

Série de Certificação GCP, 1.1



Prashanta Paudel

12 de outubro de 2018 · 13 min de leitura

Desta série, estarei tentando passar por seções na Certificação GCP e documentar as etapas para executar as tarefas mencionadas no subtítulo.

O Google mencionou o Associate Cloud Engineer como aquele que poderia realizar as seguintes tarefas

Associate Cloud Engineer

Um Engenheiro de Nuvem Associado implanta aplicativos, monitora operações e gerencia soluções corporativas. Esse indivíduo pode usar o Google Cloud Console e a interface da linha de comando para executar tarefas comuns baseadas em plataforma para manter uma ou mais soluções implantadas que aproveitam serviços gerenciados pelo Google ou autogerenciados no Google Cloud.

O exame Associate Cloud Engineer avalia sua capacidade de:

- Configurar um ambiente de solução em nuvem
- Planeje e configure uma solução de nuvem
- Implantar e implementar uma solução em nuvem
- Garanta o sucesso da operação de uma solução de nuvem
- Configurar acesso e segurança

Toda a Certificação é dividida em 5 seções e outras subseções. Meu plano é passar por cada subseção para que o aprendizado seja fácil e peça por peça.

Então, hoje vamos passar pela seção 1.1 da seção 1.

Antes de ir diretamente para a seção 1.1, devemos ter informações sobre a hierarquia de recursos do GCP. O objetivo é vincular os recursos

ao proprietário e manter a herança de propriedade, além de fornecer controle de acesso e política para os recursos.

Geralmente, podemos comparar a hierarquia de recursos com o sistema de arquivos no sistema operacional tradicional. Essa organização hierárquica de recursos permite que você defina políticas de controle de acesso e definições de configuração em um recurso pai, e as políticas e as configurações do IAM são herdadas pelos recursos filhos.

Google diz:

No nível mais baixo, os recursos são os componentes fundamentais que compõem todos os serviços do GCP. Exemplos de recursos incluem máquinas virtuais do Compute Engine (VMs), tópicos do Cloud Pub / Sub, intervalos do Cloud Storage, instâncias do App Engine. Todos esses recursos de nível inferior só podem ser criados por projetos, que representam o primeiro mecanismo de agrupamento da hierarquia de recursos do GCP.

Os clientes do G Suite e do Cloud Identity têm acesso a recursos adicionais da hierarquia de recursos do GCP que oferecem benefícios, como visibilidade e controle centralizados, além de outros mecanismos de agrupamento, como pastas. Lançamos a ferramenta de gerenciamento do Cloud Identity. Para detalhes sobre como usar o Cloud Identity, consulte [Migração para o Cloud Identity](#).

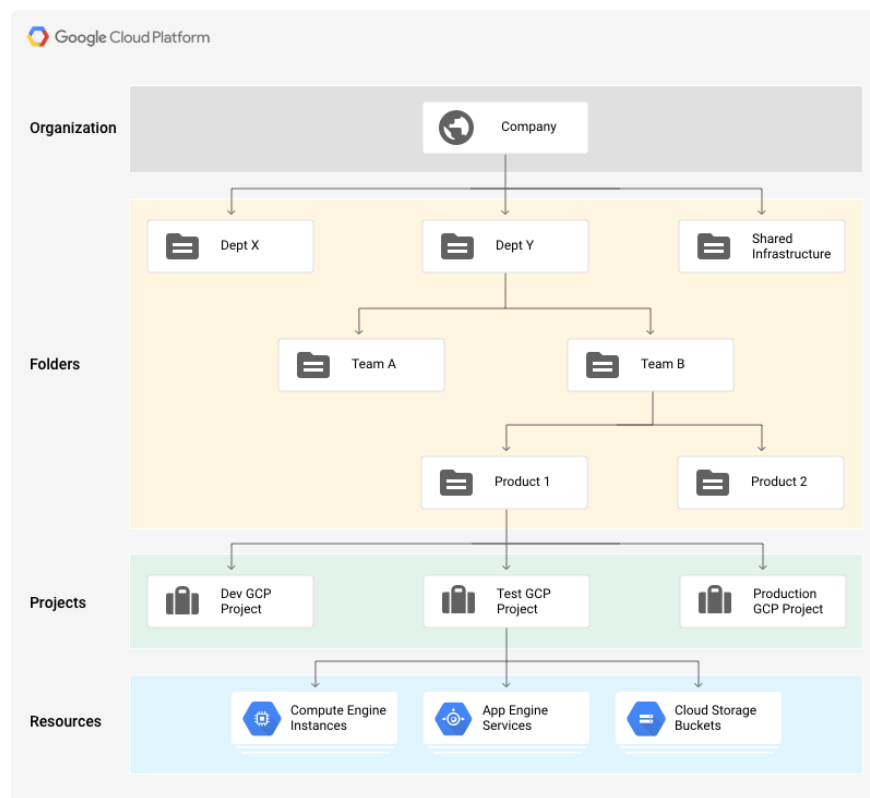
Os recursos do GCP são organizados hierarquicamente. Começando na parte inferior da hierarquia, os projetos são o primeiro nível e contêm outros recursos. Todos os recursos devem pertencer a exatamente um projeto.

O recurso Organização é o nó raiz da hierarquia de recursos do GCP e todos os recursos pertencentes a uma organização são agrupados no nó da organização. Isso fornece visibilidade central e controle sobre todos os recursos que pertencem a uma organização.

Pastas são um mecanismo de agrupamento adicional em cima de projetos. Você é obrigado a ter um recurso da Organização como um pré-requisito para o uso de pastas. Pastas e projetos são todos mapeados no recurso Organização.

A hierarquia de recursos do GCP, especialmente em sua forma mais completa, que inclui recursos e pastas da organização, permite que as empresas mapeiem sua organização para o GCP e fornece pontos de anexação lógicos para políticas de gerenciamento de acesso e políticas da organização. As políticas do Cloud IAM e da Organização são herdadas por meio da hierarquia, e a política efetiva em cada nó da hierarquia é o resultado de políticas aplicadas diretamente no nó e políticas herdadas de seus ancestrais.

