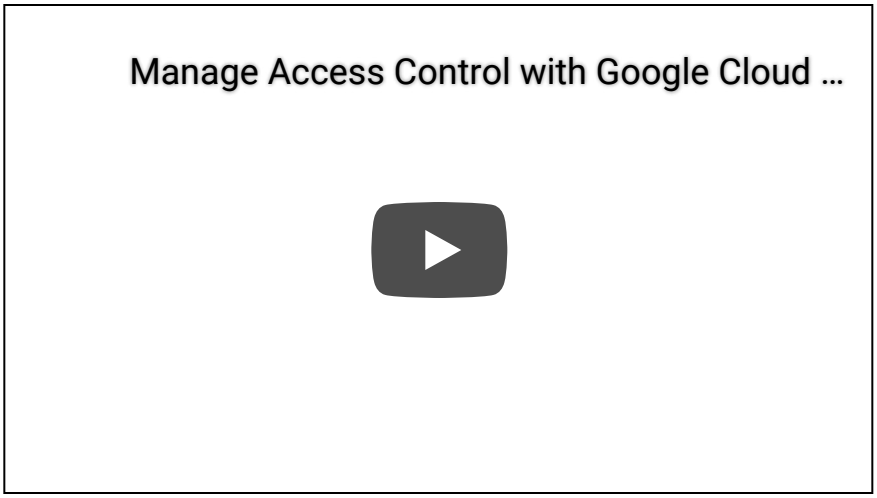
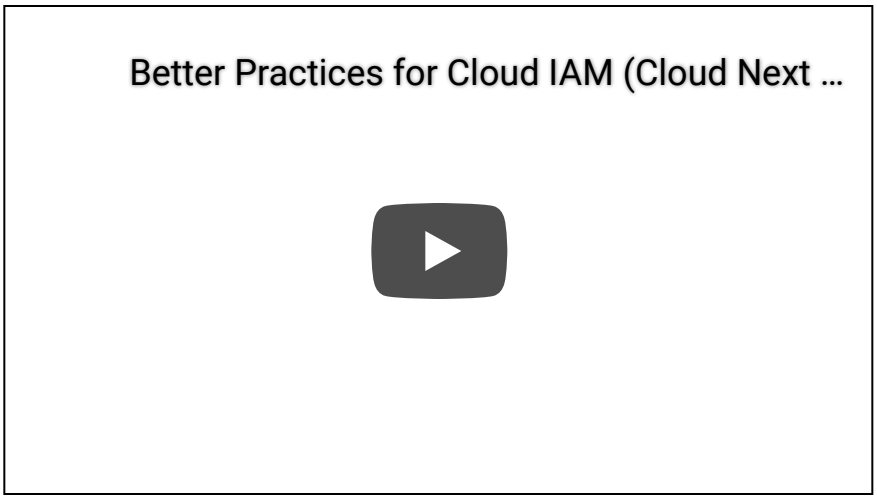
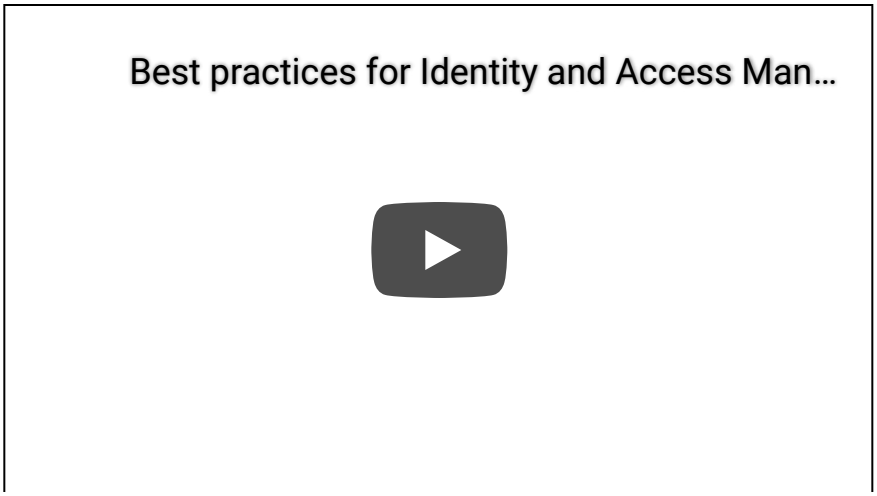
Série de Certificação GCP: Seção 5: Configurando acesso e segurança, 5.1 Gerenciando o Gerenciamento de Identidades e Acesso (IAM)

Prashanta Paudel Segue
13 de novembro de 2018 · 22 minutos de leitura

Esta é a última seção da série de Certificação GCP, assim como no curso. Esta seção trata principalmente sobre como gerenciar o acesso e a segurança das instâncias e produtos no Google Cloud Platform.







