

# Preparando-se para implantar o Gerenciador de operações no GCP manualmente

Última atualização da página: 15 de fevereiro de 2019

Este tópico descreve as etapas de preparação necessárias para instalar o Gerenciador de operações do Pivotal Cloud Foundry (PCF) no Google Cloud Platform (GCP).

## Pré-requisitos

Before you prepare your Ops Manager installation, do the following depending on the runtime you intend to deploy:

- If you are deploying Pivotal Application Service (PAS), see [PCF on GCP Requirements](#).
- If you are deploying Pivotal Container Service (PKS), see [GCP Prerequisites and Resource Requirements](#).

## Configuration and Components

This section outlines high-level infrastructure options for PCF on GCP. A PCF deployment includes Ops Manager and your chosen runtime. For example, both Ops Manager with PAS and Ops Manager with PKS are PCF deployments. For more information, review the deployment options and recommendations in [Reference Architecture for Pivotal Cloud Foundry on GCP](#).

Você pode implantar o PCF usando uma das duas principais configurações em uma nuvem privada virtual (VPC) do GCP:

- Uma configuração de *projeto único* que fornece ao Ops Manager acesso total aos recursos do VPC
- Uma configuração *compartilhada de VPC* na qual o Gerenciador de OPS compartilha recursos de VPC

Consulte [VPCs de compartilhamento único versus projeto único](#) no [tópico Arquitetura de referência do Fundido de nuvem principal no GCP](#) para obter uma discussão e recomendações completas.

Ao implantar o PCF no GCP, a Pivotal recomenda usar os seguintes componentes do GCP:

- [Google Cloud SQL](#) para serviços de banco de dados externos
- [Instâncias de Gateway NAT](#) para limitar o número de VMs com endereços IP públicos
- [Google Cloud Storage](#) para [armazenamento](#) externo de arquivos

## Etapa 1: configurar contas de serviço do IAM

O Gerenciador de operações usa contas de serviço do IAM para acessar recursos do GCP.

**Para uma instalação de projeto único :** Conclua as etapas a seguir para criar uma conta de serviço para o Gerenciador de Operações.

**Para uma instalação de VPC compartilhada :** Conclua as etapas a seguir duas vezes para criar uma conta de host e conta de serviço para o Gerenciador de operações.

1. No console do GCP, selecione **IAM e administrador e** , em seguida, **contas de serviço** .

2. Clique em **Criar conta de serviço** :

- **Nome da conta de serviço** : insira um nome. Por exemplo, `bosh` .
- **Função** : selecione as seguintes funções:
  - **Contas de serviço**> **Usuário da conta de serviço**
  - **Contas de serviço**> **Criador de token da conta de serviço**
  - **Compute Engine**> **Administrador de instâncias de cálculo (v1)**
  - **Compute Engine**> **Compute Network Admin**
  - **Compute Engine**> **Compute Storage Admin**

## ■ Armazenamento&gt; Administrador de Armazenamento

**Nota:** Você deve rolar para baixo nas janelas pop-up para selecionar todas as funções necessárias.

A função de **usuário da conta de serviço** só é necessária se você planeja usar a **conta de serviço da VM do Gerenciador de operações** para implantar o Gerenciador de operações. Para obter mais informações sobre a **conta de serviço da VM do Gerenciador de operações**, consulte a [Etapa 2: configuração do Google Cloud Platform](#) em *Configurar o BOSH Director no GCP*.

- **ID da conta de serviço** : o campo gera automaticamente um ID exclusivo com base no nome de usuário.
- **Fornecer uma nova chave privada** : Selecione esta caixa de seleção e JSON como o **tipo de chave**.

**Create service account**

**Service account name** ?

bosh

**Service account ID**

bosh-48 @cf-sf-onboarding-env-3.iam.gcp

☒ **Furnish a new private key**  
Downloads a file that contains the private key. Store the file in a secure location. The key can't be recovered if lost.

**Key type**

☒ **JSON**  
Recommended

☐ **P12**  
For backward compatibility with code using the P12 key format.

☐ **Enable G Suite Domain-wide Delegation**  
Allows this service account to be authorized to access all domain resources without manual authorization on their part. [Learn more](#)

**Role** ?

Compute Instance Admin (v1)

**Selected**

- ✓ Compute Instance Admin (v1)
- ✓ Compute Network Admin
- ✓ Compute Storage Admin
- ✓ Service Account Token Creator
- ✓ Service Account User
- ✓ Storage Admin

Project

App Engine

BigQuery

Billing

Cloud IAP

Cloud KMS

Cloud SQL

Cloud Security Scanner

3. Clique em **Criar**. Seu navegador faz o download automático de um arquivo JSON com uma chave privada para essa conta. Salve este arquivo em um local seguro.

## Etapa 2: ative as APIs do Google Cloud

O Ops Manager gerencia os recursos do GCP usando as APIs do Google Compute Engine e do Cloud Resource Manager. Para ativar essas APIs, faça o seguinte:

1. Faça login no Google Developers Console em <https://console.developers.google.com>.
2. No console, navegue até os projetos do GCP em que você deseja instalar o Gerenciador de Operações.
  - Para uma instalação de projeto único, conclua as etapas a seguir para o projeto Ops Manager.

