Série de Certificação GCP: 5.2 Gerenciando contas de serviço

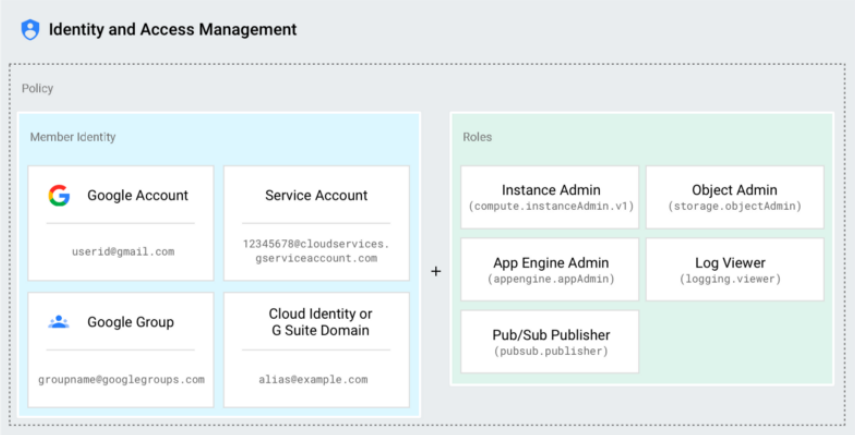
Prashanta Paudel

14 de novembro de 2018 · 26 min de leitura

visão global

Esta página descreve os conceitos básicos do Cloud Identity and Access Management.

O Google Cloud Platform (GCP) oferece o Cloud IAM, que permite gerenciar o controle de acesso definindo ***quem* (identidade) tem *qual acesso* (função) para *qual* recurso.**



https://cloud.google.com/iam/docs/overview

Com o Cloud IAM, você pode conceder acesso granular a recursos específicos do GCP e impedir o acesso indesejado a outros recursos. O Cloud IAM permite que você adote o princípio de segurança de menor privilégio, para conceder apenas o acesso necessário aos seus recursos.

Conceitos relacionados à identidade

No Cloud IAM, você concede acesso aos **membros** . Os membros podem ser dos seguintes tipos:

- conta do Google
- Conta de serviço
- Grupo do Google
- Domínio do G Suite
- Domínio do Cloud Identity

conta do Google

Uma conta do Google representa um desenvolvedor, um administrador ou qualquer outra pessoa que interage com o GCP. Qualquer endereço de e-mail associado a uma conta do Google pode ser uma identidade, incluindo gmail.com ou outros domínios. Novos usuários podem se inscrever em uma conta do Google acessando a página de inscrição da Conta do Google .

Conta de serviço

Uma conta de serviço é uma conta que pertence ao seu aplicativo em vez de a um usuário final individual. Quando você executa o código hospedado no GCP, especifica a conta na qual o código deve ser executado. Você pode criar quantas contas de serviço forem necessárias para representar os diferentes componentes lógicos de seu aplicativo. Para obter mais informações sobre o uso de uma conta de serviço no seu aplicativo, consulte Introdução à autenticação .

Grupo do Google

Um grupo do Google é uma coleção nomeada de contas do Google e contas de serviço. Cada grupo tem um endereço de e-mail exclusivo associado ao grupo. Você pode encontrar o endereço de e-mail associado a um grupo do Google clicando em **Sobre** na página inicial de qualquer grupo do Google. Para mais informações sobre os grupos do Google, consulte a página inicial dos grupos do Google .

Os grupos do Google são uma forma conveniente de aplicar uma política de acesso a uma coleção de usuários. Você pode conceder e

alterar controles de acesso para um grupo inteiro de uma só vez, em vez de conceder ou alterar controles de acesso, um por um, para usuários individuais ou contas de serviço. Você também pode adicionar membros e remover membros de um grupo do Google com facilidade, em vez de atualizar uma política do Cloud IAM para adicionar ou remover usuários.

Observe que os grupos do Google não têm credenciais de login e você não pode usar grupos do Google para estabelecer identidade para fazer uma solicitação para acessar um recurso.

Domínio do G Suite

O domínio do G Suite representa um grupo virtual de todas as contas do Google que foram criadas na conta do G Suite de uma organização . Os domínios do G Suite representam o nome de domínio da Internet da sua organização (como *example.com*) e, quando você adiciona um usuário ao seu domínio do G Suite, uma nova Conta do Google é criada para o usuário dentro desse grupo virtual (como *username@example.com*).

Como os grupos do Google, os domínios do G Suite não podem ser usados para estabelecer identidade, mas permitem o gerenciamento conveniente de permissões.

Domínio do Cloud Identity

Um domínio do Cloud Identity é como um domínio do G Suite, pois representa um grupo virtual de todas as contas do Google em uma organização. No entanto, os usuários do domínio do Cloud Identity não têm acesso aos aplicativos e recursos do G Suite. Para mais informações, consulte Sobre o Cloud Identity .

allAuthenticatedUsers

Este é um identificador especial que representa qualquer pessoa autenticada com uma Conta do Google ou uma conta de serviço. Os usuários que não são autenticados, como visitantes anônimos, não estão incluídos.

todos os usuários

Este é um identificador especial que representa qualquer pessoa que esteja na Internet, incluindo usuários autenticados e não autenticados. Observe que algumas APIs do GCP exigem autenticação de qualquer usuário que acesse o serviço e, nesses casos, allUsers implicará apenas autorização para todos os usuários autenticados.

Conceitos relacionados ao gerenciamento de acesso

Quando um membro autenticado tenta fazer uma solicitação, o Cloud IAM toma uma decisão de autorização sobre se o membro tem permissão para executar a operação em um recurso.

Esta seção descreve as entidades e conceitos envolvidos no processo de autorização.

Recurso

Você pode conceder acesso aos usuários para um recurso do GCP. Alguns exemplos de recursos são projetos, instâncias do Compute Engine e intervalos do Cloud Storage.

Alguns serviços, como o Cloud Pub / Sub e o Compute Engine, dão suporte a permissões do Cloud IAM com uma granularidade melhor do que o nível do projeto. Por exemplo, você pode conceder a `pubsub.subscriber` função a um usuário para um determinado tópico do Cloud Pub / Sub ou pode conceder a `compute.instanceAdmin` função a um usuário para uma instância específica do Compute Engine.

Em outros casos, você pode conceder permissões do Cloud IAM no nível do projeto. As permissões são então herdadas por todos os recursos dentro desse projeto. Por exemplo, para conceder acesso a um intervalo do Cloud Storage, você deve conceder o acesso ao projeto que contém o intervalo. Para obter informações sobre quais funções podem ser concedidas em quais recursos, consulte Noções básicas sobre funções .

Permissões

Permissões determinam quais operações são permitidas em um recurso. No mundo do Cloud IAM, as permissões são representadas na

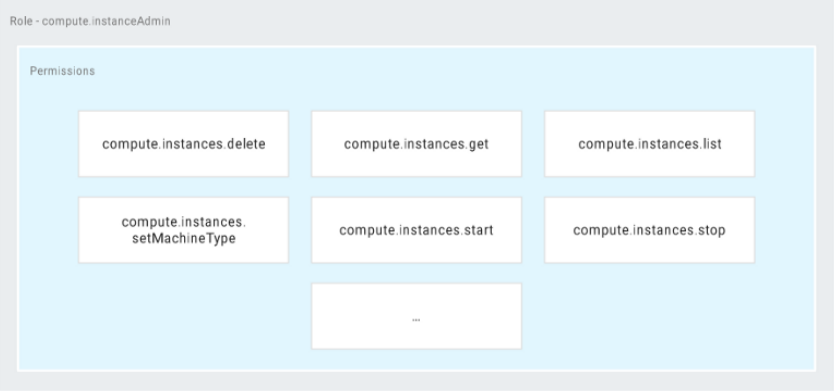
forma de `<service>.<resource>.<verb>` , por exemplo `pubsub.subscriptions.consume` .