O gerenciamento de identidade e acesso é a estrutura de negócios e organização para facilitar a identidade digital. O IAM é basicamente uma solução de segurança em geral.

O IAM possibilita que as organizações concedam direitos de acesso adequados às pessoas de acordo com seu cargo. Desta forma, ninguém terá mais acesso e as coisas vão funcionar sem problemas.

referência: https://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system

Outro aspecto do IAM é o gerenciamento de contas de serviço. Agora, com esse recurso, você pode permitir que determinados serviços possam operar em uma instância, permitindo a conta de serviço.

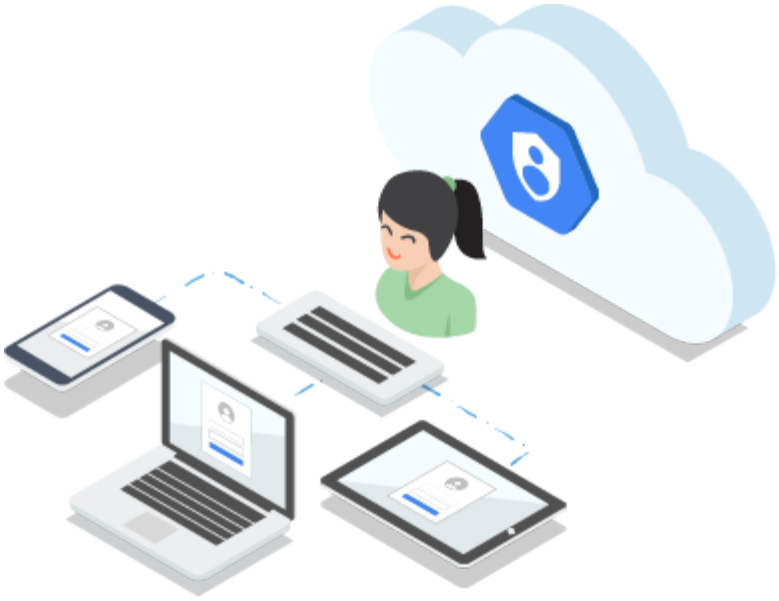
O Cloud Identity e o Access Management (Cloud IAM) permitem que você crie e gerencie permissões para recursos do Google Cloud Platform. O Cloud IAM unifica o controle de acesso aos serviços do Cloud Platform em um único sistema e apresenta um conjunto consistente de operações.

As tecnologias de identidade e gerenciamento incluem (mas não estão limitadas a) ferramentas de gerenciamento de senha, software de provisionamento, aplicativos de aplicação de políticas de segurança, relatórios e monitoramento de aplicativos e repositórios de identidades.

Controle de acesso de nível empresarial

O Cloud Identity & Access Management (Cloud IAM) permite que os administradores autorizem quem pode tomar medidas em recursos específicos, dando a você controle total e visibilidade para gerenciar

recursos de nuvem centralmente. Para empresas estabelecidas com estruturas organizacionais complexas, centenas de grupos de trabalho e potencialmente muito mais projetos, o Cloud IAM fornece uma visão unificada da política de segurança em toda a organização, com auditoria interna para facilitar os processos de conformidade.



Identidade corporativa facilitada

Aproveite o Cloud Identity, a identidade gerenciada integrada do Google Cloud para criar ou sincronizar com facilidade contas de usuários em aplicativos e projetos. Com o Cloud Identity, é fácil provisionar e gerenciar usuários e grupos, configurar o logon único e configurar a autenticação de vários fatores diretamente no Google Admin Console. Com o Cloud Identity, você obtém acesso à organização do GCP, que permite gerenciar centralmente os projetos por meio do Cloud Resource Manager.