O diagrama abaixo representa uma hierarquia de recursos de exemplo do GCP em forma completa:



Seção 1: Configurando um ambiente de solução em nuvem

1.1 Configurando projetos e contas na nuvem. Atividades incluem:

- Criando projetos.
- Atribuindo usuários a funções do IAM predefinidas em um projeto.
- Vinculando usuários a identidades do G Suite.

- Ativando APIs nos projetos.
- Provisionamento de uma ou mais contas do Stackdriver.

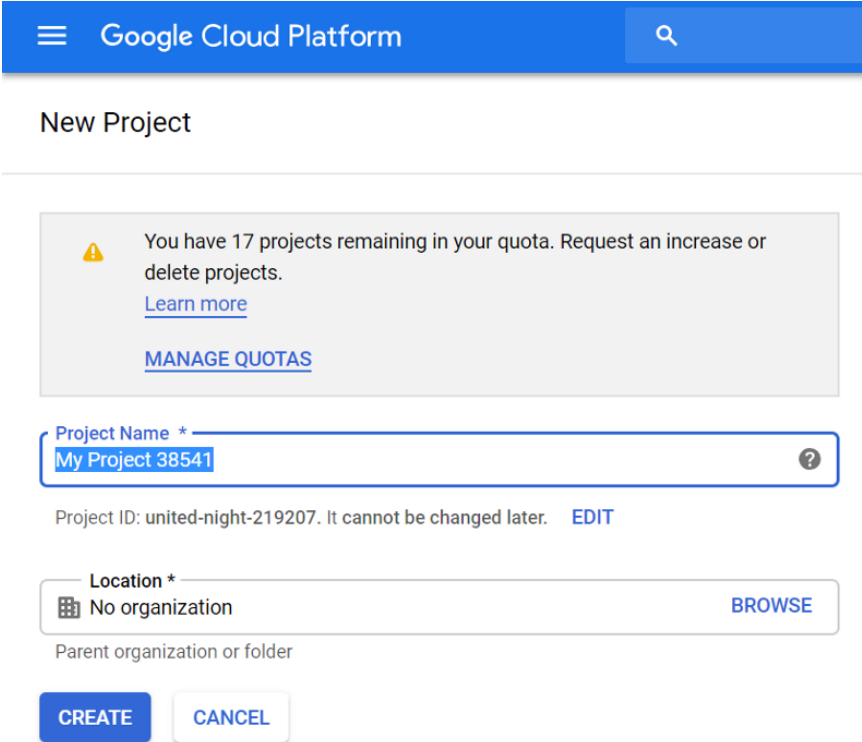
Criando o projeto

A coisa mais básica a fazer no GCP é criar o projeto. Criar o projeto em si não completa nada, mas ele irá iniciar o processo para que você possa adicionar entidades no projeto e construir sua própria rede, criar um banco de dados, escrever código, construir um servidor, etc.

O número do projeto e o código do projeto são exclusivos no Google Cloud Platform. Se outro usuário tiver um ID de projeto para o projeto, você não poderá usar o mesmo ID de projeto. Além disso, o nome como Google ou SSL não pode ser usado para o nome do projeto.

Todas as instâncias estão anexadas ao projeto. Então, você entendeu que tudo está dentro do projeto.

Para criar o projeto, primeiro você precisa ter acesso ao console na nuvem.



The screenshot shows the 'New Project' form in the Google Cloud Platform console. At the top is a blue header with the Google Cloud Platform logo and a search icon. Below the header, the title 'New Project' is displayed. A warning box indicates that the user has 17 projects remaining in their quota and provides links to 'Learn more' and 'MANAGE QUOTAS'. The 'Project Name' field is required and contains the text 'My Project 38541'. Below this, the 'Project ID' is shown as 'united-night-219207', with a note that it cannot be changed later and an 'EDIT' link. The 'Location' field is required and currently shows 'No organization' with a 'BROWSE' button. At the bottom, there are 'CREATE' and 'CANCEL' buttons.

criar projeto

Se você está executando uma conta gratuita, você deve selecionar "individual" ao criar a própria conta. Usuários gratuitos recebem cota limitada, portanto, se o número de projetos que podem ser criados for menor que 30, você receberá a mensagem mostrada acima.

O nome do projeto é um nome legível para a simplicidade, enquanto todo o processamento será feito usando o ID do projeto mencionado logo abaixo do nome do projeto.

Você pode estar trabalhando no console para mais de um projeto, portanto, é sempre uma boa idéia verificar o nome do projeto durante a execução de tarefas.

Para criar um novo projeto, use o `gcloud projects create` comando:

```
gcloud projects create PROJECT_ID
```

Por exemplo

```
prashantagcppaudel @ cloudshell: ~ (webproject-217416) $  
gcloud projetos create testdemotrial123  
Crie em andamento para  
[https://cloudresourcemanager.googleapis.com/v1/projects/testdemotrial123].  
Esperando por [operations / cp.6134727994789518289] terminar  
... pronto.
```

Onde PROJECT_ID é o ID do projeto que você deseja criar. Um ID de projeto deve começar com uma letra minúscula e pode conter apenas letras ASCII, dígitos e hífens e deve ter entre 6 e 30 caracteres.