- Para uma instalação de VPC compartilhada, conclua as etapas a seguir para projetos de host e de serviço, para permitir que eles acessem a Google Cloud API.

3. Selecione **Gerenciador de API > Biblioteca**.

4. Nas **APIs do Google Cloud**, selecione a **Compute Engine API**.

5. Na página da **API do Google Compute Engine**, clique em **Ativar**.

6. No campo de pesquisa, insira `Google Cloud Resource Manager API`.

7. Na página da **API do Google Cloud Resource Manager**, clique em **Ativar**.

8. Para verificar se as APIs foram ativadas, execute as seguintes etapas:

- a. Faça login no GCP usando a conta de serviço do IAM que você criou em [Configurar contas de serviço do IAM](#):

```
$ gcloud auth activar serviço-conta -chave-chave JSON_KEY_FILENAME
```

- b. Listar seus projetos:

```
Lista de projetos do $ gcloud
PROJECT_ID NAME PROJECT_NUMBER
my-host-project-id meu-host-nome-de-projeto #####
my-service-project-id meu-serviço-nome-de-projeto #####
```

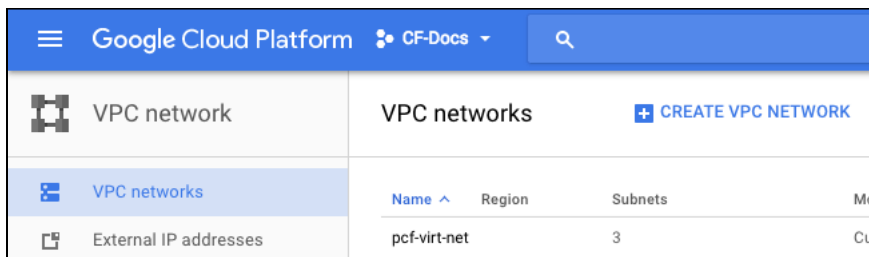
Este comando lista os projetos em que você ativou as APIs do Google Cloud.

## Etapa 3: criar uma rede GCP com sub-redes

1. Faça o login no [console](#) do [GCP](#).

2. Navegue até o projeto do GCP no qual você deseja instalar o Gerenciador de operações. Para uma instalação compartilhada do VPC, navegue até o projeto do host.

3. Selecione a **rede VPC** e, em seguida, **CREATE VPC NETWORK**.



4. No campo **Nome**, insira um nome de sua escolha para a rede VPC. Esse nome ajuda a identificar recursos para essa implantação no console do GCP. Os nomes de rede devem estar em minúsculas. Por exemplo, `pcf-virt-net`.

[←](#)
**Create a VPC network**

**Name** ⓘ
  ⓘ

- a. Em **Sub-redes**, preencha o formulário da seguinte maneira para criar uma sub-rede de infra-estrutura para as instâncias do Ops Manager e do NAT:

<b>Nome</b>	<input type="text" value="pcf-infrastructure-subnet-GCP-REGION"/> Example: <input type="text" value="pcf-infrastructure-subnet-us-west1"/>
<b>Region</b>	A region that supports three availability zones. For help selecting the correct region for your deployment, see the <a href="#">Google documentation about regions and zones</a> .

IP address range	A CIDR ending in <input type="text" value="/26"/> Example: <input type="text" value="192.168.101.0/26"/>
------------------	-------------------------------------------------------------------------------------------------------------

See the following image for an example:

**Note:** For deployments that do not use external IP addresses, enable **Private Google access** to allow your runtime to make API calls to Google services.

b. Click **Add subnet** to add a second subnet for the BOSH Director and components specific to your runtime. Complete the form as follows:

Name	<input type="text" value="pcf-RUNTIME-subnet-GCP-REGION"/> Example: <input type="text" value="pcf-pas-subnet-us-west1"/>
Region	The same region you selected for the infrastructure subnet
IP address range	A CIDR ending in <input type="text" value="/22"/> Example: <input type="text" value="192.168.16.0/22"/>

c. Click **Add subnet** to add a third **Subnet** with the following details:

<b>Name</b>	pcf-services-subnet-GCP-REGION Example: pcf-services-subnet-us-west1
<b>Region</b>	The same region you selected for the previous subnets
<b>IP address range</b>	A CIDR in /22 Example: 192.168.20.0/22

See the following image for an example:

VPC networks <span>CREATE VPC NETWORK</span> <span>REFRESH</span>							
Name ^	Region	Subnets	Mode	IP addresses ranges	Gateways	Firewall Rules	Global dynamic routing
pcf-virt-network		3	Custom			0	Off
	us-west1	pcf-subnet-ert-us-west1		192.168.16.0/22	192.168.16.1		
	us-west1	pcf-subnet-infrastructure-us-west1		192.168.101.0/26	192.168.101.1		
	us-west1	pcf-subnet-services-us-west1		192.168.20.0/22	192.168.20.1		