Os papéis certos

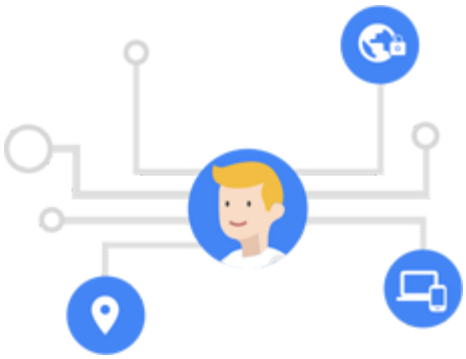
O Cloud IAM fornece as ferramentas certas para gerenciar permissões de recursos com o mínimo de barulho e alta automação. Mapeie as funções do trabalho em sua empresa para grupos e funções. Os usuários obtêm acesso apenas ao que precisam para realizar o trabalho, e os administradores podem facilmente conceder permissões padrão a grupos inteiros de usuários.

Controle de recursos granulares

O Cloud IAM permite conceder acesso a recursos da nuvem em níveis refinados, além do acesso no nível do projeto.

Acesso com reconhecimento de contexto

Crie políticas de controle de acesso mais granulares para recursos com base em atributos como status de segurança do dispositivo, endereço IP, tipo de recurso e data / hora. Essas políticas ajudam a garantir que os controles de segurança apropriados estejam em vigor ao conceder acesso aos recursos da nuvem. Inscreva-se no beta privado das condições do Cloud IAM aqui.



Simplicidade primeiro

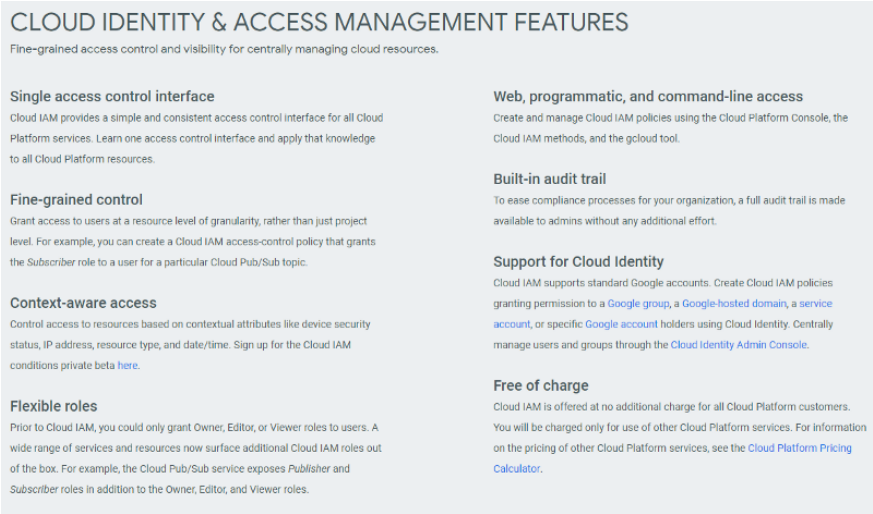
Reconhecemos que a estrutura e as políticas internas de uma organização podem se tornar complexas rapidamente. Projetos, grupos de trabalho e gerenciamento de quem tem autorização para fazer o que tudo muda dinamicamente. O Cloud IAM é projetado com a simplicidade em mente: uma interface limpa e universal permite gerenciar o controle de acesso de todos os recursos do Google Cloud Platform de forma consistente. Então você aprende uma vez e aplica em todos os lugares.

Trilha de auditoria interna

Um histórico completo da trilha de auditoria de autorização de permissões, remoção e delegação é exibido automaticamente para seus administradores. O Cloud IAM permite que você se concentre nas políticas de negócios em torno de seus recursos e facilita a conformidade.

Controle de acesso do seu jeito

Controle permissões de recursos usando uma variedade de opções: graficamente no console do Cloud Platform, programaticamente por meio dos métodos do Cloud IAM ou usando a interface de linha de comando gcloud.



Referência: https://cloud.google.com/iam/

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 os grupos do Google página inicial dos .