Para criar um projeto com uma organização (não para uma conta gratuita) ou uma pasta como pai, use

```
--organization OU --folder bandeiras.
```

Como um recurso pode ter apenas um pai, apenas um desses sinalizadores pode ser usado:

```
gcloud projects create PROJECT_ID --organization=ORGANIZATION_ID
```

```
gcloud projects create PROJECT_ID --folder=FOLDER_ID
```

Para verificar os metadados do projeto, consulte o Painel de controle do projeto ou use

```
# gcloud projects describe PROJECT_ID
```

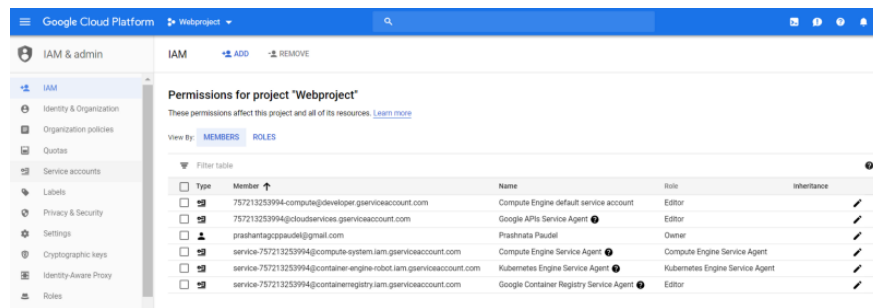
```
root @-devshell-vm-4663cdf8-e36b-46af-a81b-16d2c81e115c CS-6000: projetos # gcloud / home / prashantagcpaudel  
descrever testdemotrial123  
CreateTime: '2018-10-12T07: 50: 46.560Z'  
lifecycleState: ACTIVE  
nome: testdemotrial123  
projectId : testdemotrial123  
projectNumber: '376521124726'
```

Atribuindo usuários a funções do IAM predefinidas em um projeto

Quando um novo projeto é criado, a conta usada no GCP automaticamente obtém o acesso do proprietário. Existem poucos tipos de acesso de usuário padrão ou funções.

1. Navegador
2. editor
3. Proprietário
4. Visualizador

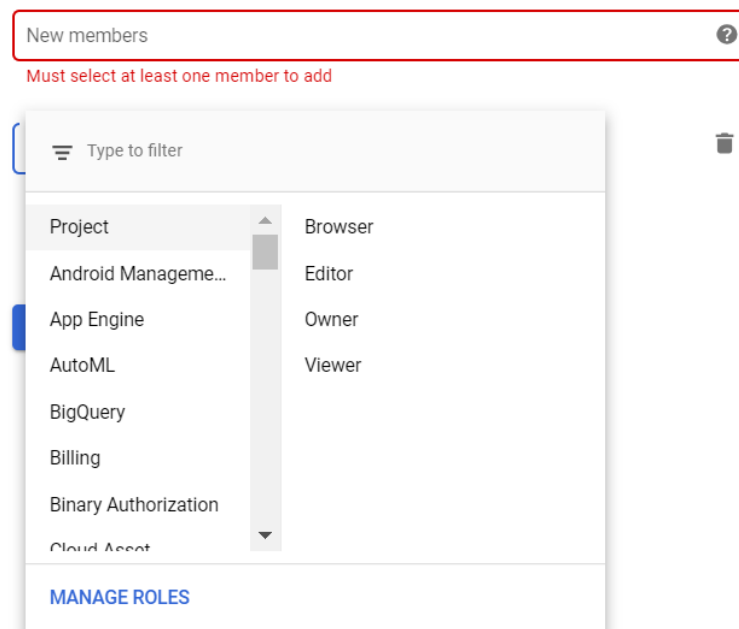
Depois que o projeto for criado, clique no projeto e, em seguida, em IAM e Admin para acessar a página Gerenciamento de identidade e acesso.



quando você clica em ADICIONAR, você terá a opção de adicionar usuários ao projeto. Aqui você verá várias opções para incluir acesso a projetos e faturamentos. Selecione o projeto e, em seguida, digite o tipo de acesso.

Add members, roles to "Webproject" project

Enter one or more members below. Then select a role for these members to grant them access to your resources. Multiple roles allowed. [Learn more](#)



Google diz:

Com o Cloud IAM, todos os métodos do Google Cloud Platform exigem que a conta que faz a solicitação da API tenha permissões apropriadas para acessar o recurso. As permissões permitem que os usuários executem ações específicas nos recursos do Cloud. Por exemplo, a `resourcemanager.projects.list` permissão permite que um usuário liste os projetos que possui, enquanto

`resourcemanager.projects.delete` permite que um usuário exclua um projeto.

A tabela a seguir lista as permissões que o chamador deve ter para chamar uma API de projetos:

Method	Required Permission(s)
<code>resourcemanager.projects.create()</code>	<code>resourcemanager.projects.create</code>
<code>resourcemanager.projects.delete()</code>	<code>resourcemanager.projects.delete</code>
<code>resourcemanager.projects.get()</code>	<code>resourcemanager.projects.get</code>
<code>resourcemanager.projects.getIamPolicy()</code>	<code>resourcemanager.projects.getIamPolicy</code>
<code>resourcemanager.projects.list()</code>	Does not require any permission. The method lists projects for which the caller has <code>resourcemanager.projects.get</code> permission. If you provide a filter while calling <code>list()</code> , for example, <code>byParent</code> , the method lists projects for which you have the <code>resourcemanager.projects.get</code> permission and which satisfies the filter condition.
<code>resourcemanager.projects.setIamPolicy()</code>	<code>resourcemanager.projects.setIamPolicy</code>
<code>resourcemanager.projects.testIamPermissions()</code>	Does not require any permission.
<code>resourcemanager.projects undelete()</code>	<code>resourcemanager.projects undelete</code>
<code>resourcemanager.projects.update()</code>	To update a project's metadata, requires <code>resourcemanager.projects.update</code> permission. To update a project's parent and move the project into an organization, requires <code>resourcemanager.projects.create</code> permission on the organization.

Você não dá permissões diretamente aos usuários; em vez disso, você concede a eles *funções*, que têm uma ou mais permissões agrupadas dentro delas.

Você pode conceder uma ou mais funções no mesmo projeto. Ao usar o `resourcemanager.projects.getIamPolicy()` método para exibir permissões, somente as permissões atribuídas ao projeto serão exibidas, não as permissões herdadas.

Utilizando Funções Predefinidas

A tabela a seguir lista as funções que você pode conceder para acessar um projeto, a descrição do que a função faz e as permissões agrupadas nessa função.