5. Under **Dynamic routing mode**, leave **Regional** selected.

6. Click **Create**.

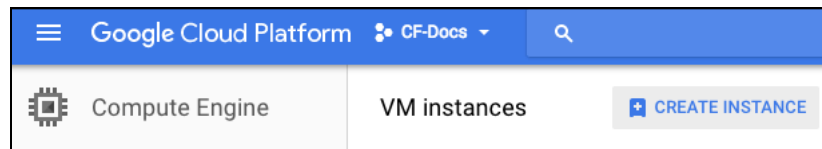
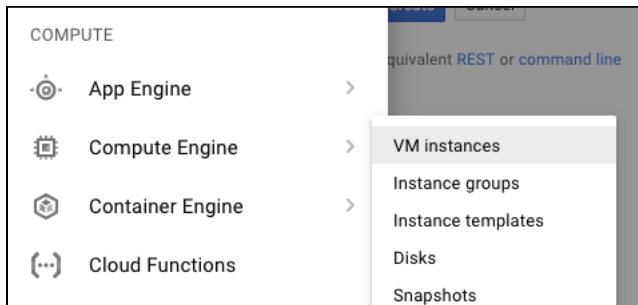
## Step 4: Create NAT Instances

Use NAT instances when you want to expose only a minimal number of public IP addresses.

Creating NAT instances permits internet access from cluster VMs. You might, for example, need this internet access for pulling Docker images or enabling internet access for your workloads.

For more information, see [Reference Architecture for Pivotal Cloud Foundry on GCP](#) and [GCP documentation](#).

1. In the GCP console, with your single project or shared-VPC host project selected, navigate to **Compute Engine > VM instances**.



2. Click **CREATE INSTANCE**.

3. Complete the following fields:

- Name:** Enter `pcf-nat-gateway-pri`.  
This is the first, or primary, of three NAT instances you need. If you use a single AZ, you need only one NAT instance.
- Zone:** Select the first zone from your region.  
Example: For region `us-west1`, select zone `us-west1-a`.
- Machine type:** Select `n1-standard-4`.

- **Boot disk:** Click **Change** and select `Ubuntu 14.04 LTS`.