As permissões geralmente, mas nem sempre, correspondem a 1: 1 com os métodos REST. Ou seja, cada serviço do GCP tem um conjunto associado de permissões para cada método REST que ele expõe. O chamador desse método precisa dessas permissões para chamar esse método. Por exemplo, o chamador `Publisher.Publish()` precisa da `pubsub.topics.publish` permissão.

Você não atribui permissões aos usuários diretamente. Em vez disso, você atribui a eles uma **função que** contém uma ou mais permissões.

Papéis

Uma função é uma coleção de permissões. Você não pode atribuir uma permissão ao usuário diretamente; em vez disso, você concede a eles um papel. Quando você concede uma função a um usuário, concede a eles todas as permissões que a função contém.



Existem três tipos de funções no Cloud IAM:

- **Papéis primitivos** : as funções historicamente disponíveis no Console do Google Cloud Platform continuarão funcionando. Estas são as funções de **proprietário** , **editor** e **visualizador** .
- **Funções predefinidas** : **funções** predefinidas são as funções do Cloud IAM que fornecem um controle de acesso mais refinado do que as funções primitivas. Por exemplo, a função predefinida **Pub**

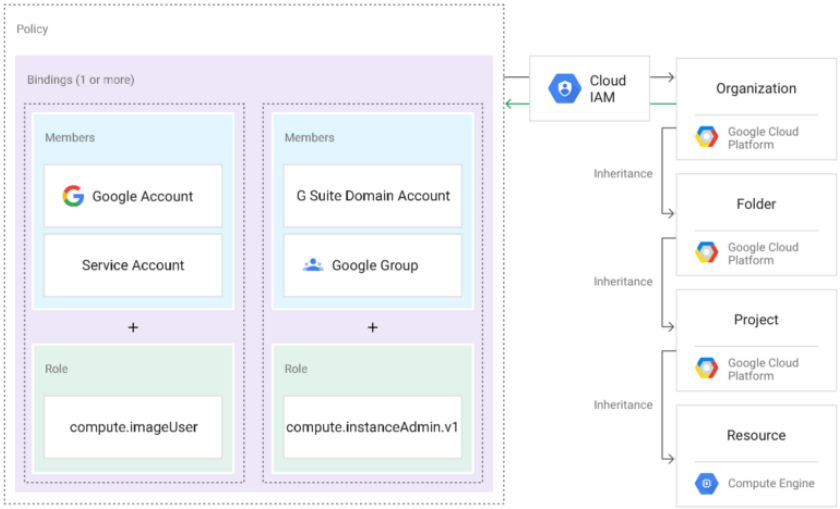
/ **Sub Publisher** (roles / pubsub.publisher) fornece acesso *apenas* para publicar mensagens em um tópico do Cloud Pub / Sub.

- Funções **personalizadas** : **funções** criadas para adaptar as permissões às necessidades de sua organização quando as funções predefinidas não atendem às suas necessidades.

Para saber como atribuir uma função ao usuário, consulte Concedendo, alterando e revogando o acesso . Para obter informações sobre as funções predefinidas refinadas do Cloud IAM, consulte Noções básicas sobre funções . Para obter informações sobre funções personalizadas, consulte Noções Básicas de Funções Customizadas e Criação e Gerenciamento de Funções Customizadas .

Política do IAM

Você pode conceder funções aos usuários criando uma *política do Cloud IAM* , que é uma coleção de instruções que definem quem tem o tipo de acesso. Uma política é anexada a um recurso e é usada para impor o controle de acesso sempre que esse recurso for acessado.



Uma política do Cloud IAM é representada pelo `Policy` objeto IAM . Um `Policy` objeto IAM consiste em uma lista de ligações. A `Binding` liga uma lista de `members` para um `role` .

`role` é a função que você deseja atribuir ao membro. O `role` é especificado na forma de `roles/<name of the role>`. Por exemplo, `roles/storage.objectAdmin`, `roles/storage.objectCreator`, e `roles/storage.objectViewer`.

`members` contém uma lista de uma ou mais identidades, conforme descrito na seção Conceitos relacionados à identidade acima. Cada tipo de membro é identificado com um prefixo, como uma Conta do Google (`user:`), uma conta de serviço (`serviceAccount:`), um grupo do Google (`group:`) ou um domínio do G Suite ou do Cloud Identity (`domain:`). No exemplo de trecho abaixo, o `storage.objectAdmin` papel é atribuído às seguintes membros utilizando o prefixo apropriado: `user:alice@example.com`, `serviceAccount:my-other-app@appspot.gserviceaccount.com`, `group:admins@example.com`, e `domain:google.com`. O `objectViewer` papel é atribuído a `user:bob@example.com`.

O snippet de código a seguir mostra a estrutura de uma política do Cloud IAM.

```
{
  "bindings": [
   {
     "role": "roles/storage.objectAdmin",
     "members": [
       "user:alice@example.com",
       "serviceAccount:my-other-
app@appspot.gserviceaccount.com",
       "group:admins@example.com",
       "domain:google.com" ]
   },
   {
     "role": "roles/storage.objectViewer",
     "members": ["user:bob@example.com"]
   }
   ]
}
```

Cloud IAM e APIs de política

O Cloud IAM fornece um conjunto de métodos que você pode usar para criar e gerenciar políticas de controle de acesso nos recursos do GCP. Esses métodos são expostos pelos serviços que suportam o Cloud IAM. Por exemplo, os métodos do Cloud IAM são expostos pelas APIs do

Resource Manager, do Cloud Pub / Sub e do Cloud Genomics, apenas para citar alguns.

Os métodos do Cloud IAM são:

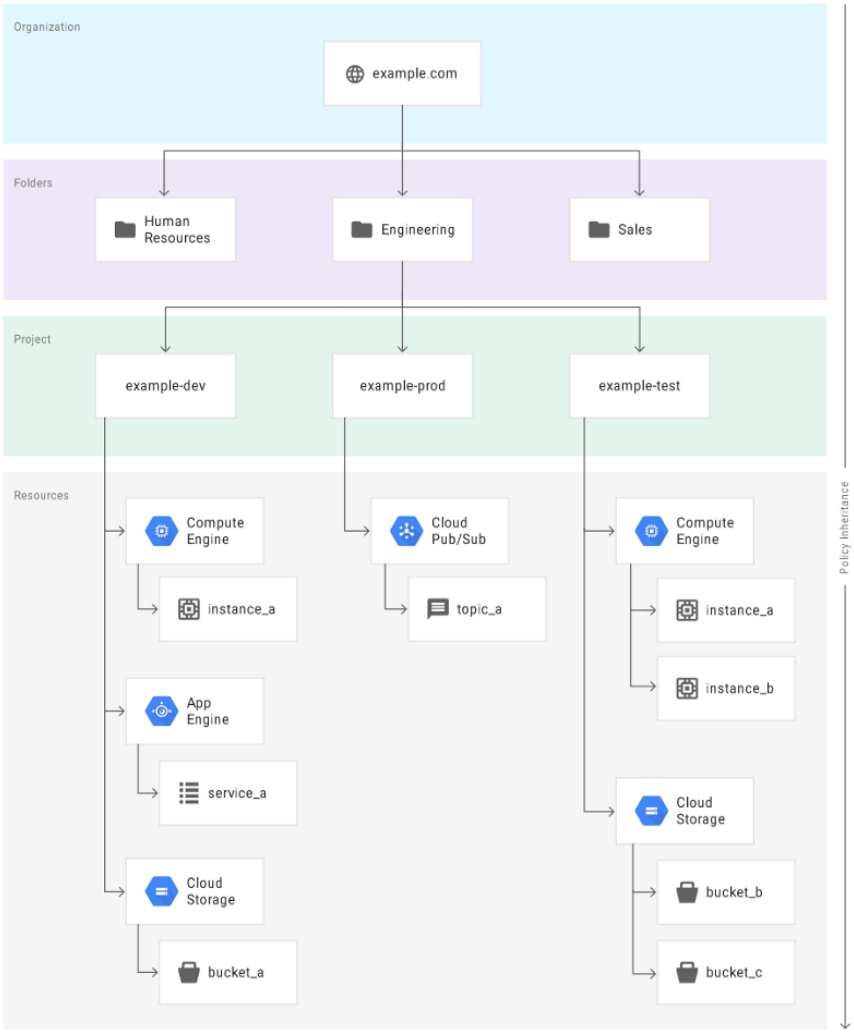
- `setIamPolicy()` : Permite que você defina políticas em seus recursos.
- `getIamPolicy()` : Permite que você obtenha uma política definida anteriormente.
- `testIamPermissions()` : Permite testar se o chamador tem as permissões especificadas para um recurso.

Você pode encontrar os tópicos de referência da API para esses métodos na documentação de cada serviço compatível com o Cloud IAM.

Hierarquia de políticas

Os recursos do GCP são organizados hierarquicamente, em que o nó da organização é o nó raiz na hierarquia, os projetos são os filhos da organização e os outros recursos são os descendentes dos projetos. Cada recurso tem exatamente um pai. Consulte o tópico Hierarquia de Recursos do Resource Manager para obter mais informações.

O diagrama a seguir é um exemplo de uma hierarquia de recursos do GCP:



Você pode definir uma política do Cloud IAM em qualquer nível na hierarquia de recursos: o nível da organização, o nível da pasta, o nível do projeto ou o nível do recurso. Recursos herdam as políticas do recurso pai. Se você definir uma política no nível da organização, ela será automaticamente herdada por todos os seus projetos filhos e, se você definir uma política no nível do projeto, ela será herdada por todos os seus recursos filhos. A política efetiva para um recurso é a união do conjunto de políticas nesse recurso e a política herdada de mais acima na hierarquia.

Essa herança de política é transitiva; Em outras palavras, os recursos herdam as políticas do projeto, que herdam as políticas das pastas, que herdam as políticas da organização. Portanto, as políticas no nível da organização também se aplicam no nível do recurso.

Por exemplo, no diagrama acima, topic_a é um recurso do Cloud Pub / Sub que mora sob o projeto example-prod. Se você concede a função de editor para micah@gmail.com por exemplo-prod e concede a função de editor para song@gmail.com para topic_a, você concede efetivamente a função de editor para topic_a a micah@gmail.com e a função de editor para song @ gmail.com.

A hierarquia de políticas do Cloud IAM segue o mesmo caminho da hierarquia de recursos do GCP. Se você alterar a hierarquia de recursos, a hierarquia de políticas também será alterada. Por exemplo, mover um projeto para uma organização atualizará a política do Cloud IAM do projeto para herdar da política do Cloud IAM da organização.

Políticas filhas não podem restringir o acesso concedido em um nível superior. Por exemplo, se você conceder a função Editor a um usuário para um projeto e conceder a função Visualizador ao mesmo usuário para um recurso filho, o usuário ainda terá a concessão de função Editor para o recurso filho.

Suporte do Cloud IAM para serviços do GCP

Com o Cloud IAM, todos os métodos da API em todos os serviços do GCP são verificados para garantir que a conta que faz a solicitação da API tenha a permissão apropriada para usar o recurso.

Antes do Cloud IAM, você só podia conceder funções de Proprietário, Editor ou Visualizador. Essas funções dão acesso muito amplo a um projeto e não permitem a separação minuciosa de tarefas. Os serviços do GCP agora oferecem funções predefinidas adicionais que fornecem controle de acesso mais refinado do que as funções do Proprietário, Editor e Visualizador. Por exemplo, o Compute Engine oferece funções como *Administrador de Instância* e *Administrador de Rede,* e o Google App Engine oferece funções como *Administrador de Aplicativos* e *Administrador de Serviços* . Essas funções predefinidas estão disponíveis além das funções herdadas de Proprietário, Editor e Visualizador.

Se você precisar de mais controle sobre as permissões, considere a criação de uma função personalizada .

Os seguintes produtos oferecem funções predefinidas do Cloud IAM:

- Projeto do Google Cloud Platform
- Organização do GCP
- Compute Engine
- Repositórios de origem em nuvem
- App Engine
- Armazenamento na núvem
- BigQuery
- Cloud Bigtable
- IAM para o Cloud SQL
- Stackdriver Debugger
- Cloud Deployment Manager
- Cloud Genomics
- Serviço de gerenciamento de chaves na nuvem
- Cloud Pub / Sub
- Mecanismo de aprendizado de máquina em nuvem
- Cloud Spanner
- Stackdriver Logging
- Cloud IAM para o Stackdriver Monitoring
- Cloud Dataflow
- Cloud IAM para Cloud Datastore
- Cloud IAM para Cloud Dataproc
- Cloud IAM para o Google Kubernetes Engine
- Cloud IAM para Cloud DNS
- Cloud IAM para Stackdriver Trace
- Cloud IAM para Cloud Billing API

- Cloud IAM for Service Management

Para obter uma lista completa de funções predefinidas, consulte Noções básicas sobre funções .

Você pode conceder aos usuários determinadas funções para acessar recursos com granularidade *melhor do que o nível do projeto* . Por exemplo, você pode criar uma política de controle de acesso do Cloud IAM que concede a um usuário a função de *Assinante* para um determinado tópico do Cloud Pub / Sub. Para obter informações sobre quais funções podem ser concedidas em quais recursos, consulte Noções básicas sobre funções .

++

O que são contas de serviço?

Uma conta de serviço é uma conta do Google especial que pertence ao seu aplicativo ou a uma máquina virtual (VM), em vez de um usuário final individual.

Seu aplicativo usa a conta de serviço para chamar a API do Google de um serviço para que os usuários não sejam envolvidos diretamente.

Por exemplo, uma VM do Compute Engine pode ser executada como uma conta de serviço e essa conta pode receber permissões para acessar os recursos de que precisa. Dessa forma, a conta de serviço é a identidade do serviço e as permissões da conta de serviço controlam quais recursos o serviço pode acessar.

Uma conta de serviço é identificada por seu endereço de e-mail, que é exclusivo da conta.

Chaves da conta de serviço

Cada conta de serviço está associada a um par de chaves, gerenciado pelo Google Cloud Platform (GCP). Ele é usado para autenticação de serviço a serviço no GCP. Essas chaves são giradas automaticamente pelo Google e são usadas para assinatura por no máximo duas semanas.