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

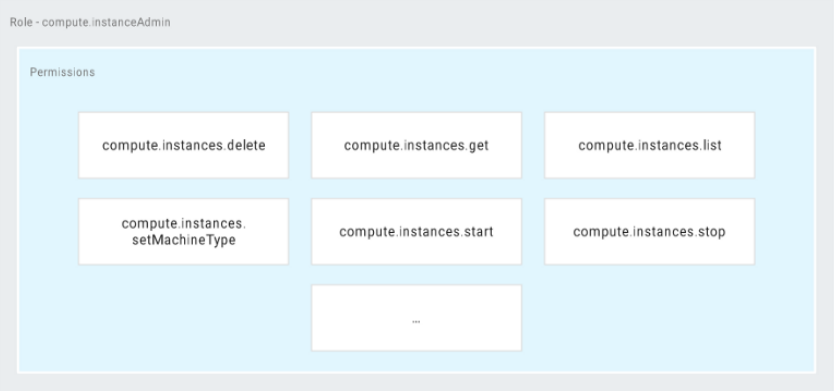
Permissões determinam quais operações são permitidas em um recurso. No mundo do Cloud IAM, as permissões são representadas na forma de `<service>.<resource>.<verb>` , por exemplo `pubsub.subscriptions.consume` .

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 do `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.



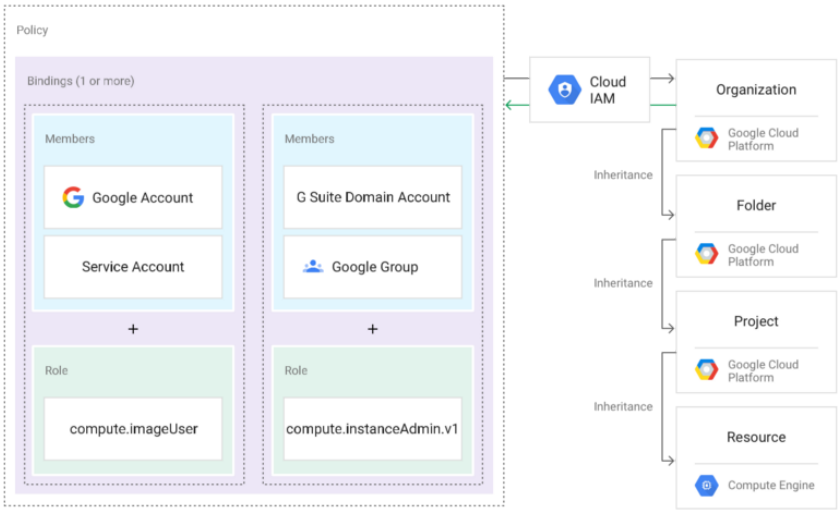
Existem três tipos de funções no Cloud IAM:

- **Papéis primitivos** : as funções historicamente disponíveis no Console do Google Cloud Platform continuarão funcionando. Estes são o **proprietário** , **editor** e **visualizador** funções de .
- **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 *somente a* publicar mensagens em um tópico do Cloud Pub / Sub.
- **Papéis personalizados**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:

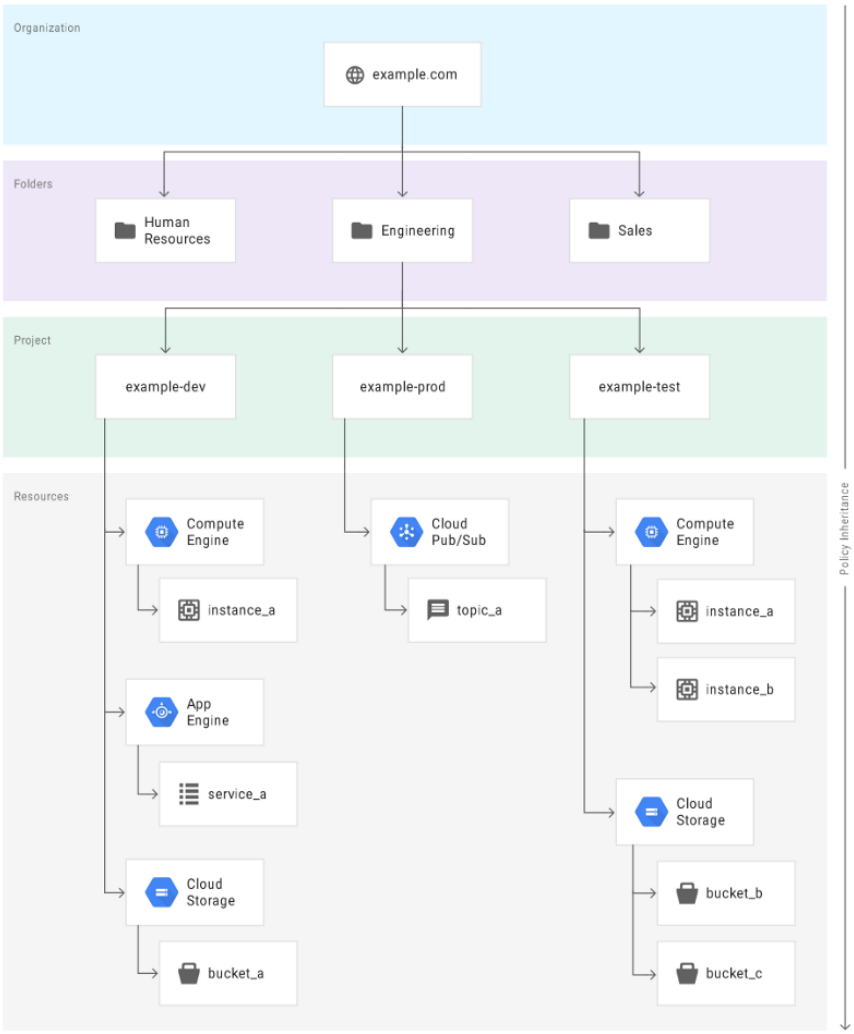
- `setIamPolicy()` : Permite que você defina políticas em seus recursos.
- `getIamPolicy()` : Permite que você obtenha uma política definida anteriormente.
- `testIamPermissions()` : Permite testar se o chamador tem as permissões especificadas para um recurso.