4. Expand the additional configuration fields by clicking **Management, disks, networking, SSH keys**.

- a. In the **Startup script** field under **Automation**, enter the following text:

```
#!/bin/bash
sudo sysctl -w net.ipv4.ip_forward=1
sudo sh -c 'echo net.ipv4.ip_forward=1 >> /etc/sysctl.conf'
sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

5. Click **Networking** to open additional network configuration fields:

- In the **Network tags** field, add the following: `nat-traverse` and `pcf-nat-instance`.
- Click on the **Networking** tab and the pencil icon to edit the **Network interface**.
- For **Network**, select `pcf-virt-net`. You created this network in [Step 1: Create a GCP Network with Subnets](#).
- For **Subnetwork**, select `pcf-infrastructure-subnet-GCP-REGION`.
- For **Primary internal IP**, select `Ephemeral (Custom)`. Enter an IP address, for example, `192.168.101.2`, in the **Custom ephemeral IP address** field. The IP address must meet the following requirements:
  - The IP address must exist in the CIDR range you set for the `pcf-infrastructure-subnet-GCP-REGION` subnet.
  - The IP address must exist in a reserved IP range set later in BOSH Director. The reserved range is typically the first `.1` through `.9` addresses in the CIDR range you set for the `pcf-infrastructure-subnet-GCP-REGION` subnet.
  - The IP address cannot be the same as the Gateway IP address set later in Ops Manager. The Gateway IP address is typically the first `.1` address in the CIDR range you set for the `pcf-infrastructure-subnet-GCP-REGION` subnet.

- f. Para **IP externo**, selecione `Ephemeral`.

**Nota :** Se você selecionar um endereço IP externo estático para a instância NAT, poderá usar o IP estático para proteger ainda mais o acesso às suas instâncias do CloudSQL.

g. Definir o **encaminhamento de IP** para `On`.

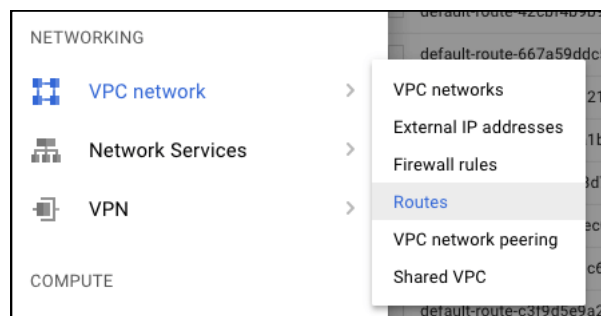
h. Clique em **Concluído**.

6. Clique em **Criar** para concluir a criação da instância do NAT.

7. Repita as etapas 2 a 6 para criar duas instâncias NAT adicionais com os nomes e as zonas especificados na tabela abaixo. O resto da configuração permanece o mesmo.

Instância 2	Nome	<code>pcf-nat-gateway-sec</code>
	Zona	Selecione a segunda zona da sua região. Exemplo: para região <code>us-west1</code> , selecione zona <code>us-west1-b</code> .
	IP interno	Selecione <code>Custom</code> e insira um endereço IP no campo <b>Endereço IP interno</b> . Exemplo: <code>192.168.101.3</code> .  Conforme descrito acima, esse endereço deve estar no intervalo CIDR definido para a <code>pcf-infrastructure-subnet-GCP-REGION</code> sub-rede, deve existir em um intervalo IP reservado definido posteriormente no BOSH Director e não pode ser o mesmo que o endereço IP do Gateway definido posteriormente no Gerenciador de Ops.
Instância 3	Nome	<code>pcf-nat-gateway-ter</code>
	Zona	Selecione a terceira zona da sua região. Exemplo: para região <code>us-west1</code> , selecione zona <code>us-west1-c</code> .
	IP interno	Selecione <code>Custom</code> e insira um endereço IP no campo <b>Endereço IP interno</b> . Exemplo: <code>192.168.101.4</code> .  Conforme descrito acima, esse endereço deve estar no intervalo CIDR definido para a <code>pcf-infrastructure-subnet-GCP-REGION</code> sub-rede, deve existir em um intervalo IP reservado definido posteriormente no BOSH Director e não pode ser o mesmo que o endereço IP do Gateway definido posteriormente no Gerenciador de Ops.

## Criar rotas para instâncias de NAT



1. Navegue para **redes VPC > rotas**.

2. Clique em **CRIAR ROTA**.

3. Preencha o formulário da seguinte forma:

- **Nome:** `pcf-nat-pri`
- **Rede:** `pcf-virt-net`
- **Faixa de IP de destino:** `0.0.0.0/0`
- **Prioridade:** `800`
- **Tags de instâncias:** `pcf`
- **Próximo salto:** `Specify an instance`
- **Instância do próximo salto:** `pcf-nat-gateway-pri`

4. Clique em **Criar** para concluir a criação da rota.

5. Repita as etapas 2 a 4 para criar duas rotas adicionais com os nomes e instâncias do próximo salto especificadas na tabela abaixo. O resto da configuração permanece o mesmo.

<b>Rota 2</b>	Nome : <input type="text" value="pcf-nat-sec"/> instância do próximo salto : <input type="text" value="pcf-nat-gateway-sec"/>
<b>Rota 3</b>	Nome : <input type="text" value="pcf-nat-ter"/> instância do próximo salto : <input type="text" value="pcf-nat-gateway-ter"/>