Como opção, você pode criar um ou mais pares de chaves externas para uso fora do GCP (por exemplo, para uso com Credenciais Padrão do Aplicativo). Quando você cria um novo par de chaves, faz o download da chave privada (que não é retida pelo Google). Com chaves externas, você é responsável pela segurança da chave privada e outras operações de gerenciamento, como a rotação de chaves. As chaves externas podem ser gerenciadas pela API do IAM, `gcloud` pela ferramenta de linha de comando ou pela página Contas de serviço no console do Google Cloud Platform. Você pode criar até 10 chaves de conta de serviço por conta de serviço para facilitar a rotação de chaves.

Tipos de contas de serviço

Contas de serviço gerenciadas pelo usuário

Quando você cria um novo projeto do Cloud usando o Console do GCP e se a API do Compute Engine está ativada para o seu projeto, uma conta do Compute Engine Service é criada para você por padrão. É identificável usando o email:

```
PROJECT_NUMBER-compute@developer.gserviceaccount.com
```

Se o seu projeto contém um aplicativo do App Engine, a conta de serviço padrão do App Engine é criada no seu projeto por padrão. É identificável usando o email:

```
PROJECT_ID@appspot.gserviceaccount.com
```

Se você criar uma conta de serviço em seu projeto, nomeará a conta de serviço e receberá um email com o seguinte formato:

```
SERVICE_ACCOUNT_NAME@PROJECT_ID.iam.gserviceaccount.com
```

Você pode criar até 100 contas de serviço por projeto (incluindo a conta de serviço padrão do Compute Engine e a conta de serviço do App Engine) usando a API do IAM, o console do GCP ou a `gcloud` ferramenta de linha de comando. Essas contas de serviço padrão e as contas de serviço que você cria explicitamente são as contas de serviço gerenciadas pelos usuários.

Cuidado: o comportamento exato de quando as contas de serviço padrão são criadas e de como elas são exibidas no projeto pode mudar no futuro, já que elas foram projetadas para serem usadas pelo Google Compute Engine e pelo Google App Engine, por isso é recomendável que você não confie sobre a existência dessas contas padrão para seu uso. É recomendável criar contas de serviço adicionais explicitamente usando a API do IAM, o Console do GCP ou a `gcloud` ferramenta de linha de comando para seu uso a longo prazo.

Contas de serviço gerenciadas pelo Google

Além das contas de serviço gerenciadas pelos usuários, você pode ver algumas contas de serviço adicionais na política do IAM do seu projeto ou no Console do GCP. Essas contas de serviço são criadas e de propriedade do Google. Essas contas representam diferentes serviços do Google e cada conta recebe automaticamente funções do IAM para acessar seu projeto do GCP.

Conta de serviço das APIs do Google

Um exemplo de uma conta de serviço gerenciada pelo Google é uma conta de serviço da API do Google identificável usando o e-mail:

```
PROJECT_NUMBER@cloudservices.gserviceaccount.com
```

Essa conta de serviço foi projetada especificamente para executar processos internos do Google em seu nome e não está listada na seção **Contas de serviço** do Console do GCP. Por padrão, a conta recebe automaticamente a função de editor de projeto no projeto e é listada na seção **IAM** do console do GCP. Esta conta de serviço é excluída somente quando o projeto é excluído. Os serviços do Google dependem da conta ter acesso ao seu projeto, portanto, você não deve remover ou alterar a função da conta de serviço em seu projeto.

Permissões da conta de serviço

Além de ser uma identidade , uma conta de serviço é um recurso que possui políticas do IAM associadas a ela. Essas políticas determinam quem pode usar a conta de serviço.

Por exemplo, Alice pode ter a função de editor em uma conta de serviço e Bob pode ter a função de visualizador em uma conta de serviço. Isso é

como conceder papéis para qualquer outro recurso do GCP.

As contas de serviço padrão do Compute Engine e do Google App Engine recebem funções de editor no projeto quando são criadas, para que o código em execução na sua instância do aplicativo ou da VM tenha as permissões necessárias. Nesse caso, as contas de serviço são identidades que recebem a função de editor de um recurso (projeto).

Se você quiser permitir que sua automação acesse um intervalo do Cloud Storage, conceda à conta de serviço (que sua automação usa) as permissões para ler o intervalo do Cloud Storage. Nesse caso, a conta de serviço é a identidade que você está concedendo permissões para outro recurso (o intervalo do Cloud Storage).

A função de usuário da conta de serviço

Você pode conceder a `iam.serviceAccountUser` função no nível do projeto para todas as contas de serviço no projeto ou no nível da conta de serviço.

- A concessão da `iam.serviceAccountUser` função a um usuário para um projeto fornece ao usuário acesso a todas as contas de serviço no projeto, incluindo contas de serviço que podem ser criadas no futuro.
- A concessão da `iam.serviceAccountUser` função a um usuário para uma conta de serviço específica fornece ao usuário acesso à conta de serviço.

Se você conceder a um usuário a `compute.instanceAdmin` função com a `iam.serviceAccountUser` função, ele poderá criar e gerenciar instâncias do Compute Engine que usam uma conta de serviço.

Depois de conceder funções do IAM a contas de serviço, você pode atribuir a conta de serviço a uma ou mais novas instâncias de máquina virtual. Para obter instruções sobre como fazer isso, consulte Configurando uma nova instância para executar como uma conta de serviço .

Os usuários que são serviceAccountUsers podem usar a conta de serviço para acessar indiretamente todos os recursos aos quais a conta de serviço tem acesso. Por exemplo, um usuário que é um

serviceAccountUser pode iniciar uma instância usando a conta de serviço. Eles podem usar a instância para acessar qualquer coisa que a identidade da conta de serviço tenha acesso. No entanto, a função serviceAccountUser não permite que um usuário use diretamente as funções da conta de serviço. Portanto, seja cauteloso ao conceder a `iam.serviceAccountUser` função a um usuário.

As contas de serviço representam sua segurança no nível de serviço. A segurança do serviço é determinada pelas pessoas que têm funções do IAM para gerenciar e usar as contas de serviço e pelas pessoas que possuem chaves externas privadas para essas contas de serviço. As melhores práticas para garantir a segurança incluem o seguinte:

- Use a API do IAM para auditar as contas de serviço, as chaves e as políticas nessas contas de serviço.
- Se as suas contas de serviço não precisarem de chaves externas, exclua-as.
- Se os usuários não precisarem de permissão para gerenciar ou usar contas de serviço, remova-os da Política do IAM.

Para saber mais sobre práticas recomendadas, consulte Noções básicas sobre contas de serviço .

O papel do criador de token da conta de serviço

Essa função permite a representação de contas de serviço para criar tokens de acesso OAuth2, assinar blobs ou assinar JWTs.

A função Ator da conta de serviço

Esta função foi reprovada. Se você precisar executar operações como a conta de serviço, use a função Usuário da Conta de Serviço . Para fornecer efetivamente as mesmas permissões que o Ator de Conta de Serviço, você também deve conceder o Criador de Token de Conta de Serviço .