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 .

- -

Contas de serviço

Esta página explica as contas de serviço, os tipos de contas de serviço e as funções do IAM disponíveis para as contas de serviço.

Antes de você começar

- Entenda os conceitos básicos do Cloud IAM .

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 a 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 .

==========

Usando o IAM com segurança

Introdução

Esta página recomenda as práticas recomendadas de segurança que você deve ter em mente ao usar o Cloud IAM.

Esta página foi criada para usuários com proficiência no Cloud IAM. Se você está apenas começando com o IAM, essas instruções não ensinam como usá-lo; Em vez disso, os novos usuários devem começar com o início rápido do IAM do Cloud.

Ultimo privilégio

❑Os papéis definidos fornecem acesso mais granular do que os papéis primitivos. Conceda funções predefinidas às identidades quando possível, para que você forneça o mínimo de acesso necessário para acessar seus recursos.

❑Grandes papéis primitivos nos seguintes casos:

- quando o serviço do Cloud Platform não fornece uma função predefinida. Consulte a tabela de funções predefinidas para obter uma lista de todas as funções predefinidas disponíveis.

- quando você deseja conceder permissões mais amplas para um projeto. Isso geralmente acontece quando você concede permissões em ambientes de desenvolvimento ou teste.
- Quando você precisar permitir que um membro modifique permissões para um projeto, você deverá conceder a ele a função de proprietário, pois somente os proprietários têm permissão para conceder acesso a outros usuários para projetos.
- quando você trabalha em uma pequena equipe em que os membros da equipe não precisam de permissões granulares.

❑Trate cada componente do seu aplicativo como um limite de confiança separado. Se você tiver vários serviços que exigem permissões diferentes, crie uma conta de serviço separada para cada um dos serviços, de modo que eles possam ter permissão diferente.

❑ Lembre-se de que um conjunto de políticas em um recurso filho não pode restringir o acesso concedido a seu pai. Verifique a política concedida em todos os recursos e certifique-se de compreender a herança hierárquica.

❑Grupos papéis no menor escopo necessário. Por exemplo, se um usuário precisar apenas de acesso para publicar o tópico Pub / Sub, conceda a função de Publicador ao usuário desse tópico.

❑Restrinja quem pode atuar como contas de serviço. Os usuários que recebem a função de Ator de Conta de Serviço para uma conta de serviço podem acessar todos os recursos aos quais a conta de serviço tem acesso. Portanto, seja cauteloso ao conceder a função de Ator de Conta de Serviço a um usuário.

❑Restrinja quem tem acesso para criar e gerenciar contas de serviço em seu projeto.

❑Gerenciar o papel de proprietário para um membro permitirá modificar a política do IAM. Portanto, conceda a função de proprietário somente se o membro tiver uma finalidade legítima para gerenciar a política do IAM. Isso porque, como sua política contém dados confidenciais de controle de acesso e ter um conjunto mínimo de usuários, isso simplifica qualquer auditoria que você tenha que fazer.