## Etapa 5: criar regras de firewall para a rede

O GCP permite atribuir tags a instâncias de VMs e criar regras de firewall que se aplicam a VMs com base em suas tags. Para mais informações sobre tags, consulte [Recursos de rotulagem](#) na documentação do Google Cloud. Esta etapa atribui tags e regras de firewall aos componentes e VMs do Gerenciador de Operações que lidam com o tráfego de entrada.

1. Com o projeto de projeto de um único projeto ou VPC compartilhado selecionado, navegue até o painel de **rede Rede > VPC** e selecione **Regras de firewall**.

2. Aplique as regras de firewall na tabela a seguir:

Regras de firewall	
<b>Regra 1</b>	<p>Esta regra permite o SSH de redes públicas.</p> <p>Nome : <input type="text" value="pcf-allow-ssh"/>  Rede : <input type="text" value="pcf-virt-net"/>  protocolos e portas permitidos : <input type="text" value="tcp:22"/>  filtro de origem : intervalos  IP Intervalos IP de origem : <input type="text" value="0.0.0.0/0"/>  tags de destino : <input type="text" value="allow-ssh"/></p>
<b>Regra 2</b>	<p>Esta regra permite HTTP de redes públicas.</p> <p>Nome : <input type="text" value="pcf-allow-http"/>  de rede : <input type="text" value="pcf-virt-net"/>  protocolos e portas permitidas : <input type="text" value="tcp:80"/>  filter Fonte : IP varia  Fonte intervalos de IP : <input type="text" value="0.0.0.0/0"/>  etiquetas alvo : <input type="text" value="allow-http"/> , <input type="text" value="router"/></p>
<b>Regra 3</b>	<p>Essa regra permite HTTPS de redes públicas.</p> <p>Nome : <input type="text" value="pcf-allow-https"/>  de rede : <input type="text" value="pcf-virt-net"/>  protocolos e portas permitidas : <input type="text" value="tcp:443"/>  filter Fonte : IP varia  Fonte intervalos de IP : <input type="text" value="0.0.0.0/0"/>  etiquetas alvo : <input type="text" value="allow-https"/> , <input type="text" value="router"/></p>
<b>Regra 4</b>	<p>Esta regra permite verificações de saúde de Gorouter.</p> <p>Nome : <input type="text" value="pcf-allow-http-8080"/>  Rede : <input type="text" value="pcf-virt-net"/>  protocolos e portas permitidos : <input type="text" value="tcp:8080"/>  filtro de origem : intervalos de  IPs Intervalos de IP de origem : <input type="text" value="0.0.0.0/0"/>  tags de destino : <input type="text" value="router"/></p>
<b>Regra 5</b>	<p>Essa regra permite a comunicação entre trabalhos implantados no BOSH.</p>



	<p>Nome : <code>pcf-allow-pas-all</code></p> <p>de rede : <code>pcf-virt-net</code></p> <p>admitidos protocolos e portas : <code>tcp;udp;icmp</code></p> <p>Fonte filtro : Source Tag</p> <p>Tag alvo : <code>pcf</code> , <code>pcf-opsman</code> , <code>nat-traverse</code></p> <p>etiquetas Fonte : <code>pcf</code> , <code>pcf-opsman</code> , <code>nat-traverse</code></p>
Regra 6 (Opcional)	<p>Esta regra permite acesso ao roteador TCP.</p> <p>Nome : <code>pcf-allow-cf-tcp</code></p> <p>Rede : <code>pcf-virt-net</code></p> <p>Filtro de origem : intervalos de</p> <p>IPs Intervalos de IP de origem : <code>0.0.0.0/0</code></p> <p>protocolos e portas permitidos : <code>tcp:1024-65535</code></p> <p>Tags de destino : <code>pcf-cf-tcp</code></p>
Regra 7 (Opcional)	<p>Esta regra permite acesso ao proxy SSH.</p> <p>Nome : <code>pcf-allow-ssh-proxy</code></p> <p>de rede : <code>pcf-virt-net</code></p> <p>filter Fonte : intervalos de IP</p> <p>Source IP varia : <code>0.0.0.0/0</code></p> <p>protocolos e portas permitidas : <code>tcp:2222</code></p> <p>etiquetas alvo : <code>pcf-ssh-proxy</code> , <code>diego-brain</code></p>



**Nota:** Se você quiser que suas regras de firewall permitam somente o tráfego em sua rede privada, modifique os **intervalos de IP de origem** da tabela de acordo.

3. Se você estiver usando apenas o projeto do GCP para implantar o Gerenciador de operações, poderá excluir as seguintes regras de firewall padrão:

- `default-allow-http`
- `default-allow-https`
- `default-allow-icmp`
- `default-allow-internal`
- `default-allow-rdp`
- `default-allow-ssh`

Se você estiver implantando **apenas o PKS** , continue com as [próximas etapas](#) .

Se você estiver implantando o **PAS** ou **outros tempos de execução** , prossiga para a etapa a seguir.


## Etapa 6: Criar Instância de Banco de Dados e Bancos de Dados

### Criar Instância do Banco de Dados

1. Para uma instalação de VPC compartilhada, selecione o projeto de serviço no console do GCP. Esta etapa e as etapas a seguir alocam recursos para o projeto de serviço, não para o projeto de host.
