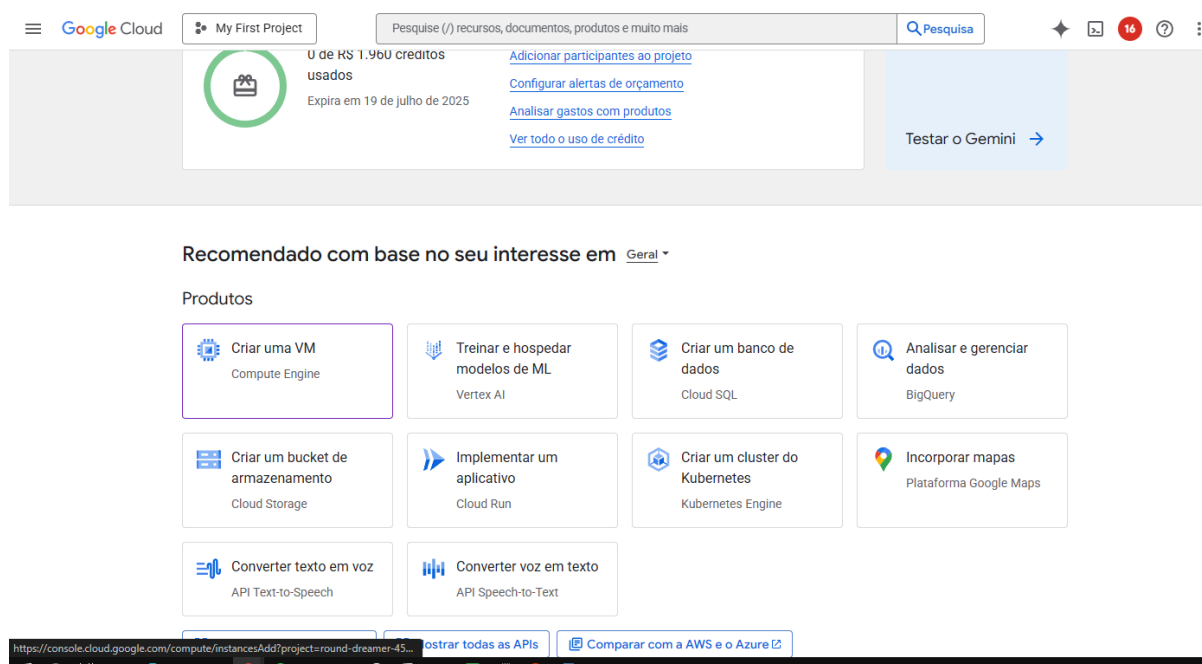


Documentação do Processo de Instalação do GLPI no Google Cloud com Docker e Portainer (Apenas para Debian/Ubuntu)

1. Criação da Conta no Google Cloud Platform (GCP)

Acesse o Google Cloud: Abra seu navegador e vá para <https://cloud.google.com/>. Crie uma conta ou faça login: Se você já possui uma conta Google, faça login. Caso contrário, siga as instruções para criar uma nova conta. Você provavelmente precisará fornecer informações de pagamento para configurar uma conta de faturamento, mesmo para usar os recursos da camada gratuita (se aplicável). Crie um projeto: Após fazer login, você será solicitado a criar um projeto. Um projeto organiza todos os seus recursos do Google Cloud. Dê um nome descritivo ao seu projeto (por exemplo, glpi-projeto).



2. Criação de uma Instância de Máquina Virtual (VPS) no Compute Engine

Navegue até o Compute Engine: No menu de navegação (canto superior esquerdo), vá em "Compute Engine" e selecione "Instâncias de VM". Crie uma nova instância: Clique em "CRIAR INSTÂNCIA". Configure a instância: Nome: Dê um nome para sua instância (por exemplo, glpi-vps). Região e Zona: Escolha uma região geograficamente próxima de você para menor latência. Selecione uma zona dentro dessa região. Série da máquina: Escolha um tipo de máquina adequado para sua carga de trabalho. Para testes, uma máquina da série "e2-medium" ou similar pode ser suficiente. Imagem do disco de inicialização: Clique em "Alterar" e selecione um sistema operacional. Recomenda-se uma distribuição Linux popular como Ubuntu ou Debian. Escolha a versão mais recente e clique em "Selecionar". Disco de inicialização: Ajuste o tamanho do disco conforme necessário. O tipo de disco padrão (geralmente disco persistente padrão) é adequado para a maioria dos casos de teste. Rede: Aceite a rede VPC padrão ou configure uma rede personalizada, se necessário. Firewall: Marque as opções "Permitir tráfego HTTP" e "Permitir tráfego HTTPS". Isso já abrirá as portas 80 e 443 no firewall padrão da instância. Você precisará adicionar