Role	Description	Permissions
roles/owner	Full access to all resources.	All permissions for all resources.
roles/editor	Edit access to all resources.	Create and update access for all resources.
roles/viewer	Read access to all resources.	Get and list access for all resources.
roles/browser ^{Beta}	Access to browse resources in the project.	<ul style="list-style-type: none"> • resourcemanager.organizations.get • resourcemanager.projects.get • resourcemanager.projects.getIamPolicy • resourcemanager.projects.list • resourcemanager.projectInvites.get

Proteção contra exclusão acidental

Para proteger qualquer proprietário / administrador acidentalmente excluir o projeto, o GCP possui um recurso chamado privilégios. Você pode usar penhoras no projeto para bloquear a exclusão de projetos até que seja revogado. A maneira mais fácil de usar liens é o shell gcloud

Colocar liens

Para colocar uma garantia em um projeto, um usuário deve ter a `resourcemanager.projects.updateLiens` permissão que é concedida pelas funções `roles/owner` e `roles/resourcemanager.lienModifier`.

```
gcloud alpha resource-manager liens create \
  --restrictions=resourcemanager.projects.delete \
  --reason="Super important production system"
```

Os parâmetros disponíveis `liens create` são:

- `--project` - O projeto ao qual a garantia se aplica.
- `--restrictions` - Uma lista separada por vírgulas de permissões do IAM a serem bloqueadas.
- `--reason` - Uma descrição legível por humanos da razão pela qual esta garantia existe.
- `--origin` - Uma cadeia curta denotando o usuário / sistema que originou o penhor. Obrigatório, mas a ferramenta gcloud a

preencherá automaticamente com o endereço de e-mail do usuário, se deixado de fora.

Atualmente, a única restrição válida para um projeto é

```
resourcemanager.projects.delete .
```

Listando liens em um projeto

Para listar liens aplicados a um projeto, um usuário deve ter a

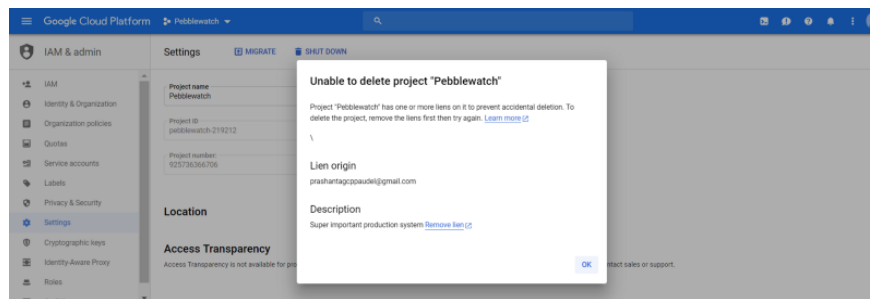
`resourcemanager.projects.get` permissão. Use o `liens list` comando `gcloud`.

```
gcloud alpha resource-manager liens list
```

Aqui está um exemplo de saída para este comando:

```
gcloud alpha resource-manager liens list
NAME                                     ORIGIN
REASON
p1061081023732-l3d8032b3-ea2c-4683-ad48-5ca23ddd00e7
user@example.com testing
```

Se você tentar excluir o projeto, será exibida uma mensagem de erro



Remoção de ônus de um projeto

Para remover um penhor de um projeto, um usuário deve ter a

`resourcemanager.projects.updateLiens` permissão concedida por

roles/owner e roles/resource-manager.lienModifier .

```
gcloud alpha gerenciador de recursos liens delete  
[LIEN_NAME]  
  
gcloud alpha resource-manager liens excluir p925736366706-  
lb2d80913-a41b-47a4-b4af-799489f09f96  
Excluído [liens / p925736366706-lb2d80913-a41b-47a4-b4af-  
799489f09f96].
```

Onde:

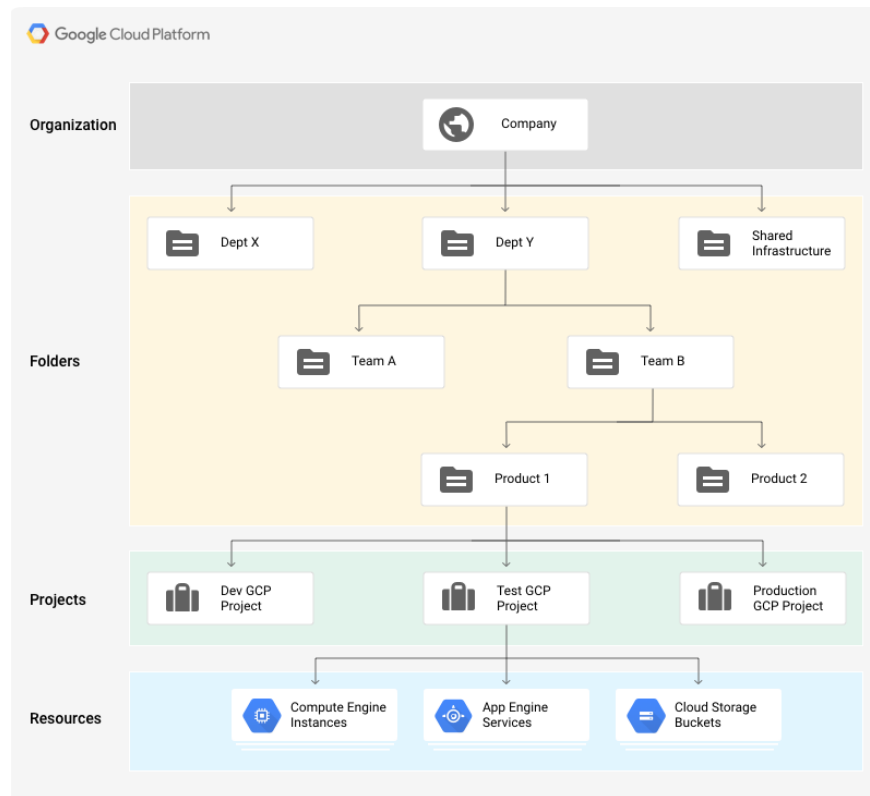
- [LIEN_NAME] é o nome da garantia a ser excluída.

Herança de políticas do IAM

O Google Cloud Platform oferece IAM (Cloud Identity and Access Management) , que permite atribuir acesso granular a recursos específicos do Google Cloud Platform e impede o acesso indesejado a outros recursos. O IAM permite controlar quem (**usuários**) tem quais acessos (**funções**) para quais **recursos** , definindo políticas do IAM nos recursos.