2. No console do GCP, selecione **SQL** e clique em **CREATE INSTANCE** .
3. Assegure-se de que o **MySQL** esteja selecionado e clique em **Avançar** .
4. No **MySQL** , selecione o tipo de instância **Segunda Geração** .
5. Clique em **Configure MySQL** sob sua escolha para o tipo de instância: Development, Staging ou Production.

6. Configure a instância da seguinte forma:

- **ID da instância** : `pcf-pas-sql`
- **Senha Raiz** : Defina uma senha para o usuário root.
- **Região** : selecione a região que você especificou ao criar redes.
- **Zona** : qualquer .
- **Configure o tipo de máquina e armazenamento** :
  - Clique em **Alterar** e selecione **db-n1-standard-2** .
  - Certifique-se de que **Ativar aumento automático de armazenamento** esteja selecionado. Isso permite que o armazenamento do banco de dados cresça automaticamente quando o espaço é necessário.
- **Ativar backups automáticos e alta disponibilidade** : faça as seguintes seleções:
  - Deixe **Automatizar backups** e **Ativar registro binário** selecionado.
  - Em **Alta disponibilidade** , selecione a caixa de seleção **Criar réplica de failover** .
- **Autorizar redes** : clique em **Adicionar rede** e crie uma rede com nome `all` que permita o tráfego `0.0.0.0/0` .

 **Nota:** Se você tiver atribuído endereços IP estáticos às suas instâncias NAT, poderá limitar o acesso às instâncias do banco de dados, especificando os endereços IP NAT.

7. Clique em **Criar** .


## Criar bancos de dados

1. Navegue até a página **Instâncias** e selecione a instância do banco de dados que você acabou de criar.
2. Selecione a guia **Bancos de Dados** .
3. Clique em **Criar banco de dados** para criar os seguintes bancos de dados:

- `account`
- `app_usage_service`
- `autoscale`
- `ccdb`
- `console`
- `diego`
- `loket`
- `networkpolicyserver`
- `nfsvolume`
- `notifications`
- `routing`
- `silk`
- `uaa`
- `credhub`

4. Selecione a guia **USERS** .

5. Clique em **Criar conta de usuário** para criar um nome de usuário e senha exclusivos para cada banco de dados criado acima. Para o **nome do host** , selecione **Permitir qualquer host** . Você deve criar um total de quatorze contas de usuário.

 **Nota:** Assegure-se de que o usuário do banco de dados networkpolicyserver tenha a `ALL PRIVILEGES` permissão.

## Etapa 7: criar depósitos de armazenamento

1. Com o projeto de projeto único ou de serviço VPC compartilhado selecionado no console do GCP, selecione **Armazenamento** > **Navegador** .
2. Usando **CREATE BUCKET** , crie buckets com os seguintes nomes. Para **Classe de armazenamento padrão** , selecione **Multi-regional** :

- `pcf-buildpacks`
- `pcf-droplets`
- `pcf-packages`
- `pcf-resources`

## Etapa 8: criar um balanceador de carga HTTP

Para balanceamento de carga, você pode usar um balanceador de carga HTTP global ou um balanceador de carga interno e regional com um endereço IP privado.


Instalações autônomas e de projeto único geralmente usam um balanceador de carga HTTP global. Consulte [Criar Balanceador de Carga HTTP](#) para saber como configurar isso.

A instalação do Shared-VPC normalmente usa um balanceador de carga TCP / UDP interno para minimizar os endereços IP públicos. Consulte [Criar o Load Balancer Interno](#) para saber como configurar isso.

## Criar balanceador de carga interno

Para criar um balanceador de carga interno para o Gerenciador de operações no GCP, faça o seguinte.

1. Crie um balanceador de carga TCP / UDP interno para cada região da implantação do PCF.

 **Observação** : o balanceador de carga interno do GCP (iLB) é um produto regional. Dentro da mesma VPC / rede, as VMs cliente em uma região diferente do iLB não podem acessar o iLB. Veja [o problema de roteamento global](#) na documentação do Google Cloud *Setting Up Internal Load Balancing* .

2. Atribuir endereços IP privados aos balanceadores de carga.
3. Depois de implantar o Gerenciador de operações, siga as instruções em [Criar ou atualizar uma extensão de VM](#) para adicionar uma extensão de VM personalizada que aplique o balanceamento de carga interno a todas as VMs implantadas pelo BOSH.
  - Por exemplo, o código de manifesto a seguir adiciona uma extensão de VM `backend-pool` às VMs de PCF:

```
vm_extensions:  
- name: backend-pool  
cloud_properties:  
  ephemeral_external_ip: true  
backend_service:  
  name: name-of-backend-service  
  scheme: INTERNAL
```

## Criar balanceador de carga HTTP

Para criar um balanceador de carga HTTP global para o PCF no GCP, faça o seguinte:

1. [Criar grupo de instâncias](#)
2. [Criar verificação de saúde](#)
3. [Configurar back end](#)
4. [Configurar o front end](#)

### Criar grupo de instâncias

1. Navegue para o **Compute Engine** > **Grupos de instâncias** .
2. Clique em **CREATE INSTANCE GROUP** .

3. Preencha o formulário da seguinte forma:

- o Para **Nome**, insira `pcf-http-lb`.
- o Para **Localização**, selecione **Zona única**.
- o Para **Zona**, selecione a primeira zona da sua região.  
Exemplo: para região `us-west1`, selecione zona `us-west1-a`.
- o Em **Tipo de grupo**, selecione **Grupo de instâncias não gerenciadas**.
- o Para **rede**, selecione `pcf-virt-net`.
- o Para **Sub-** `pcf-pas-subnet-my-gcp-region` rede, selecione a sub - rede que você criou anteriormente.
- o Clique em **Criar**.

4. Crie um segundo grupo de instâncias com os seguintes detalhes:

- o **Nome**: `pcf-http-lb`
- o **Localização**: **zona única**
- o **Zona**: selecione a segunda zona da sua região.  
Exemplo: para região `us-west1`, selecione zona `us-west1-b`.
- o **Tipo de grupo**: selecione **Grupo de instâncias não gerenciadas**.
- o **Rede**: selecione `pcf-virt-net`.
- o **Sub** - `pcf-pas-subnet-my-gcp-region` rede: selecione a sub - rede que você criou anteriormente.

5. Crie um terceiro grupo de instâncias com os seguintes detalhes:

- o **Nome**: `pcf-http-lb`
- o **Localização**: **zona única**
- o **Zona**: selecione a terceira zona da sua região.  
Exemplo: para região `us-west1`, selecione zona `us-west1-c`.
- o **Tipo de grupo**: selecione **Grupo de instâncias não gerenciadas**.
- o **Rede**: selecione `pcf-virt-net`.
- o **Sub** - `pcf-pas-subnet-my-gcp-region` rede: selecione a sub - rede que você criou anteriormente.

## Criar verificação de saúde

1. Navegue para o **Compute Engine** > **verificações de integridade**.

2. Clique em **CRIAR VERIFICAÇÃO DE SAÚDE**.

3. Preencha o formulário da seguinte forma:

- o **Nome**: `pcf-cf-public`
- o **Porta**: `8080`
- o **Caminho de solicitação**: `/health`
- o **Verifique o intervalo**: `30`
- o **Timeout**: `5`
- o **Limiar saudável**: `10`
- o **Limiar insalubre**: `2`

4. Clique em **Criar**.

## Configurar back end

1. Navegue até **Serviços de rede** > **Balanceamento de carga**.

2. Clique em **CREATE LOAD BALANCER**.

3. Em **Balanceamento de carga HTTP (S)**, clique em **Iniciar configuração**.

4. Para o **nome**, digite `pcf-global-pcf`.

5. Selecione a **configuração de back-end**

- a. Na lista suspensa, selecione **Serviços de back-end** > **Criar um serviço de back-end**.

b. Preencha o formulário da seguinte forma:

c. **Nome** : `pcf-http-lb-backend` .

d. **Protocolo** : `HTTP` .

e. **Porto chamado** : `http` .

f. **Timeout** : `10 seconds` .

g. Em **Backends > Novo back-end** , selecione o **grupo Instância** que corresponde à primeira zona do grupo de instâncias de várias zonas que você criou. Por exemplo: `pcf-http-lb (us-west1-a)` . Clique em **Concluído** .

h. Clique em **Adicionar back-end** , selecione o **grupo Instância** que corresponde à segunda zona do grupo de instâncias de várias zonas que você criou. Por exemplo: `pcf-http-lb (us-west1-b)` . Clique em **Concluído** .

i. Clique em **Adicionar back-end** , selecione o **grupo Instância** que corresponde à terceira zona do grupo de instâncias de várias zonas que você criou. Por exemplo: `pcf-http-lb (us-west1-c)` . Clique em **Concluído** .

j. **Verificação de saúde** : selecione a `pcf-cf-public` verificação de saúde que você criou.

k. **Cloud CDN** : verifique se o Cloud CDN está desativado.

l. Clique em **Criar** .

## Configurar o front end

1. Clique em **Regras de host e caminho** para preencher os campos padrão e uma marca de seleção verde.

2. Selecione **Configuração de front-end** e adicione o seguinte:

- **Nome** : `pcf-cf-lb-http`

- **Protocolo** : `HTTP`

- **IP** : execute os seguintes passos:

1. Selecione **Criar endereço IP** .

2. Digite um **nome** para o novo endereço IP estático e uma descrição opcional. Por exemplo, `pcf-global-pcf` .

3. Clique em **Reservar** .


- **Porta** : `80`

3. Se você usar um certificado SSL confiável ou já tiver um certificado autoassinado, continue na etapa 5.

4. Se você quiser usar um certificado autoassinado gerado durante [a configuração de rede do PAS](#) , pule a próxima etapa de adicionar a configuração do frontend HTTPS até depois de gerar o certificado no PAS. Depois de gerar o certificado, retorne à etapa 5 usando as seguintes diretrizes:

- Copie e cole o conteúdo gerado dos campos **Certificado de Rescisão SSL de Terminação e Chave Privada** do PAS nos campos certificado público e chave privada.
- Como você está usando um certificado autoassinado, não insira um valor no campo **Cadeia de Certificados** .

5. Clique em **Adicionar IP e porta de front-end** e adicione o seguinte:

 **Nota:** ignore esta etapa se você não tiver um certificado SSL autoassinado ou confiável. Ao configurar o bloco para o tempo de execução escolhido, você terá a oportunidade de criar um novo certificado autoassinado. Ao criar um certificado, você pode concluir a seção **Adicionar IP e porta de front-end** .

- **Nome** : `pcf-cf-lb-https`

- **Protocolo** : `HTTPS`

- **Endereço IP** : selecione o `pcf-global-pcf` endereço que você criou para o **IP e a porta de frontend** anteriores .

- **Porta** : `443`

- Selecione **Criar um novo certificado** . O diálogo **Criar um Novo Certificado** é exibido.

- o No campo **Nome** , insira um nome para o certificado.
- o No campo **Certificado de Chave Pública** , copie o conteúdo do seu certificado público ou carregue seu certificado como um arquivo .pem. Se o certificado for gerado em tempo de execução, copie e cole o conteúdo gerado do campo Certificado do tempo de execução no campo Ops Manager **Public key certificate** .