regras para outras portas posteriormente (como a do Portainer). Outras configurações (opcional): Você pode configurar chaves SSH para acesso mais seguro, definir metadados, etc. Crie a instância: Clique em "Criar". O Google Cloud provisionará sua VPS e fornecerá um endereço IP externo.

Configuração da máquina

Nome *
instance-20250420-044728

Região *
us-central1 (Iowa)

Zona *
Tudo

SO e armazenamento
Debian GNU/Linux 12 (bookworm)

Proteção de dados
Programações de snapshot

Rede
1 interface de rede

Observabilidade
Instalar o Agente de operações

Segurança

Avançado

Tipos de máquinas para cargas de trabalho comuns, otimizadas para custo e flexibilidade

Series	Descrição	vCPUs	Memory	Plata
C4	Desempenho consistente e constante	2 - 192	4 a 1.488 GB	Intel E
C4A	Alto desempenho consistente baseado em arm	1 - 72	2 a 576 GB	Googl
C4D	Alto desempenho consistente	2 - 384	3 a 3.024 GB	AMD
N4	Flexível e econômico	2 - 80	4 a 640 GB	Intel E
C3	Desempenho consistente constante	4 - 192	8 a 1.536 GB	Intel E
C3D	Desempenho consistente e constante	4 - 360	8 a 2.880 GB	AMD
E2	Computação diária de baixo custo	0.25 - 32	1 a 128 GB	Intel E
N2	Equilíbrio entre preço e desempenho	2 - 128	2 a 864 GB	Intel C
N2D	Equilíbrio entre preço e desempenho	2 - 224	2 a 896 GB	AMD

Estimativa mensal

US\$ 25,46
Cerca de US\$ 0,03 por hora

Pague pelo que usar: faturamento por segundo e sem custos iniciais

Item	Estimativa mensal
2 vCPU + 4 GB memory	US\$ 24,46
Disco permanente balanceado com 10 GB	US\$ 1,00
Logging	O custo varia
Monitoring	O custo varia
Programação de snapshots	O custo varia
Total	US\$ 25,46

