

Passos para implementação do Projeto Hands-on - Parte 1

Amazon Web Services (AWS)

- Acessar a console da AWS. Na barra de pesquisas, digite IAM. Na seção Services, clique em IAM.
- Clique em Add user, insira o nome **terraform-pt-1** e clique em Next para criar o usuário do tipo programmatic.

Specify user details

User details

User name

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☐ **Enable console access - optional**
Enables a password that allows users to sign in to the AWS Management Console.

For programmatic access, you can generate access keys after you create the user. [Learn more](#)

Cancel

Next

- Após avançar, em **Set permissions**, clique no botão **Attach existing policies directly**.

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

☐ **Add user to group**
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ **Copy permissions**
Copy all group memberships, attached managed policies, and inline policies from an existing user.

☒ **Attach policies directly**
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1037)

Choose one or more policies to attach to your new user.

Filter distributions by text, property or value

< 1 2 3 4 5 6 7 ... 52 >

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AccessAnalyzerServiceRolePolicy	AWS managed	0
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	1
<input type="checkbox"/>	AdministratorAccess-Amplify	AWS managed	0
<input type="checkbox"/>	AdministratorAccess-AWSElasticBeanstalk	AWS managed	0
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	0
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS managed	0

- Digite **AmazonS3FullAccess** em **Filter distributions by text, property or value** e aperte **Enter**.
- Selecione **AmazonS3FullAccess**

Permissions policies (1/1037)

Choose one or more policies to attach to your new user.

Filter distributions by text, property or value

1 match

AmazonS3FullAccess

Clear filters

☒

Policy name

Type

Attached entities

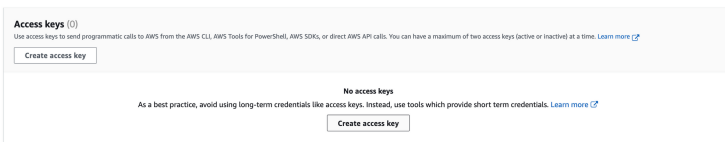
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	2
-------------------------------------	--------------------	-------------	---

- Clique em **Next**

- Revise todos os detalhes
- Clique em **Create user**

[NEW] AWS has recently changed the way to create/download the access key. Follow the new steps:

- Acesse o usuário **terraform-pt-1**
- Clique em **Security credentials**
- Navegue até a seção Access keys
- Clique em **Create access key**



- Selecione Command Line Interface (CLI) e I **understand the above recommendation and want to proceed to create an access key.**
- Clique em **Next.**
- Clique em **Create access key**
- Clique em **Download .csv file**
- Após o download finalizar, clique em Done.
- Com o download feito, renomeie o **.csv** para **accessKeys.csv**

Google Cloud Platform (GCP)

- [CLIQUE AQUI para baixar os arquivos do projeto hands-on.](#)
- Acessar a console da GCP e abrir o Cloud Shell
- Fazer o upload dos arquivos accessKeys.csv e mission1.zip para o Cloud Shell
- Após fazer o upload, executar os comandos de preparação dos arquivos:

```
mkdir mission1_pt mv mission1.zip  
mission1_pt cd mission1_pt unzip  
mission1.zip mv ~/accessKeys.csv  
mission1/pt cd mission1/pt chmod +x  
*.sh
```

- Execute os comandos abaixo para preparar o ambiente da AWS e GCP

```
./aws_set_credentials.sh accessKeys.csv  
gcloud config set project <your-  
project-id>
```

- Clique em Autorize e execute o comando abaixo para setar o projeto no Google Cloud Shell

```
./gcp_set_project.sh
```

- Execute o comando para habilitar as APIs do Kubernetes, Container Registry e Cloud SQL

```
gcloud services enable  
containerregistry.googleapis.com gcloud  
services enable  
container.googleapis.com gcloud  
services enable sqladmin.googleapis.com
```

OBS IMPORTANTE (NÃO PULE ESTE PASSO):

- **Antes de executar os comandos do terraform, abra o Google Cloud Editor e atualizar o arquivo tcb_aws_storage.tf substituindo o nome do bucket para um exclusivo (na AWS, os buckets precisam ter nomes únicos).**
 - Na linha 4 do arquivo tcb_aws_storage.tf:
 - Abra o Google Cloud Editor
 - Substituir **xxxx** pelas iniciais do seu nome mais dois números:
Exemplo: luxxy-covid-testing-system-pdf-pt-jr29
- Execute os seguintes comandos para provisionar os recursos de infraestrutura

```
cd ~/mission1_pt/mission1/pt/terraform/  
terraform init  
terraform plan  
terraform apply
```



Após acessar o serviço do GKE para criar o cluster, clicar no botão Compare para "Comparar os modos de cluster para entender mais sobre as suas diferenças".

Create cluster

Select the cluster mode that you want to use.



Autopilot: Google manages your cluster (Recommended)

A pay-per-Pod Kubernetes cluster where GKE manages your nodes with minimal configuration required. [Learn more](#)



Standard: You manage your cluster

A pay-per-node Kubernetes cluster where you configure and manage your nodes. [Learn more](#)



Compare cluster modes to learn more about their differences.

Create cluster

Select the cluster mode that you'd like to use. [Learn more](#)

Autopilot mode

Optimized Kubernetes cluster with a hands-off experience

CONFIGURE

TRY THE DEMO

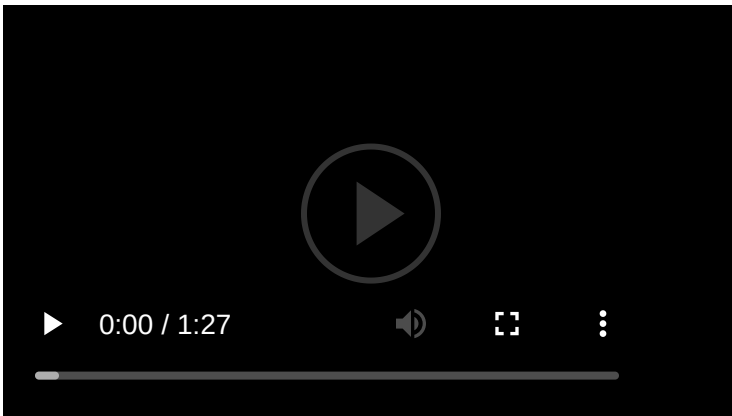
Scaling	Automatic based on workload	Yes
Nodes	Google manages and configures your nodes	Yes no
Configuration	Streamlined configuration ready to use	Yes
Workloads supported	Most workloads except these limitations	All
Billing method	Pay per pod	Pay
SLA	Kubernetes API and node availability	Kubernetes

[View all](#)



Faça o Download do Visual Studio Code utilizado pelo Jean durante a Imersão [AQUI](#)

[New] Configuração de Rede SQL



- Após a conclusão do provisionamento da instância do CloudSQL, acesse o serviço do Cloud SQL.
- Clique na sua instância do Cloud SQL.
- Na lateral direita, em Primary Instance, clique em “**Connections**”.

- Em **Instance IP assignment**, habilite o Private IP.
 - Em **Associated Network**, selecione "Default".
 - Clique em **Set up connection**
 - Enable **Service Networking API** (se solicitar)
 - Selecione **Use an automatically allocated IP range in your network**.
 - Clique em **Continue**.
 - Clique em **Create connection** e aguarde alguns minutos.
- Após finalizar, em **"Connections", Authorized Networks**, clique em **"Adicionar Rede (Add Network)"**.
 - Em **New Network**, insira as seguintes informações:
 - **Nome:** Public Access (Apenas para testes)
 - **Network:** 0.0.0.0/0
 - Clique em **Done**.