Acessar escopos

Escopos de acesso são o método legado de especificar permissões para sua VM. Antes da existência de funções do IAM, os escopos de acesso eram o único mecanismo para conceder permissões a contas de serviço. Embora eles não sejam a principal forma de conceder permissões agora, você ainda deve definir escopos de acesso ao configurar uma instância para ser executada como uma conta de serviço. Para obter informações sobre escopos de acesso, consulte a documentação do Google Compute Engine

Credenciais da conta de serviço de curta duração

Você pode criar credenciais de curta duração que permitem assumir a identidade de uma conta de serviço do GCP. Essas credenciais podem ser usadas para autenticar chamadas para APIs do Google Cloud Platform ou outras APIs que não são do Google.

O caso de uso mais comum para essas credenciais é delegar temporariamente o acesso aos recursos do GCP em diferentes projetos, organizações ou contas. Por exemplo, em vez de fornecer um chamador externo com as credenciais permanentes de uma conta de serviço altamente privilegiada, o acesso de emergência temporário pode ser concedido em seu lugar. Como alternativa, uma conta de serviço designada com permissões restritas pode ser representada por um chamador externo sem exigir credenciais de conta de serviço mais altamente privilegiadas.

Para obter mais informações, consulte Criando Credenciais de Conta de Serviço com Curto Prazo .

Credenciais Padrão do Aplicativo

As credenciais padrão do aplicativo são um mecanismo para facilitar o uso de contas de serviço ao operar dentro e fora do GCP, bem como em vários projetos do GCP. O caso de uso mais comum é testar o código em uma máquina local e, em seguida, mover para um projeto de desenvolvimento no GCP e, em seguida, mover para um projeto de produção no GCP. O uso de credenciais padrão do aplicativo garante que a conta de serviço funcione sem problemas; ou seja, ele usa uma chave de conta de serviço armazenada localmente ao testar em sua máquina local, mas usa a conta de serviço padrão do Compute Engine

do projeto quando é executada no Compute Engine. Para obter mais informações, consulte Credenciais padrão do aplicativo .

Criando e gerenciando contas de serviço

Quando você cria um novo projeto de nuvem, o Google Cloud Platform (GCP) cria automaticamente uma conta de serviço do Compute Engine e uma conta de serviço do Google App Engine nesse projeto. Você pode criar até 98 contas de serviço adicionais para o seu projeto para controlar o acesso aos seus recursos.

Permissões necessárias

Para permitir que um usuário gerencie contas de serviço, conceda uma das seguintes funções:

- *Usuário da conta de serviço* (`roles/iam.serviceAccountUser`): Concede permissões para obter, listar ou representar uma conta de serviço.
- *Administrador da conta de serviço* (`roles/iam.serviceAccountAdmin`): inclui permissões de *usuário da conta de serviço* e também concede permissões para criar, atualizar, excluir e definir ou obter a política do Cloud IAM em uma conta de serviço.

As funções primitivas do Cloud IAM também contêm permissões para gerenciar contas de serviço. No entanto, recomendamos que você conceda uma das funções predefinidas acima para impedir o acesso desnecessário a outros recursos do GCP.

Consulte o tópico Funções de Conta de Serviço para obter mais informações sobre funções relacionadas a contas de serviço.

Criando uma conta de serviço

Criar uma conta de serviço é semelhante à adição de um membro ao seu projeto, mas a conta de serviço pertence aos seus aplicativos, e não a um usuário final individual.

Nos exemplos abaixo, **[SA-NAME]** é o nome da conta de serviço. Este é um identificador único; ele aparecerá no endereço de e-mail da conta

de serviço e você o usará para atualizar a conta de serviço com outras APIs. Não pode ser alterado depois de criado. **[SA-DISPLAY-NAME]** é um nome amigável para a conta de serviço. **[PROJECT-ID]** é o código do seu projeto do Google Cloud Platform.

Para criar uma conta de serviço, no mínimo, o usuário deve receber a função *Administrador da Conta de Serviço* (`roles/iam.serviceAccountAdmin`) ou a função primitiva do *Editor* (`roles/editor`).

1. Abra a página **Contas de serviço** no console do GCP.
2. ABRA A PÁGINA DE CONTAS DE SERVIÇO
3. Clique em **Selecionar um projeto** .
4. Selecione seu projeto e clique em **Abrir** .
5. Clique em **Criar Conta de Serviço** .
6. Digite um nome de conta de serviço, selecione uma função que você deseja conceder à conta de serviço e clique em **Salvar** .

Depois de criar uma conta de serviço, conceda uma ou mais funções à conta de serviço para que ela possa agir em seu nome.

Listando contas de serviço

Ao listar contas de serviço, você pode especificar parâmetros para limitar o número de contas de serviço a serem incluídas na resposta. Você pode usar `ListServiceAccountsResponse.next_page_token` em uma solicitação subsequente para listar as contas de serviço restantes.

Use esse método para auditar contas e chaves de serviço ou para criar ferramentas personalizadas para gerenciar contas de serviço.

Para listar contas de serviço, no mínimo, o usuário deve receber a função *Usuário da Conta de Serviço* (`roles/iam.serviceAccountUser`) ou a função primitiva do *Visualizador* (`roles/viewer`).

1. Abra a página **Contas de serviço** no console do GCP.
2. ABRA A PÁGINA DE CONTAS DE SERVIÇO

3. Clique em **Selecionar um projeto** .
4. Selecione seu projeto e clique em **Abrir** . Todas as contas de serviço estão listadas na página Contas de serviço.

Renomeando uma conta de serviço

O nome de exibição de uma conta de serviço é comumente usado para capturar informações adicionais sobre a conta de serviço, como a finalidade da conta de serviço ou uma pessoa de contato da conta.

Para renomear uma conta de serviço, no mínimo, o usuário deve receber a função *Administrador da Conta de Serviço* (`roles/iam.serviceAccountAdmin`) ou a função primitiva do *Editor* (`roles/editor`).

1. Abra a página **Contas de serviço** no console do GCP.
2. ABRA A PÁGINA DE CONTAS DE SERVIÇO
3. Clique em **Selecionar um projeto** .
4. Selecione seu projeto e clique em **Abrir** .
5. Procure a conta de serviço que deseja renomear, clique no botão **Mais** more_vert nessa linha e clique em **Editar** .
6. Digite o novo nome e clique em **Salvar** .

Excluindo uma conta de serviço

Quando você exclui uma conta de serviço, os aplicativos não terão mais acesso aos recursos do Google Cloud Platform por meio dessa conta de serviço. Se você excluir as contas de serviço padrão do App Engine e do Compute Engine, as instâncias não terão mais acesso a recursos no projeto.

Excluir com cautela; Verifique se seus aplicativos críticos não usam mais uma conta de serviço antes de excluí-la. Além disso, as associações de função para uma conta de serviço excluída não são removidas imediatamente; eles são automaticamente removidos do sistema após um máximo de 60 dias.

Para excluir uma conta de serviço, no mínimo, o usuário deve receber a função *Administrador da Conta de Serviço* (`roles/iam.serviceAccountAdmin`) ou a função primitiva do *Editor* (`roles/editor`).

1. Abra a página **Contas de serviço** no console do GCP.
2. ABRA A PÁGINA DE CONTAS DE SERVIÇO
3. Clique em **Selecionar um projeto** .
4. Selecione seu projeto e clique em **Abrir** .
5. Selecione as contas de serviço que você deseja excluir e clique em **Excluir.**

Depois de excluir uma conta de serviço, evite criar uma nova conta de serviço com o mesmo nome. Isso pode resultar em um comportamento inesperado. Para obter mais informações, consulte Excluindo e recriando contas de serviço.