Preços do Compute Engine

Preços do produto Operações do Cloud

Menos

3. Conexão SSH à VPS

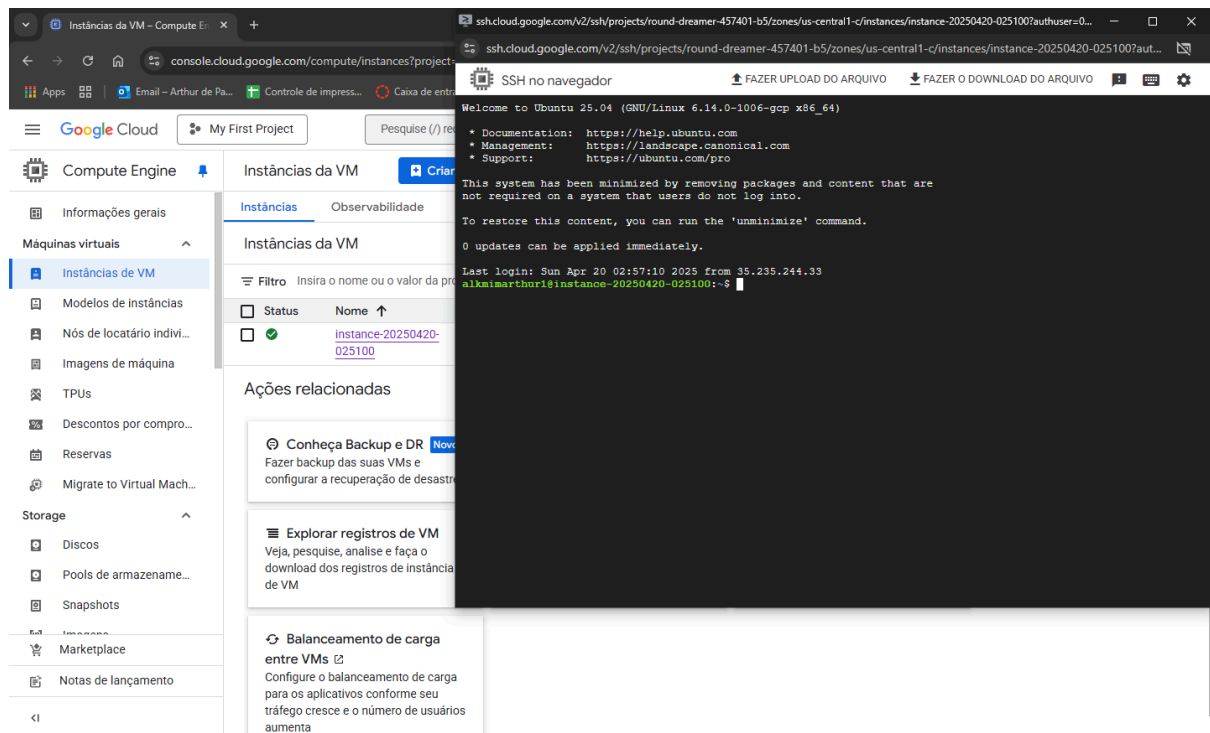
Localize o endereço IP externo: Na página "Instâncias de VM", copie o endereço IP externo da sua VPS. Abra um terminal (Linux/macOS) ou PuTTY (Windows). Use o comando SSH:

```
ssh <seu_nome_de_usuario>@<seu_ip_externo>
```

Substitua <seu_nome_de_usuario> pelo seu nome de usuário na VPS (geralmente o nome de usuário que você usou ao criar a conta ou o nome padrão do sistema operacional, como ubuntu ou debian) e <seu_ip_externo> pelo endereço IP da sua VPS. Se você estiver usando chaves SSH, o comando pode ser mais simples:

```
ssh -i <caminho_para_sua_chave_privada> <seu_nome_de_usuario>@<seu_ip_externo>
```

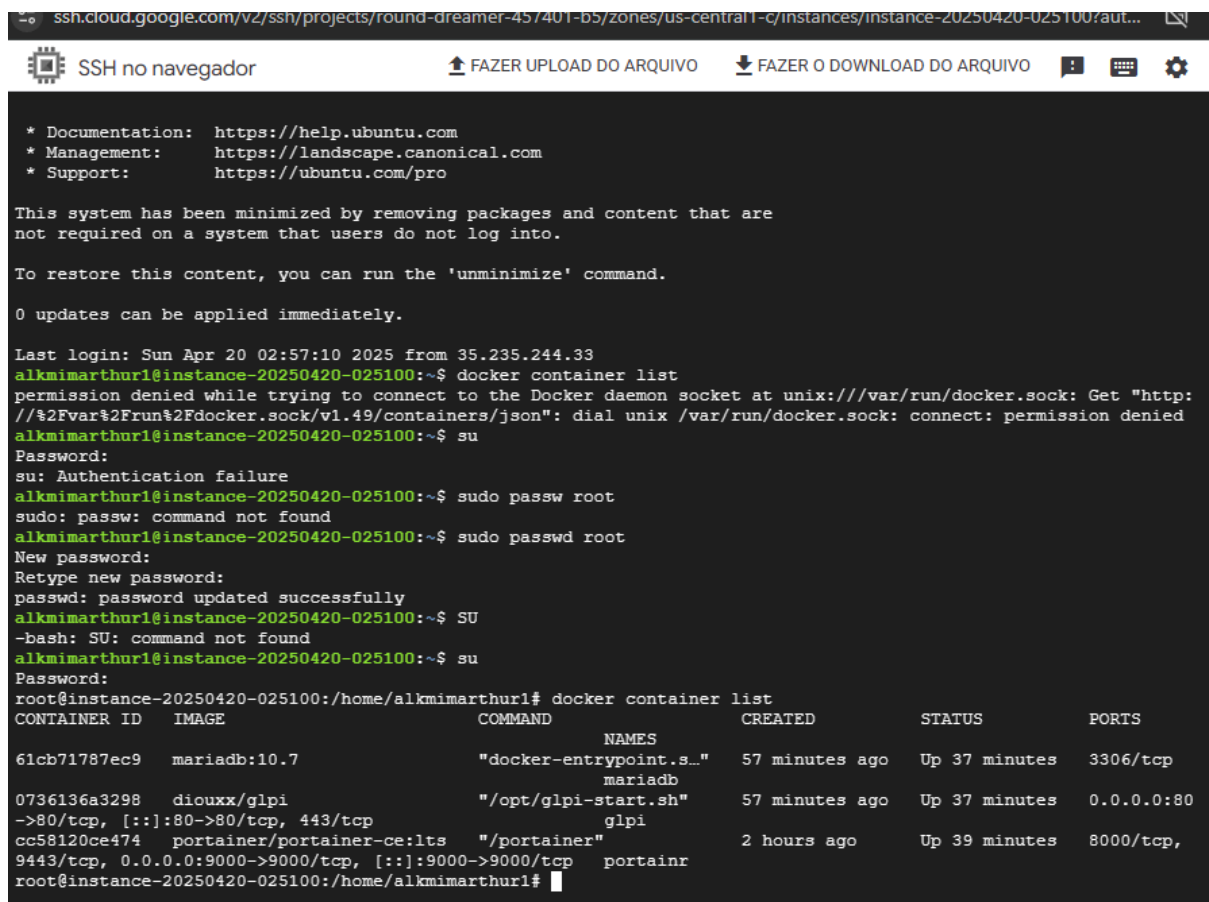
Faça login: Se for a primeira vez que você se conecta, você será solicitado a verificar a chave do host. Digite **yes**. Se você estiver usando senha, insira a senha da sua conta na VPS.



