transport Layer Security (TLS) 1.0 ou posterior. Recomendamos TLS 1.2 ou posterior. Os clientes também devem ter suporte a conjuntos de criptografia com perfect forward secrecy (PFS) como Ephemeral Diffie-Hellman (DHE) ou Ephemeral Elliptic Curve Diffie-Hellman (ECDHE). A maioria dos sistemas modernos como Java 7 e versões posteriores oferece suporte a esses modos.

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

# Monitoramento de eventos do Application Cost Profiler no

Você pode usar o Amazon EventBridge para automatizar seuAWSServiços e responda automaticamente aos eventos do sistema, como problemas de disponibilidade do aplicativo 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, consulteManual do usuário do Amazon EventBridge.

Você pode monitorarAWSEventos do Application Cost Profiler no EventBridge. O EventBridge encaminha esses dados para destinos comoAWS Lambdae 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 noAWSrecursos da AWS.

## Monitore a geração de relatórios com EventBridge

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

Para monitorar a geração de relatórios

1. Faça login noAWSUsando uma conta que tenha permissões para usar o EventBridge e Application Cost Profiler.
2. Abra o console do Amazon EventBridge emhttps://console.aws.amazon.com/artifact/.
3. Selecione Criar regra.
4. Informe um Name (Nome) para a regra e, opcionalmente, uma descrição.

   Uma regra não pode ter o mesmo nome que outra regra na mesma Região da AWS e no mesmo barramento de eventos.
5. Em Define pattern (Definir padrão), selecione Event pattern (Padrão de evento).
6. Em Event matching pattern (Padrão de correspondência de eventos), escolha Custom pattern (Padrão personalizado).
7. para oPadrão de evento, adicione o padrão a seguir e, em seguida, escolhaSalvar.

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

8. Na seção Select event bus (Selecionar barramento de eventos), escolha o barramento de eventos a ser usado. Se você não criou um barramento de eventos personalizado, escolhaAWSBarramento de eventos padrão.

   Confirme issoHabilite a regra no barramento de eventos selecionadoestá ativado.
9. para oSelecionar alvos, escolha oAWSServiço que você deseja agir quando o EventBridge detecta um evento do tipo selecionado.

10. Os campos exibidos variam de acordo com o serviço escolhido. Insira informações específicas para o tipo de destino, conforme necessário.
11. Para muitos tipos de destino, o Eventbridge precisa de permissões para enviar eventos ao destino. Nesses casos, o EventBridge pode criar aAWS Identity and Access ManagementFunção (IAM) que é necessária para sua função ser executada.

    - Para criar uma função do IAM automaticamente, escolha Create a new role for this specific resource (Criar nova função para este recurso específico).
    - Para usar uma função do IAM que você criou anteriormente, escolha Use existing role (Usar função existente)
12. para oPolítica de repetição e fila de mensagens mortas, emPolítica de repetição, insira o seguinte:

    1. para oIdade máxima do evento, insira um valor entre um minuto (00:01) e 24 horas (24:00).
    2. Em Retry attempts (Tentativas de repetição), insira um número entre 0 e 185.
13. para oFila de mensagens mortas, SELECTNenhumPara não usar uma dead-letter queue do. O EventBridge envia eventos que correspondem a essa regra para a fila de mensagens mortas se eles não forem entregues com êxito ao destino. Para usar uma fila de letras mortas ou para saber mais sobre elas, consulteUsar filas de mensagens mortasnoManual do usuário do Amazon EventBridge.
14. (Opcional) Selecione Add target (Adicionar destino) para adicionar outro destino a essa regra.
15. (Opcional) Insira uma ou mais tags para a regra. Para obter mais informações, consulteTags Amazon EventBridgenoManual do usuário do Amazon EventBridge.
16. Escolha Create (Criar).

# Exemplo de um evento gerado por relatório

Este evento informa quando um relatório é gerado e pronto para você recuperar. O`message`O campo fornece o bucket do Amazon Simple Storage Service (Amazon S3) e a chave do objeto do Amazon S3 no qual o relatório é 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 doAWSApplication Cost Profiler.

| update-history-change | update-history-description | update-history-date |
| --- | --- | --- |
| Atualizações para exemplos de políticas de bucket do S3 (p. 37) | Atualização somente de documentação dos exemplos da política do bucket do S3. Para obter mais informações, consulteConfigurar os buckets do Amazon S3 do Application Cost Profiler. | 6 de dezembro de 2021 |
| Disponibilidade geral (p. 37) | O lançamento público inicial do Application Cost Profiler. | 13 de maio de 2021 |

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.