- -

Noções básicas sobre contas de serviço

fundo

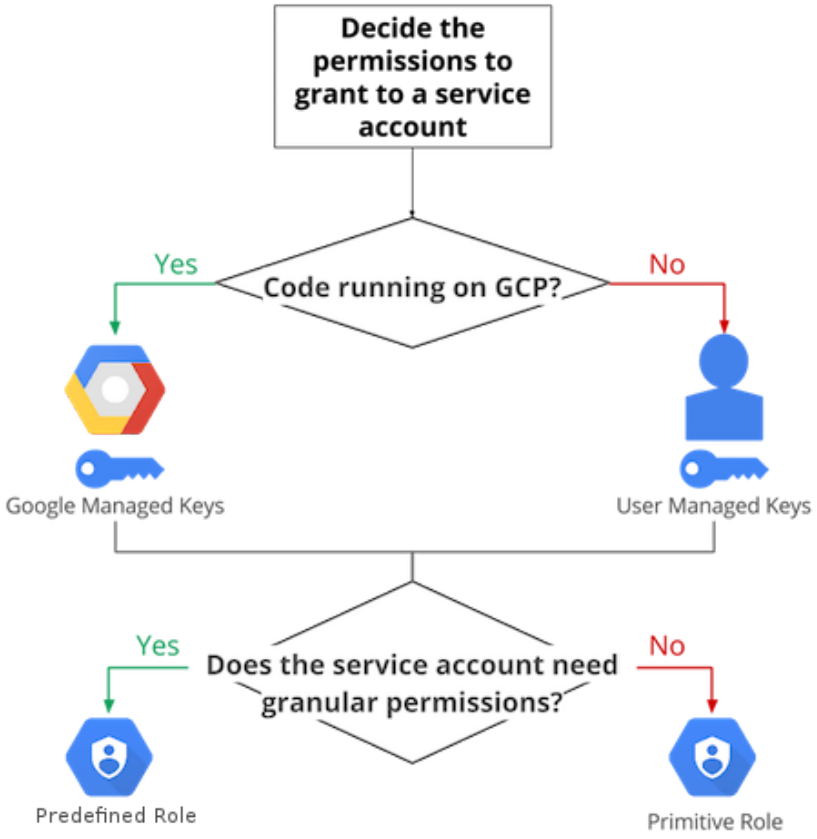
Uma conta de serviço é um tipo especial de conta do Google que pertence ao seu aplicativo ou a uma máquina virtual (VM), em vez de a um usuário final individual. Seu aplicativo assume a identidade da conta de serviço para chamar APIs do Google para que os usuários não sejam envolvidos diretamente. Uma conta de serviço pode ter zero ou mais pares de chaves de contas de serviço, que são usadas para autenticar no Google.

Depois de decidir que você precisa de uma conta de serviço, faça as seguintes perguntas para entender como usar a conta de serviço:

- Quais recursos a conta de serviço pode acessar?
- Quais permissões a conta de serviço precisa?

- Onde será executado o código que assume a identidade da conta de serviço: no Google Cloud Platform ou no local?

Use o fluxograma a seguir para descobrir as respostas para as perguntas acima:



Um dos recursos das contas de serviço do IAM é que você pode tratá-lo como um recurso e como uma identidade .

Ao tratar a conta de serviço como uma identidade, você pode conceder uma função a uma conta de serviço, permitindo que ela acesse um recurso (como um projeto).

Ao tratar uma conta de serviço como um recurso, você pode conceder permissão a um usuário para acessar essa conta de serviço. Você pode conceder a função de usuário Proprietário, Editor, Visualizador ou Conta de serviço a um usuário para acessar a conta de serviço.

Concedendo Acesso a Contas de Serviço

Conceder acesso a uma conta de serviço para acessar um recurso é semelhante a conceder acesso a qualquer outra identidade. Por exemplo, se você tiver um aplicativo em execução no Google Compute Engine e quiser que o aplicativo tenha acesso *somente* para criar objetos no Google Cloud Storage. Você pode criar uma conta de serviço para o aplicativo e conceder a ela a função Criador de Objetos de Armazenamento . O diagrama a seguir ilustra este exemplo:

Saiba mais sobre como conceder funções a contas de serviço .

Atuando como uma conta de serviço

Digamos que você tenha um trabalho de longa duração que seus funcionários tenham permissões para iniciar. Você não quer que o trabalho seja encerrado quando o funcionário que iniciou o trabalho pela última vez deixar a empresa.

A maneira como você resolveria esse problema é criando uma conta de serviço para iniciar e parar o trabalho. Você pode fazer isso usando as seguintes etapas:

1. Crie uma conta de serviço .
2. Conceda a função Usuário da conta de serviço (iam.serviceAccountUser) para a conta de serviço aos funcionários que precisam de permissão para iniciar o trabalho. Nesse cenário, o serviço é o recurso.
3. Conceda a função Administrador da instância de computação (roles / compute.instanceAdmin.v1) aos mesmos funcionários.
4. Agora, os funcionários podem criar instâncias do Compute Engine que executam essa conta de serviço, conectam-se a eles e usam a conta de serviço para iniciar o trabalho. Por exemplo:

- `gcloud compute instances create my-instance --scopes=cloud-platform \`
  `--service-account=my-service-account@test9q.iam.gserviceaccount.com \`
  `--zone=us-central1-a`

Para mais informações, consulte A função serviceAccountUser .

Observação: os usuários com as funções Usuário da conta de serviço e Administrador da instância do computador podem acessar indiretamente todos os recursos aos quais a conta de serviço tem acesso, bem como criar, modificar e excluir instâncias do Compute Engine. Portanto, seja cauteloso ao conceder essas funções aos usuários.

Migração de dados para o Google Cloud Platform

Digamos que você tenha algum processamento de dados que acontece em outro provedor de nuvem e deseja transferir os dados processados para o Google Cloud Platform. Você pode usar uma conta de serviço das máquinas virtuais na nuvem externa para enviar os dados ao Google Cloud Platform. Para fazer isso, você deve criar e baixar uma chave de conta de serviço ao criar a conta de serviço e, em seguida, usar essa chave do processo externo para chamar as APIs do Cloud Platform.

Mantendo o controle de contas de serviço

Com o tempo, à medida que você cria mais e mais contas de serviço, pode perder o controle de qual conta de serviço é usada para qual finalidade.

O nome de exibição de uma conta de serviço é uma boa maneira de capturar informações adicionais sobre a conta de serviço, como o objetivo da conta de serviço ou uma pessoa de contato da conta. Para novas contas de serviço, você pode preencher o nome de exibição ao criar a conta de serviço. Para o serviço existente, as contas usam o `serviceAccounts.update()` método para modificar o nome de exibição.

Excluindo e recriando contas de serviço

É possível excluir uma conta de serviço e criar uma nova conta de serviço com o mesmo nome. Se você reutilizar o nome de uma conta de serviço excluída, isso poderá resultar em um comportamento inesperado.

Quando você exclui uma conta de serviço, suas ligações de função não são excluídas imediatamente. Se você criar uma nova conta de serviço com o mesmo nome de uma conta de serviço excluída recentemente, as ligações antigas ainda poderão existir; no entanto, eles **não se aplicam à nova conta de serviço,** mesmo que as duas contas tenham o mesmo endereço de email. Esse comportamento ocorre porque as contas de serviço recebem um ID exclusivo no Cloud IAM na criação. Internamente, todas as associações de função são concedidas usando esses IDs, não o endereço de email da conta de serviço. Portanto, quaisquer associações de função que existiam para uma conta de serviço excluída não se aplicam a uma nova conta de serviço que usa o mesmo endereço de email.