4. Instalação do Docker na VPS

Atualize os pacotes: `sudo apt update && sudo apt upgrade -y` Instale as dependências do Docker: `sudo apt install apt-transport-https ca-certificates curl software-properties-common -y` Adicione a chave GPG do Docker: `curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /etc/apt/keyrings/docker.gpg` Adicione o repositório Docker: `echo "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg] https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null` Instale o Docker Engine: `sudo apt update && sudo apt install docker-ce docker-ce-cli containerd.io docker-compose-plugin -y` Verifique a instalação

do Docker: `sudo docker run hello-world`



The screenshot shows a terminal window with the following content:

```
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

0 updates can be applied immediately.

Last login: Sun Apr 20 02:57:10 2025 from 35.235.244.33
alkmimarthur1@instance-20250420-025100:~$ docker container list
permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get "http://%2Fvar%2Frun%2Fdocker.sock/v1.49/containers/json": dial unix /var/run/docker.sock: connect: permission denied
alkmimarthur1@instance-20250420-025100:~$ su
Password:
su: Authentication failure
alkmimarthur1@instance-20250420-025100:~$ sudo passw root
sudo: passw: command not found
alkmimarthur1@instance-20250420-025100:~$ sudo passwd root
New password:
Retype new password:
passwd: password updated successfully
alkmimarthur1@instance-20250420-025100:~$ SU
-bash: SU: command not found
alkmimarthur1@instance-20250420-025100:~$ su
Password:
root@instance-20250420-025100:/home/alkmimarthur1# docker container list
```

CONTAINER ID	IMAGE	COMMAND	NAMES	CREATED	STATUS	PORTS
61cb71787ec9	mariadb:10.7	"docker-entrypoint.s..."	mariadb	57 minutes ago	Up 37 minutes	3306/tcp
0736136a3298	dioux/glpi	"/opt/glpi-start.sh"	glpi	57 minutes ago	Up 37 minutes	0.0.0.0:80->80/tcp, [::]:80->80/tcp, 443/tcp
cc58120ce474	portainer/portainer-ce:latest	"/portainer"	portainer	2 hours ago	Up 39 minutes	8000/tcp, 9443/tcp, 0.0.0.0:9000->9000/tcp, [::]:9000->9000/tcp

```
root@instance-20250420-025100:/home/alkmimarthur1#
```

5. Instalação do Portainer no Docker

Crie um volume para os dados do Portainer: `sudo docker volume create portainer_data` Implante o Portainer CE (Community Edition): `sudo docker run -d -p 8000:8000 -p 9443:9443 --name portainer --restart always -v /var/run/docker.sock:/var/run/docker.sock -v portainer_data:/data portainer/portainer-ce:latest` Acesse o Portainer: Abra seu navegador e vá para `https://<seu_ip_externo>:9443`. A primeira vez, você precisará criar um usuário administrador e definir uma senha.