Você pode definir uma política do IAM no nível da organização , no nível da pasta , no nível do projeto ou (em alguns casos) no nível do recurso. Os recursos herdam as políticas do nó pai. Se você definir uma política no nível da Organização, ela será herdada por todas as suas pastas e 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 no recurso e a política herdada de seus ancestrais. Esta herança é transitiva. Em outras palavras, os recursos herdam as políticas do projeto, que herdam as políticas da organização. Portanto, as políticas no nível da organização também se aplicam no nível do recurso.



Por exemplo, no diagrama de hierarquia de recursos acima, se você definir uma política na pasta “Dept Y” que concede a função do Editor de projeto a bob@example.com, então Bob terá a função de editor nos projetos “Dev GCP”, “Test GCP, "E" Produção ". Por outro lado, se você atribuir alice@example.com a função de administrador da instância no projeto "Test GCP ", ela poderá gerenciar apenas as instâncias do Compute Engine nesse projeto.

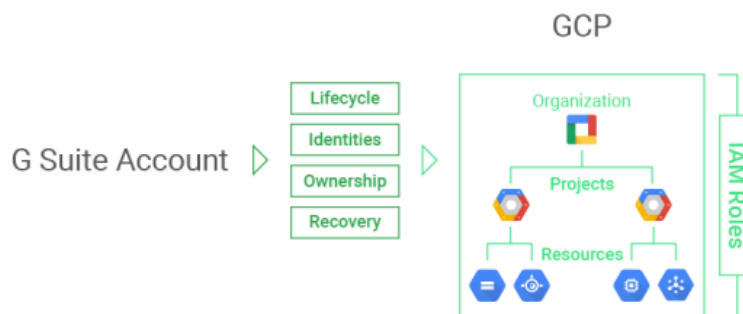
A hierarquia de políticas do IAM segue o mesmo caminho da hierarquia de recursos do GCP. Se você alterar a hierarquia de recursos, a hierarquia de políticas também será alterada. Por exemplo, mover um projeto para uma organização atualizará a política do IAM do projeto para herdar da política do IAM da organização. Da mesma forma, mover um projeto de uma pasta para outra alterará as permissões herdadas. As permissões que foram herdadas pelo projeto do pai original serão perdidas quando o projeto for movido para uma nova pasta. As permissões definidas na pasta de destino serão herdadas pelo projeto conforme são movidas.

Vinculando usuários a identidades do G Suite

Se um novo usuário quiser ter acesso aos recursos, ele já deve ter uma conta de identidade G-Suite ou Cloud para acessar esses recursos. O G-Suite geralmente representa uma empresa e é um pré-requisito para acessar os recursos da organização.

Google diz:

A conta do G Suite ou do Cloud Identity representa uma empresa e é um pré-requisito para ter acesso ao recurso da organização. No contexto do GCP, ele fornece gerenciamento de identidade, mecanismo de recuperação, propriedade e gerenciamento do ciclo de vida. A figura abaixo mostra o link entre a conta do G Suite, o Cloud Identity e a hierarquia de recursos do GCP.



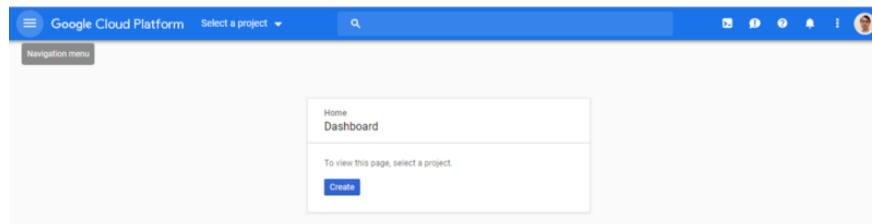
O superadministrador do G Suite é o responsável pela verificação da propriedade do domínio e o contato em casos de recuperação. Por esse motivo, o superadministrador do G Suite tem a capacidade de atribuir funções do Cloud IAM por padrão. A principal função do superadministrador do G Suite em relação ao GCP é atribuir a função de IAM do administrador da organização a usuários apropriados em seu domínio. Isso criará a separação entre as responsabilidades de administração do G Suite e do GCP que os usuários normalmente procuram.

Os usuários do GCP não precisam ter um recurso da organização. Um usuário adquire um recurso Organização somente se ele também for cliente do G Suite ou do Cloud Identity. O recurso Organização está intimamente associado a uma conta do G Suite ou do Cloud Identity. Cada conta do G Suite ou do Cloud Identity pode ter exatamente uma

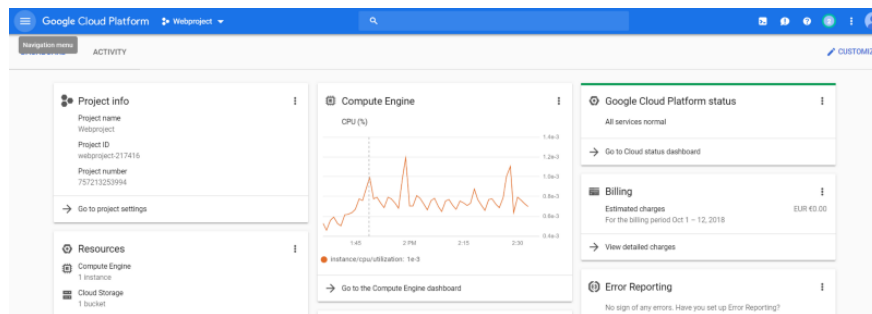
Organização provisionada com ele. Depois que um recurso da organização é criado para um domínio, todos os projetos do GCP criados por membros do domínio da conta pertencerão, por padrão, ao recurso Organização.

Por exemplo

Este usuário não foi associado a nenhum projeto ou G-Suit.



Agora vou dar acesso ao projeto de outro usuário, como mostrado abaixo. Este projeto tem um mecanismo de computação e 1 armazenamento em nuvem.