Para evitar confusão, sugerimos usar nomes de conta de serviço exclusivos. Se isso não for possível, você pode conceder uma função à nova conta de serviço:

1. Removendo explicitamente quaisquer ligações que concedem essa função à conta de serviço antiga.
2. Re-concedendo essas funções para a nova conta de serviço.

Você deve remover as associações de função antes de adicioná-las novamente. A simples concessão da função novamente falhará silenciosamente ao conceder a função à conta de serviço excluída antiga.

Concedendo permissões mínimas para contas de serviço

Você só deve conceder à conta de serviço o conjunto mínimo de permissões necessárias para atingir sua meta. Saiba mais sobre como conceder funções a uma conta de serviço para recursos específicos .

Ao conceder permissões aos usuários para acessar uma conta de serviço, lembre-se de que o usuário pode acessar todos os recursos para os quais a conta de serviço tem permissões. Portanto, é importante configurar as permissões de suas contas de serviço com cuidado; isto é, seja rigoroso sobre quem em sua equipe pode atuar como uma conta de serviço.

Usuários com funções do IAM para atualizar as instâncias do App Engine e do Compute Engine (como o App Engine Deployer ou o Compute Instance Admin) podem executar códigos como as contas de serviço usadas para executar essas instâncias e indiretamente obter acesso a todos os recursos para os quais o serviço contas têm acesso. Da mesma forma, o acesso por SSH a uma instância do Compute Engine também pode fornecer a capacidade de executar código como essa instância.

Gerenciando chaves de conta de serviço

Existem dois tipos de chaves de conta de serviço:

- **Chaves gerenciadas pelo GCP** . Essas chaves são usadas pelos serviços do Cloud Platform, como o App Engine e o Compute Engine. Eles não podem ser baixados e são automaticamente girados e usados para assinatura por no máximo duas semanas. O processo de rotação é probabilístico; o uso da nova chave aumentará gradualmente a duração da chave. Recomendamos o armazenamento em cache do conjunto de chaves públicas para uma conta de serviço por no máximo 24 horas, para garantir que você sempre tenha acesso ao conjunto de chaves atual.
- **Chaves gerenciadas pelo usuário** . Essas chaves são criadas, baixadas e gerenciadas pelos usuários. Eles expiram 10 anos após a criação.

Para chaves gerenciadas pelo usuário, você precisa ter certeza de ter processos em vigor para atender aos principais requisitos de gerenciamento, como:

- Armazenamento chave
- Distribuição chave

- Revogação da chave
- Rotação da chave
- Protegendo as chaves contra usuários não autorizados
- Recuperação de chaves

Qualquer pessoa que tenha acesso às chaves poderá acessar recursos por meio da conta de serviço. Sempre desencoraje os desenvolvedores a verificar as chaves no código-fonte ou deixá-las no diretório Downloads.

Para melhorar a segurança das chaves, siga as orientações abaixo:

- Use a API da conta de serviço do IAM para girar automaticamente as chaves da sua conta de serviço. Você pode girar uma chave criando uma nova chave, alternando os aplicativos para usar a nova chave e excluindo a chave antiga. Use os métodos `serviceAccount.keys.create()` e `serviceAccount.keys.delete()` juntos para automatizar a rotação. As chaves gerenciadas pelo GCP são alternadas aproximadamente uma vez por semana.
- Use o `serviceAccount.keys.list()` método para auditar contas e chaves de serviço.

Usando contas de serviço com o Compute Engine

As instâncias do Compute Engine precisam ser executadas como contas de serviço para terem acesso a outros recursos do Cloud Platform. Para garantir que suas instâncias do Compute Engine sejam seguras, considere o seguinte:

- Você pode criar VMs no mesmo projeto com diferentes contas de serviço. Para alterar a conta de serviço de uma VM após sua criação, use o `instances.setServiceAccount` método.
- Você pode conceder funções do IAM a contas de serviço para definir o que elas podem acessar. Em muitos casos, você não precisará mais depender de escopos. Isso lhe dá a vantagem de

poder modificar as permissões da conta de serviço de uma VM sem recriar a instância.

- Como as instâncias dependem de suas contas de serviço para ter acesso aos recursos do Cloud Platform, evite excluir as contas de serviço quando elas ainda são usadas pelas instâncias em execução. Se você excluir as contas de serviço, as instâncias poderão começar a falhar em suas operações.

Melhores práticas

- Restringir quem pode atuar como contas de serviço. Os usuários que são usuários da conta de serviço para uma conta de serviço podem acessar indiretamente todos os recursos aos quais a conta de serviço tem acesso. Portanto, tenha cuidado ao conceder a função serviceAccountUser a um usuário.
- Conceda à conta de serviço apenas o conjunto mínimo de permissões necessárias para atingir sua meta. Saiba mais sobre como conceder funções a uma conta de serviço para recursos específicos .
- Crie contas de serviço para cada serviço com apenas as permissões necessárias para esse serviço.
- Use o nome de exibição de uma conta de serviço para acompanhar as contas de serviço. Quando você cria uma conta de serviço, preencha seu nome de exibição com o propósito da conta de serviço.
- Defina uma convenção de nomenclatura para suas contas de serviço.
- Implemente processos para automatizar a rotação de chaves de contas de serviço gerenciadas pelo usuário.
- Aproveite a API da conta de serviço do IAM para implementar a rotação de chaves.
- Faça auditoria nas contas e chaves de serviço usando o `serviceAccount.keys.list()` método ou a página Visualizador de Logs no console.

- Não exclua as contas de serviço que estão em uso, executando instâncias no Google App Engine ou no Google Compute Engine.

++

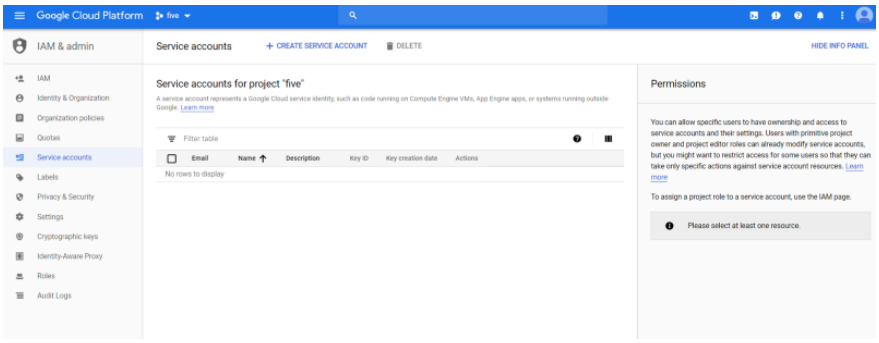
Gerenciando contas de serviço com escopos limitados

Dar acesso à conta de serviço é uma tarefa muito importante, pois o acesso errado pode levar a várias ameaças à segurança.

A melhor prática é dar a qualquer acesso necessário para cumprir o trabalho que precisa ser feito.