6. Configuração do Firewall no Google Cloud para o Portainer

Navegue até o Firewall: No console do Google Cloud, vá em "Rede VPC" e selecione "Firewall". Adicione regras de firewall: Clique em "ADICIONAR REGRA DE FIREWALL". Nome: allow-portainer-https Rede: Sua rede VPC. Direção do tráfego: Entrada. Ação em caso de correspondência: Permitir. Destinos: Todas as instâncias na rede. Filtro de origem: Intervalos de IP: 0.0.0.0/0. Protocolos e portas: TCP: 9443. Clique em "Criar". Repita o processo para a porta HTTP do Portainer (se necessário): Nome: allow-portainer-http Protocolos e portas: TCP: 8000.

Segurança da rede

Proxy seguro da Web

Cloud Armor

Painel de DDoS

Políticas do Cloud Armor

Proteção adaptativa

Nível do serviço Cloud ...

Cloud IDS

Painel do IDS

Endpoints do IDS

Ameaças do IDS

Cloud NGFW

Painel

Políticas de firewall

Ameaças

Endpoints de firewall

Componentes comuns

Grupos de endereços

Políticas de firewall

Criar política de firewall

Criar regra de firewall

Saiba ma

Porta SMTP 25 não permitida neste projeto. Saiba mais

Atualizar

Configurar registros

Excluir

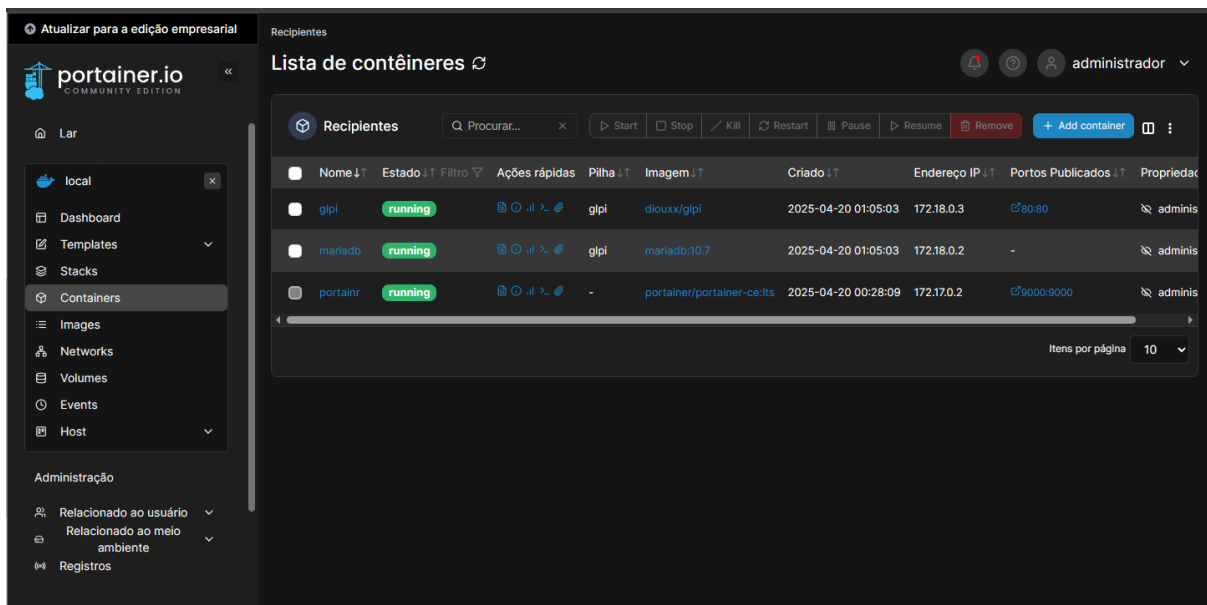
Filtro

Insira o nome ou o valor da propriedade

	Nome	Tipo	Destinos	Filtros	Protocolos / portas	Ação	Prioridade	Rede	Registros	
<input type="checkbox"/>	allow-portainer-http	Entrada	Aplicar a	Intervalos	tcp:9000	Permitir	1000	default	Ativado	
<input type="checkbox"/>	default-allow-http	Entrada	http-server	Intervalos	tcp:80	Permitir	1000	default	Desativado	
<input type="checkbox"/>	default-allow-https	Entrada	https-server	Intervalos	tcp:443	Permitir	1000	default	Desativado	
<input type="checkbox"/>	default-allow-icmp	Entrada	Aplicar a	Intervalos	icmp	Permitir	65534	default	Desativado	
<input type="checkbox"/>	default-allow-internal	Entrada	Aplicar a	Intervalos	tcp:0-65535 udp:0-65535 icmp	Permitir	65534	default	Desativado	
<input type="checkbox"/>	default-allow-rdp	Entrada	Aplicar a	Intervalos	tcp:3389	Permitir	65534	default	Desativado	
<input type="checkbox"/>	default-allow-ssh	Entrada	Aplicar a	Intervalos	tcp:22	Permitir	65534	default	Desativado	

7. Criação dos Containers GLPI e MariaDB no Portainer

Acesse o Portainer: https://<seu_ip_externo>:9443. Selecione o ambiente Docker local. Crie o container MariaDB: Vá em "Containers" e clique em "+ Add container". Name: mariadb Image: mariadb:10.7 Environment variables:
MARIADB_ROOT_PASSWORD=<sua_senha_root> MARIADB_DATABASE=glpidb
MARIADB_USER=rootzada MARIADB_PASSWORD=<sua_senha_glpi> Volumes: Crie um volume chamado db_data e mapeie /var/lib/mysql no container para este volume. Network: Use a rede bridge padrão ou crie uma rede personalizada. Restart policy: Unless stopped. Clique em "Deploy the container". Crie o container GLPI: Vá em "Containers" e clique em "+ Add container". Name: glpi Image: glpi/glpi:latest Ports mapping: Mapeie uma porta do host (por exemplo, 8080) para a porta 80 do container. Volumes: Crie um volume chamado glpi_data e mapeie /var/www/html no container para este volume. Você também pode mapear um volume para /var/www/html/config. Environment variables: DB_HOST=mariadb (o nome do serviço do container MariaDB) DB_NAME=glpidb DB_USER=rootzada DB_PASSWORD=<sua_senha_glpi> Network: Use a mesma rede do container MariaDB. Restart policy: Unless stopped. Clique em "Deploy the container".



8. Configuração do Firewall para Acesso ao GLPI

Navegue até o Firewall no Google Cloud. Adicione uma regra de firewall: Nome: allow-glpi-http Rede: Sua rede VPC. Direção do tráfego: Entrada. Ação em caso de correspondência: Permitir. Destinos: Todas as instâncias na rede. Filtro de origem: Intervalos de IP: 0.0.0.0/0. Protocolos e portas: TCP: 8080 (ou a porta que você mapeou para o GLPI). Clique em "Criar".

9. Instalação e Configuração Inicial do GLPI via Navegador

Acesse o GLPI: Abra seu navegador e vá para http://<seu_ip_externo>:8080 (substitua pela porta que você mapeou). Siga o assistente de instalação do GLPI: Selecione o idioma. Aceite os termos da licença. O GLPI verificará os pré-requisitos. Na etapa de "Conexão com o banco de dados", insira as seguintes informações (baseado na configuração dos containers): Endereço do servidor SQL (MariaDB ou MySQL): [mariadb](#) Usuário SQL: [rootzada](#) Senha SQL: [<sua_senha_glpi>](#) Clique em "Continuar". O GLPI criará o banco de dados e as tabelas. Siga as próximas etapas para configurar a conta de administrador do GLPI e outras configurações iniciais.



10.Conclusão

Nesse momento de teste do projeto identificamos que há possibilidade de oferecer essas soluções em nuvem de maneira barata, escalável e de fácil administração no google Cloud. Iremos dar prosseguimento no projeto e desenvolver o controle de segurança e personalização do sistema para realidade do cliente.

DIAGRAMA BÁSICO DE IMPLEMENTAÇÃO