Contas de serviço e chaves da conta de serviço

❑ Gere as chaves da sua conta de serviço usando a API da conta de serviço do IAM. Você pode girar uma chave criando uma nova chave, alternando os aplicativos para usar a nova chave e excluindo a chave antiga. Use o `serviceAccount.keys.create()` método e o `serviceAccount.keys.delete()` método juntos para automatizar a rotação.

❑ Implemente processos para gerenciar chaves de contas de serviço gerenciadas pelo usuário.

❑ Tenha cuidado para não confundir chaves de criptografia com chaves de conta de serviço. As chaves de criptografia geralmente são usadas para criptografar dados e as chaves da conta de serviço são usadas para acesso seguro às APIs do Google Cloud Platform.

❑Não exclua as contas de serviço que estão em uso executando instâncias. Isso pode resultar na falha total ou parcial do seu aplicativo se você não tiver feito a transição para usar uma conta de serviço alternativa primeiro.

❑Use o nome de exibição de uma conta de serviço para acompanhar o que é usado e as permissões que devem ter.

❑Não registre as chaves da conta de serviço no código-fonte ou deixe-as no diretório Downloads.

Auditoria

❑ Use os registros de auditoria da nuvem para auditar regularmente as alterações na sua política do IAM.

❑Exporte registros de auditoria para o Google Cloud Storage para armazenar seus registros por longos períodos.

❑Auditar quem tem a capacidade de alterar suas políticas do IAM em seus projetos.

❑Restrinja o acesso a registros usando as funções de registro na nuvem.

❑Aplique as mesmas políticas de acesso ao recurso do Cloud Platform que você usa para exportar logs conforme aplicado ao visualizador de registros.

❑ Use os registros de auditoria da nuvem para auditar regularmente o acesso às chaves da conta de serviço.

Gerenciamento de políticas

❑Configure as políticas do IAM no nível da organização para conceder acesso a todos os projetos da sua organização.

❑Gerenciar papéis para um grupo do Google em vez de para usuários individuais, quando possível. É mais fácil adicionar membros e remover membros de um grupo do Google em vez de atualizar uma política do Cloud IAM para adicionar ou remover usuários.

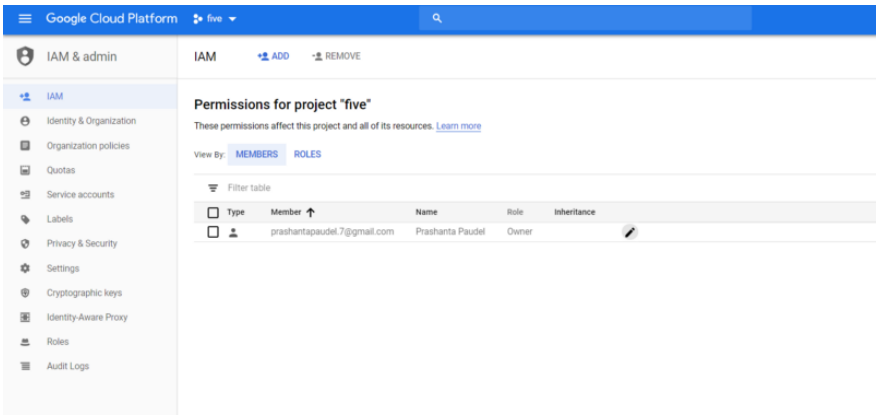
❑Se você precisar conceder várias funções para permitir uma tarefa específica, crie um grupo do Google, conceda as funções a esse grupo e adicione usuários a esse grupo.

==========

Agora vamos voltar para as principais tarefas em curso

Visualizar atribuições de IAM da conta

Para ver as atribuições do IAM para uma conta de usuário específica, acesse o IAM na página principal e verifique o painel