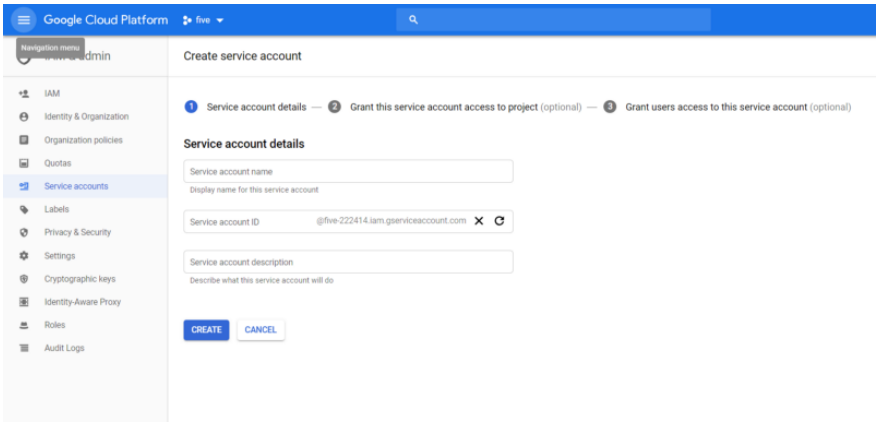
vamos ver como fazer isso.

Primeiro, vá para a guia IAM e serviços e, em seguida, para a conta do Serviço



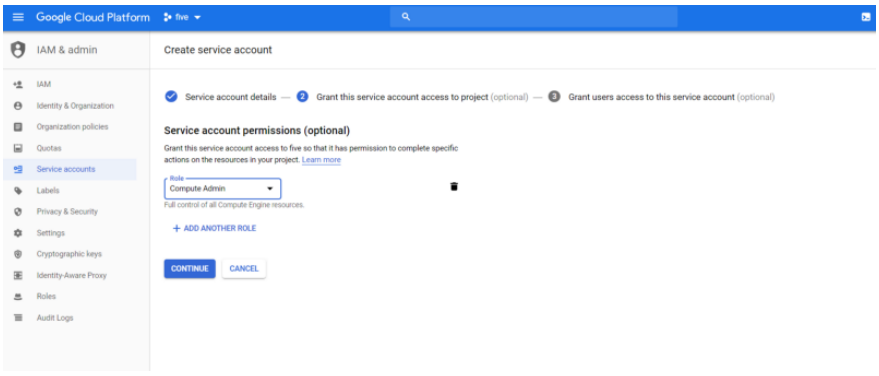
Conta de serviço

Agora clique em criar uma conta de serviço

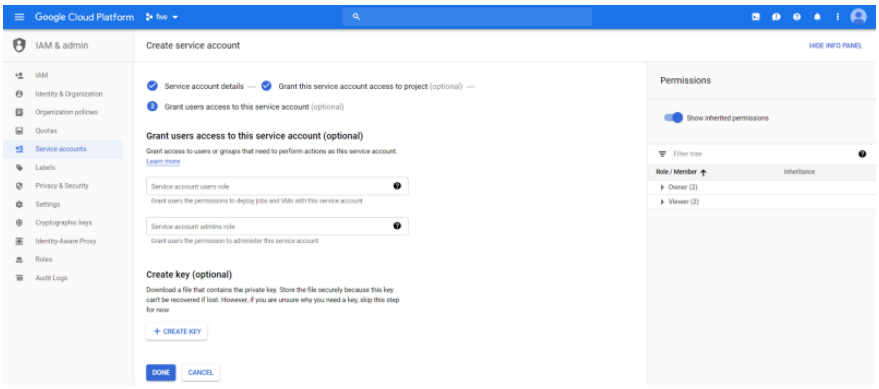


criar conta de serviço

Então você verá a página de permissões, este é um lugar onde você pode limitar o acesso para a conta de serviço.



Então você verá a página onde você pode atribuir essa conta de serviço aos usuários.

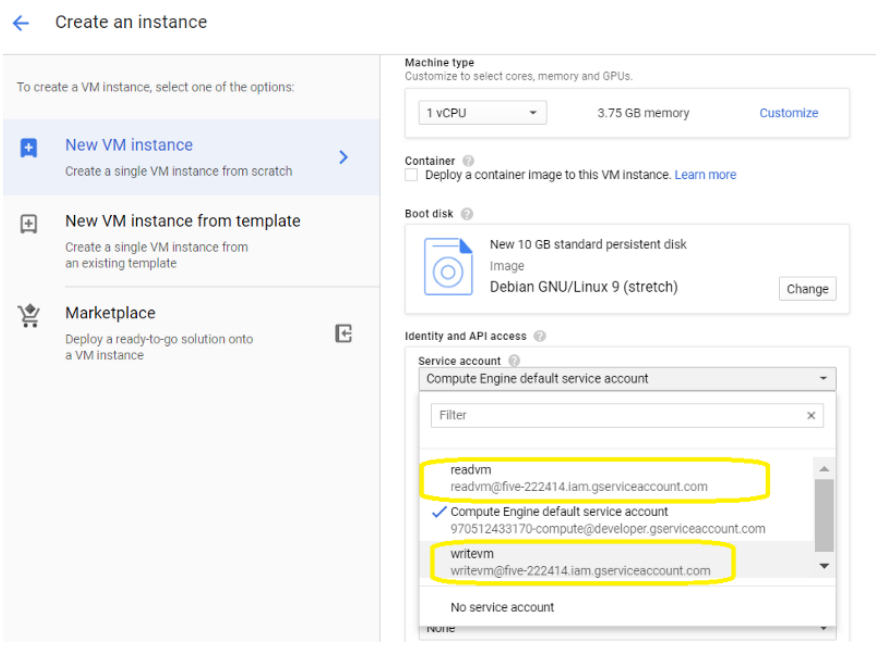


Depois de criar a conta de serviço, podemos modificar mais a partir do painel.

- -

Atribuindo uma conta de serviço a instâncias de VM

Você pode atribuir facilmente a conta de serviço à instância da VM ao criar a nova VM na seção do IAM, conforme abaixo. Para isso, você precisa criar uma conta de serviço antes de fazer a VM.



- -

Conceder acesso a uma conta de serviço em outro projeto

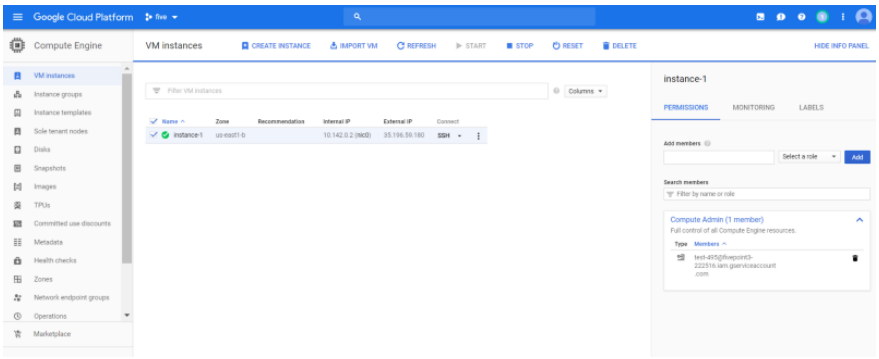
Se você tiver dois projetos e quiser conceder acesso à conta de serviço a outro projeto, poderá usar a conta de serviço nesse caso.

Primeiro, crie uma conta de serviço como acima.

Agora vá para o segundo projeto e depois para a VM onde você deseja acessar.

Selecione a VM e adicione a conta de serviço na página de permissão no lado direito.

Aplique



Adicionar conta de serviço fora do projeto

- -

Dessa maneira, você pode executar tarefas na conta de serviço.