Adicionar usuário como mostrado anteriormente

Add members to "Webproject"

Add members, roles to "Webproject" project

Enter one or more members below. Then select a role for these members to grant them access to your resources. Multiple roles allowed. [Learn more](#)

New members

@gmail.com

✕

?

Role

Owner

▼

Full access to all resources.

+

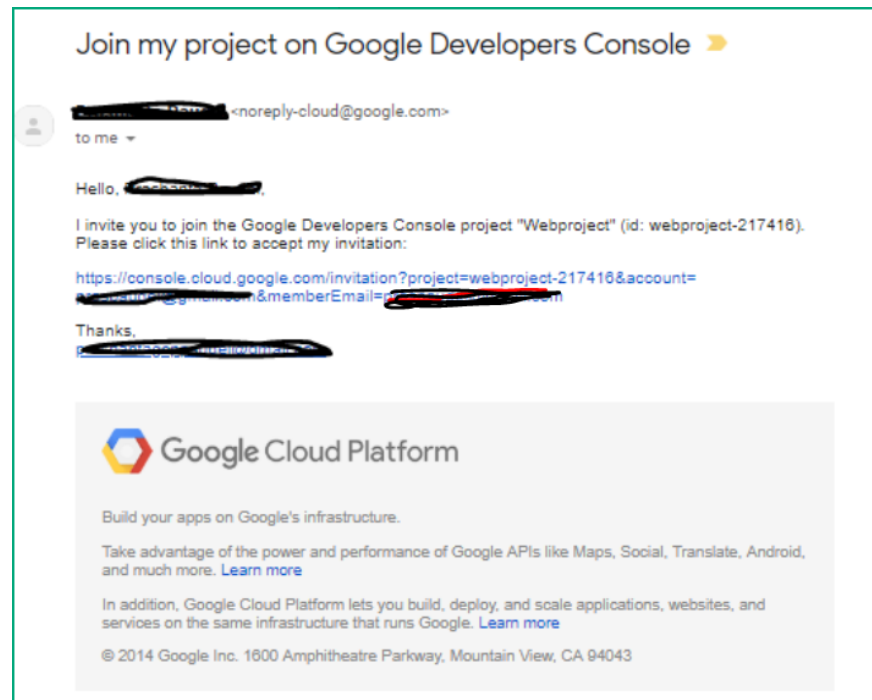
ADD ANOTHER ROLE

SAVE

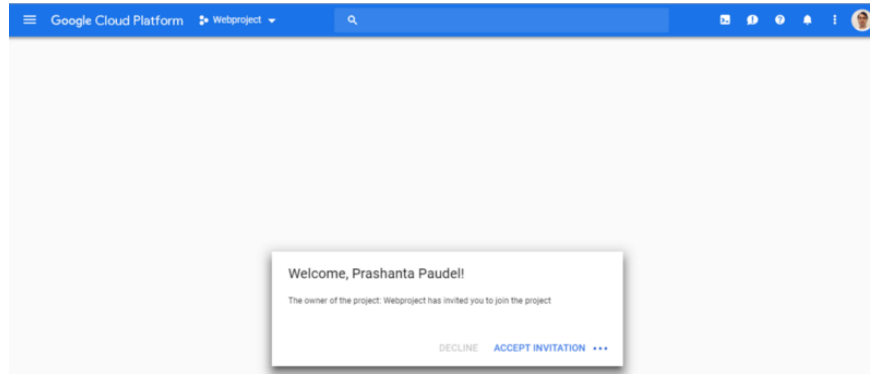
CANCEL

Aqui eu dei acesso ao projeto como um todo, por isso deve ser acessível a partir do primeiro usuário.

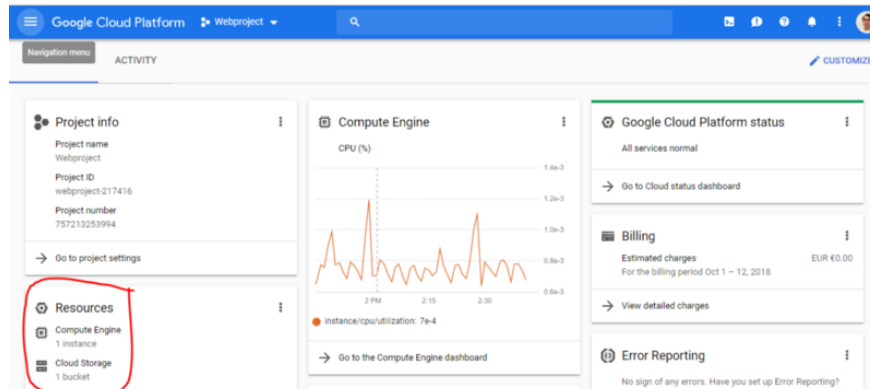
O usuário convidado receberá um e-mail solicitando a aceitação do convite, conforme mostrado abaixo



quando o link for clicado, você será redirecionado para o console e o projeto será exibido como mostrado abaixo.



Além disso, observe que as instâncias do projeto também estão listadas nos recursos disponíveis para o usuário.