EU SOU

> *da Shell*

$ gcloud iam roles list

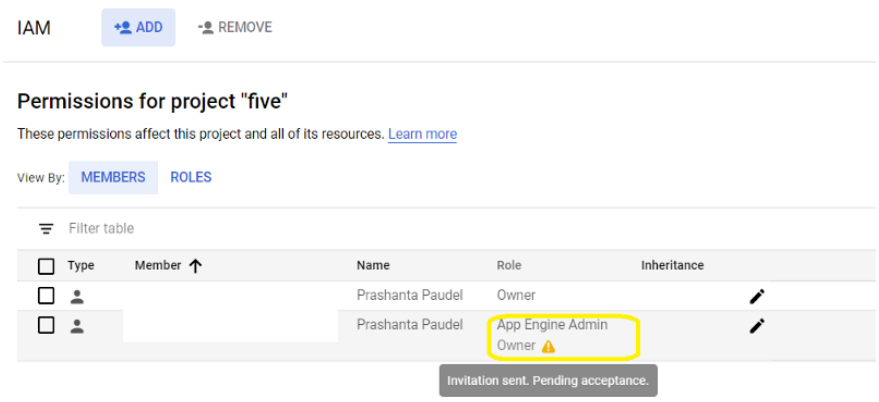
==========

Atribuindo funções do IAM a contas ou Grupos do Google

Primeiro, vá para IAM e Serviços

Em seguida, clique em ADICIONAR e siga o aviso.

Atribuir novas funções de usuário



Precisa de aceitação do convite.

Adicionando o grupo do Google ao IAM

adicionar grupo

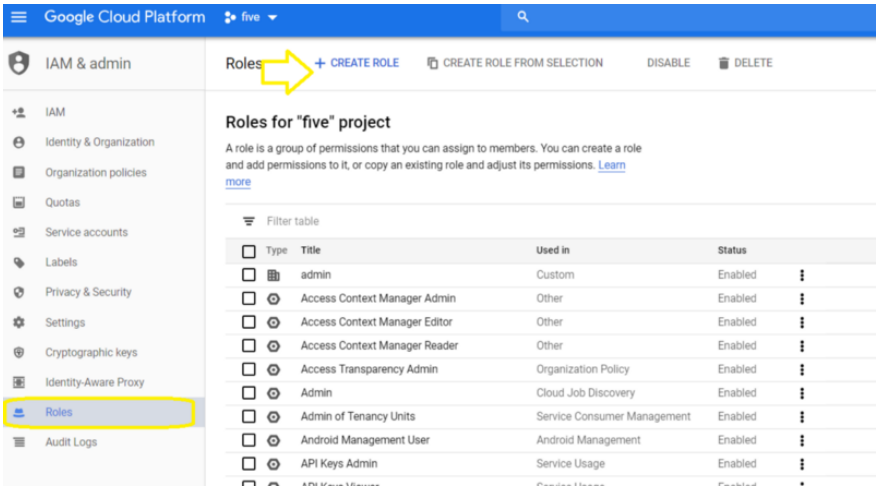
> *Com casca*

```
$ gcloud projects add-iam-policy-binding five-222414  --
member user:praspaudel@gmail.com --role roles/viewer
bindings:
- members:
  - user:praspaudel@gmail.com
  role: roles/appengine.appAdmin
- members:
  - group:prashantapaudel@googlegroups.com
  role: roles/bigquery.admin
- members:
  - user:prashantapaudel.7@gmail.com
  - user:praspaudel@gmail.com
  role: roles/owner
- members:
  - group:prashantapaudel@googlegroups.com
  - user:praspaudel@gmail.com
  role: roles/viewer
etag: BwV6jYg5HT4=
version: 1
prashantapaudel_7@cloudshell:~ (five-222414)$
```