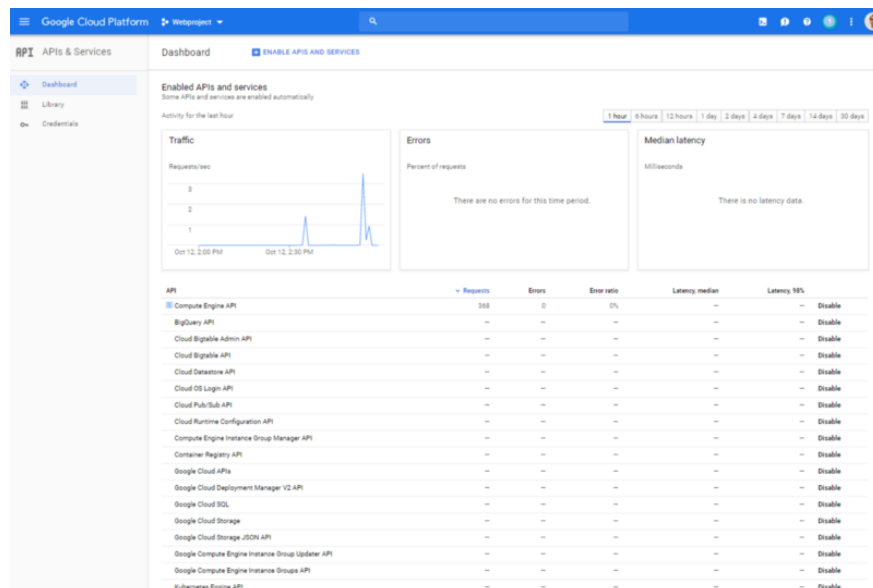
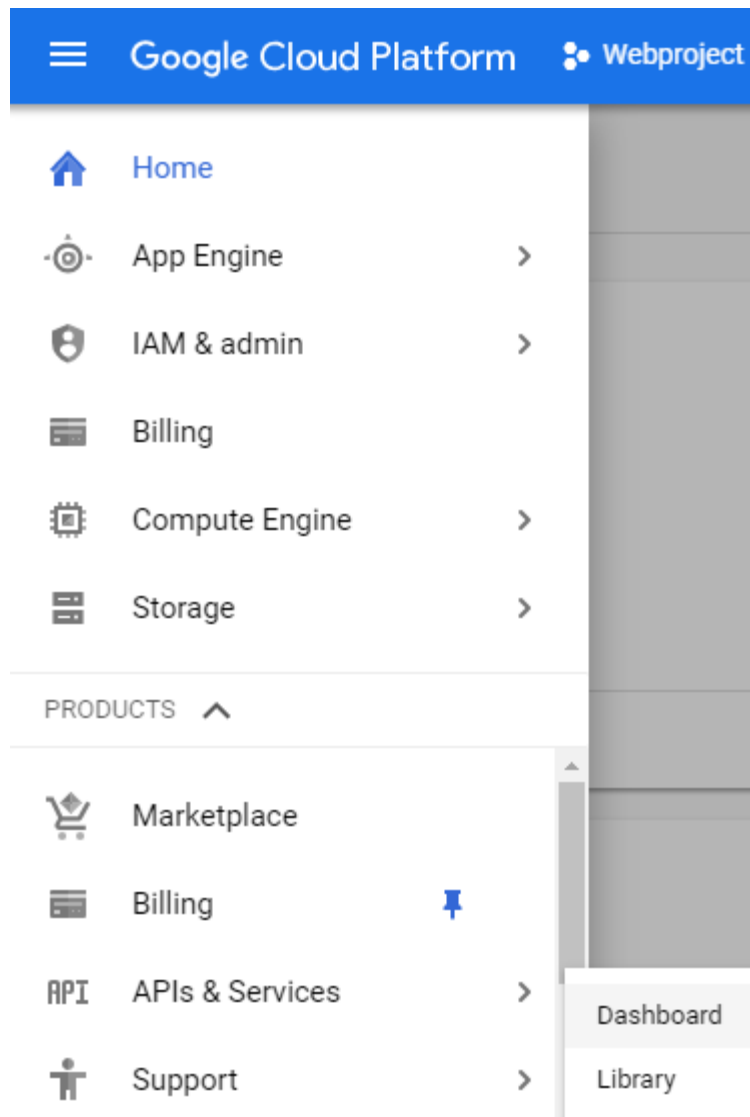


O segundo usuário pode criar, excluir e modificar instâncias se ele tiver acesso adequado.

Se acidentalmente você se remover do projeto e não houver outros usuários no projeto, você será bloqueado do projeto.

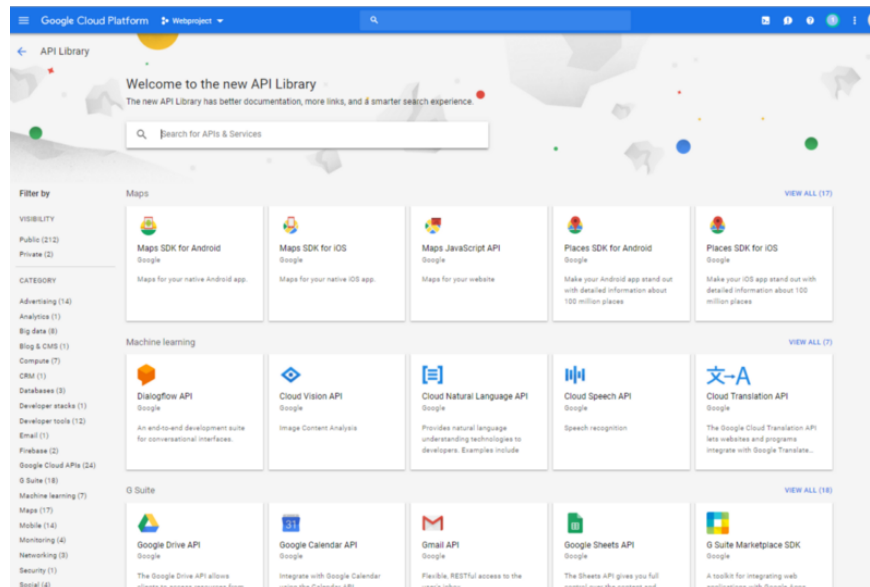
Ativando APIs nos projetos.

Todas as APIs estão acessíveis na página da consola > página API e serviços. depois de clicar em API e serviços, você será apresentado ao painel da API.

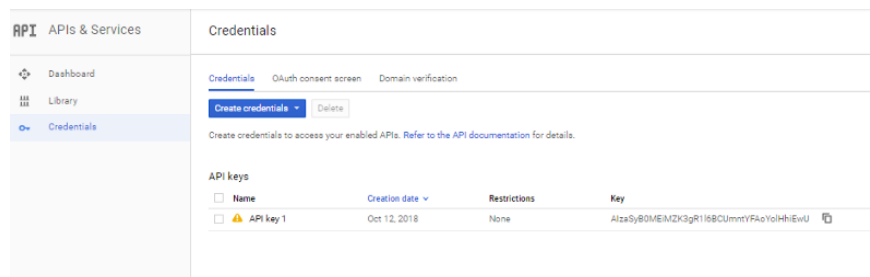


Para ativar a nova API, clique no botão Desativar à direita de cada linha.

Você também pode selecionar na biblioteca de APIs listadas na seção Biblioteca.



Outra parte importante é credenciais, para usar qualquer API você precisa ter credenciais válidas. Para encontrar as chaves para autenticar os usos da API, você pode adicionar e remover credenciais da lista.



Google diz:

Restaurando um projeto

Os proprietários do projeto podem restaurar um projeto excluído dentro do período de recuperação de 30 dias que começa quando o projeto é encerrado. Restaurar um projeto o retorna ao estado em que estava antes de ser desligado. Os recursos do Cloud Storage são

excluídos antes do final do período de 30 dias e podem não ser totalmente recuperáveis.

Alguns serviços podem precisar ser reiniciados manualmente. Para mais informações, consulte [Reiniciar os serviços do Google Cloud Platform](#).

Para restaurar um projeto:

1. Vá para a página **Gerenciar recursos** no Console do Google Cloud Platform.
2. [IR PARA A PÁGINA DE GERENCIAMENTO DE RECURSOS](#)
3. No menu suspenso **Organização**, na parte superior esquerda, selecione sua organização.
4. Abaixo da lista de projetos, clique em **Recursos com exclusão pendente**.
5. Marque a caixa do projeto que você deseja restaurar e clique em **Restaurar**. Na caixa de diálogo exibida, confirme que você deseja restaurar o projeto.

Provisionamento de uma ou mais contas do Stackdriver

Primeiro, vamos verificar o que é o driver da pilha

This embedded content is from a site that does not comply with the Do Not Track (DNT) setting now enabled on your browser.

Please note, if you click through and view it anyway, you may be tracked by the website hosting the embed.

[Learn More about Medium's DNT policy](#)

This embedded content is from a site that does not comply with the Do Not Track (DNT) setting now enabled on your browser.

Please note, if you click through and view it anyway, you may be tracked by the website hosting the embed.

Learn More about Medium's DNT policy

Instale os agentes do Stackdriver recomendados

Obtenha o máximo do seu espaço de trabalho gratuito instalando os agentes do Stackdriver Monitoring and Logging em cada uma das suas instâncias de VM. Os agentes coletam mais informações de suas instâncias de VM, incluindo métricas e registros de aplicativos de terceiros:

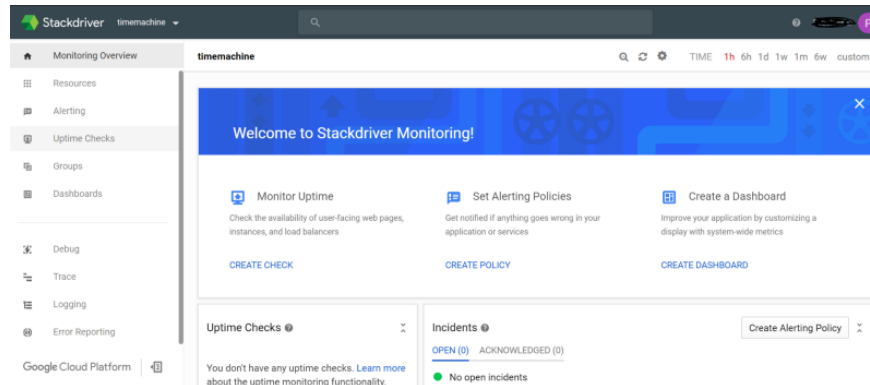
1. Alterne para o terminal conectado à sua instância de VM ou crie um novo.
2. Instale os agentes do Stackdriver executando os seguintes comandos em sua instância:

```
# To install the Stackdriver monitoring agent:
$ curl -sSO https://dl.google.com/cloudagents/install-monitoring-agent.sh
$ sudo bash install-monitoring-agent.sh

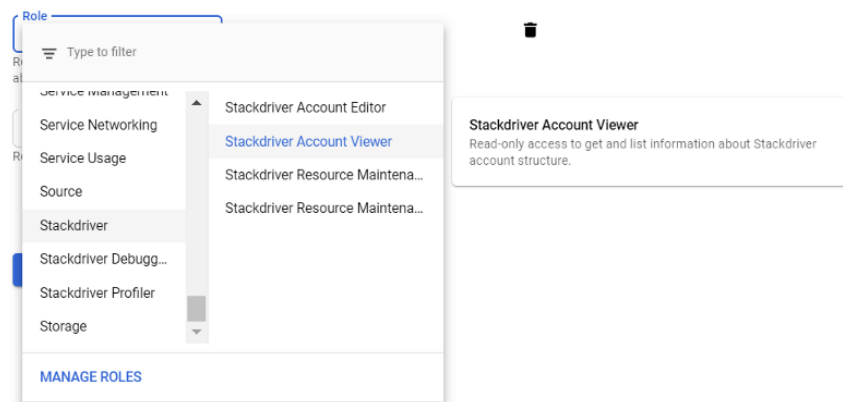
# To install the Stackdriver logging agent:
$ curl -sSO https://dl.google.com/cloudagents/install-logging-agent.sh
$ sudo bash install-logging-agent.sh
```

Eu instalo uma VM e instalei o monitoramento e o agente do driver de pilha, conforme mostrado no comando acima.

Agora vá para o console do GCP e, em seguida, para o stackdriver> monitoring. Você será apresentado com a página de boas-vindas



Agora precisamos adicionar usuários para monitoramento. Adicionando os usuários com várias funções é bastante para a frente para o driver de pilha. Não precisamos validar usuários diferentes separadamente, mas adicionar o IAM e os serviços para adicionar o novo usuário ao projeto, mas temos que selecionar as funções do Stackdriver e do Stackdriver e salvar a configuração.



Depois de adicionar o usuário, o acesso concedido permitirá que o usuário visualize / edite / exclua / monitore novos serviços / aplicativos.

Então, concluímos 1,1 da certificação do GCP.

NOTA: Os projetos mostrados no artigo são usados apenas para fins de demonstração. Todos os projetos e usuários são cancelados e não

existentes.