———————————————————————————————————————

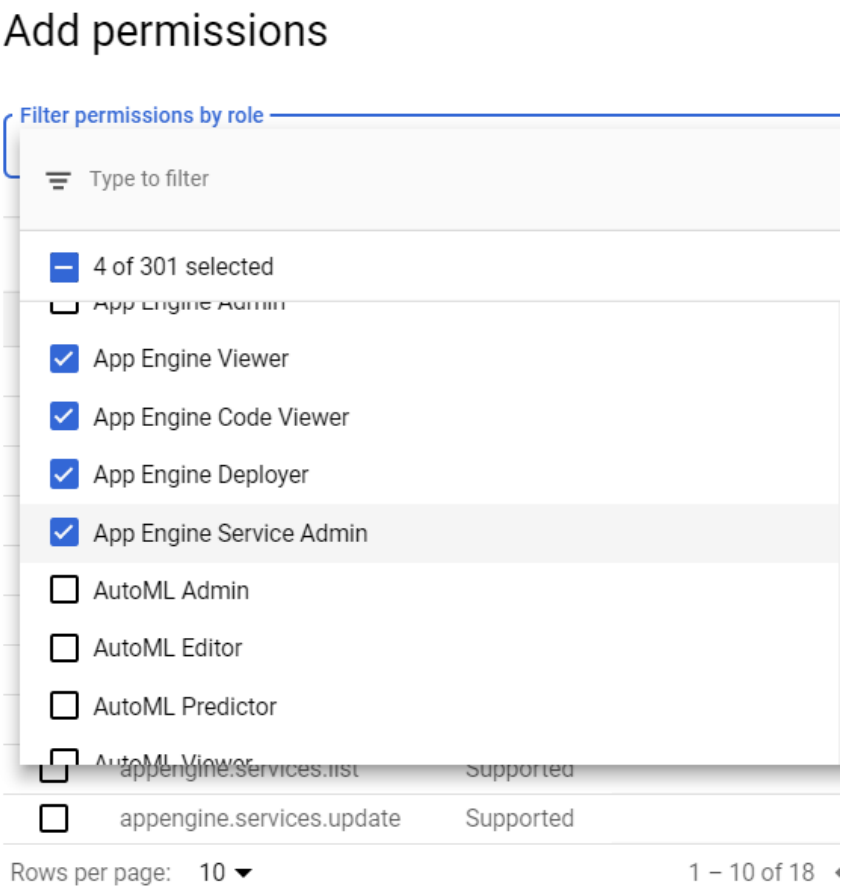
Defining custom IAM roles

First go to IAM and Services, then to Roles as shown below

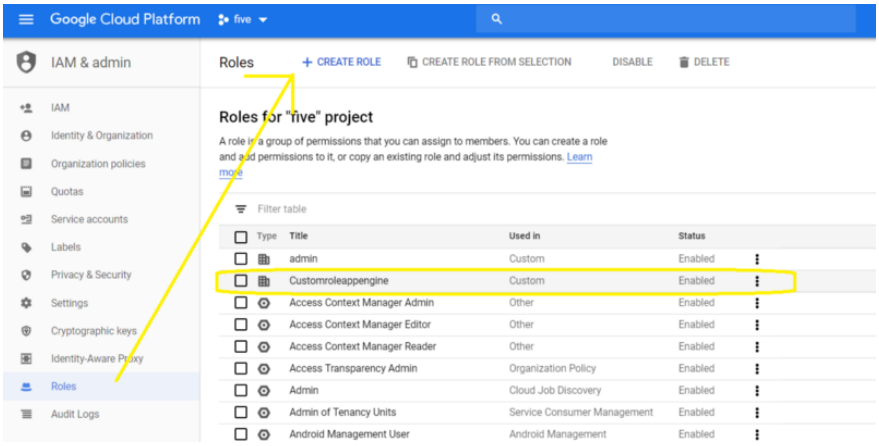


Roles

Now, I created a new role called *customrole* and added permission to operate in App engine only.

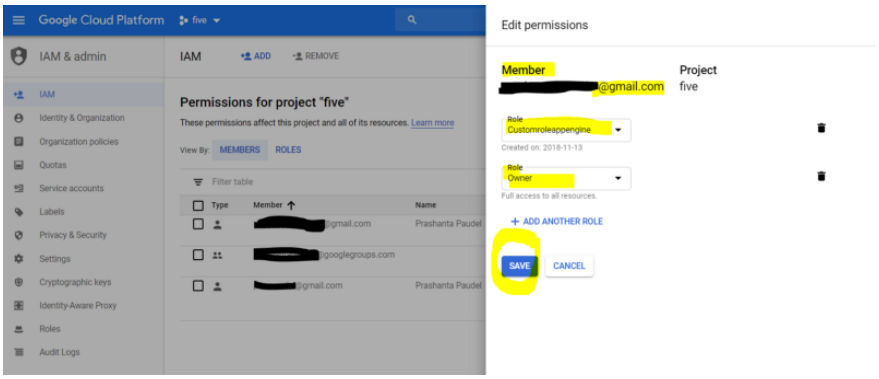


permissions



new created custom role

Now let's try to apply to a new user



new role to a new user

After implementing the role, it is seen in the IAM page which can be changed or revoked anytime.

This can be done in Shell also but will be bit complex.