- o No campo **Cadeia de certificados** , insira ou carregue sua cadeia de certificados no formato .pem. Se você estiver usando um certificado autoassinado, como um certificado gerado pelo PAS ou PKS, não insira um valor no campo **Cadeia de Certificados** .
- o No campo **Chave privada** , copie o conteúdo ou faça o upload do arquivo .pem da chave privada do certificado. Se o certificado é gerado pelo tempo de execução, copiar e colar o conteúdo gerado a partir do campo Chave Privada do tempo de execução para o Ops Gerente **de chave privada** campo.

6. Revise a configuração de frontend concluída.

7. Clique em **Revisar e finalize** para verificar sua configuração.

8. Clique em **Criar** .

## Etapa 9: Criar o Balanceador de Carga do TCP WebSockets


O balanceador de carga para registros finais com WebSockets para PCF no GCP opera na porta TCP `443` .

1. No console do GCP, selecione **Serviços de rede**> **Balanceamento de carga**> **Criar balanceador de carga** .

2. Em **Balanceamento de carga TCP** , clique em **Iniciar configuração** .

3. Na tela **Criar uma configuração do balanceador de carga** , faça as seguintes seleções:

- Sob **virados para o Internet** ou apenas para uso interno , selecione **A partir da Internet para o meu VMs** .
- Em **Várias regiões** ou **região única** , selecione **Apenas região única** .

 **Create a load balancer**

Please answer a few questions to help us select the right load balancing type for your application

**Internet facing or internal only**

Do you want to load balance traffic from the Internet to your VMs or only between VMs in your network?

☒ From Internet to my VMs

☐ Only between my VMs

**Multiple regions or single region**

Do you want to place the backends for your load balancer in a single region or across multiple regions?

☐ Multiple regions (or not sure yet)

☒ Single region only

**Connection termination**

Do you want to offload TCP or SSL processing to the Load Balancer?

☐ Yes (TCP Proxy or SSL Proxy - recommended)

☒ No (TCP)

**Continue**

- Em **Terminação de conexão** , selecione **Não (TCP)** .

4. Clique em **Continuar** .

5. Na janela **Novo balanceador de carga TCP** , insira `pcf-wss-logs` no campo **Nome** .

6. Clique em **Configuração de back-end** para configurar o serviço de back - end :

## Backend configuration

**Name** ?

pcf-wss-logs

**Region** ?

us-central1

**Backends** ?

Select existing instance groups    Select existing instances

No instance groups in this region

**Backup pool** ? (Optional)

None

**Failover ratio** ?

10 %

**Health check** ?

pcf-gorouter (HTTP)

port: 8080, timeout: 5s, check interval: 5s, unhealthy threshold: 2 attempts

**Session affinity** ?

None

- **Região** : selecione a região que você usou para criar a rede em [Criar uma rede GCP com sub-redes](#) .
- Na lista suspensa **Verificação de saúde** , crie uma verificação de integridade com os seguintes detalhes:
  - **Nome** : pcf-gorouter
  - **Porta** : 8080
  - **Caminho de solicitação** : /health
  - **Verifique o intervalo** : 30
  - **Timeout** : 5
  - **Limiar saudável** : 10
  - **Limite insalubre** : 2 A configuração back-end seção mostra uma marca de seleção verde.

7. Clique em **Configuração de front-end** para abrir sua janela de configuração e preencha os campos:

- **Protocolo** : TCP
- **IP** : execute os seguintes passos:

1. Selecione **Criar endereço IP** .



2. Para nome **Name** para o novo endereço IP estático e uma descrição opcional. Por exemplo, `pcf-gorouter-wss`.
3. Clique em **Reservar**.

o **Porta**: `443`

8. Clique em **Revisar e finalize** para verificar sua configuração.

### Review and finalize

---

**Backend**  
Name: **pcf-wss-logs**   Region: **us-central1**   Session affinity: **None**   Health check: **pcf-gorouter**  
**Frontend**  

Protocol ^	IP:Port
TCP	<div></div> :443

9. Clique em **Criar**.

## Etapa 10: criar um balanceador de carga de proxy SSH

1. No console do GCP, selecione **Serviços de rede** > **Balanceamento de carga** > **Criar balanceador de carga**.
2. Em **Balanceamento de carga TCP**, clique em **Iniciar configuração**.
3. Sob **virados para o Internet** ou **apenas para uso interno**, selecione **A partir da Internet para o meu VMs**.

### Create a load balancer

Please answer a few questions to help us select the right load balancing type for your application

**Internet facing or internal only**  
Do you want to load balance traffic from the Internet to your VMs or only between VMs in your network?

☒ From Internet to my VMs  
☐ Only between my VMs

**Multiple regions or single region**  
Do you want to place the backends for your load balancer in a single region or across multiple regions?

☐ Multiple regions (or not sure yet)  
☒ Single region only

**Connection termination**  
Do you want to offload TCP or SSL processing to the Load Balancer?

☐ Yes (TCP Proxy or SSL Proxy - recommended)  
☒ No (TCP)

**Continue**

4. Em **Terminação de conexão**, selecione **Não (TCP)**.

5. Clique em **Continuar**.

6. Na janela **Novo balanceador de carga TCP**, insira `pcf-ssh-proxy` o campo **Nome**.

7. Selecione **Configuração de back-end** e insira os seguintes valores de campo:

- o **Região**: selecione a região usada para criar a rede em [Criar uma rede GCP com sub-rede](#).

- Pool de backup : None
- Proporção de failover : 10%
- Exame de saúde : No health check

## Backend configuration

---

**Name** ?

pcf-ssh-proxy

**Region** ?

us-central1

**Backends** ?

Select existing instance groups    Select existing instances

No instance groups in this region

**Backup pool** ? (Optional)

None

**Failover ratio** ?

10 %

**Health check** ?

No health check

**Session affinity** ?

None


8. Selecione **Configuração de front-end** e adicione o seguinte:

- Protocolo : TCP
- IP : execute os seguintes passos:
  - Selecione **Criar endereço IP**.
  - Digite um **nome** para o novo endereço IP estático e uma descrição opcional. Por exemplo, `pcf-ssh-proxy`.
  - Clique em **Reservar**.
- Porta : 2222

9. (Opcional) Revise e finalize seu balanceador de carga.

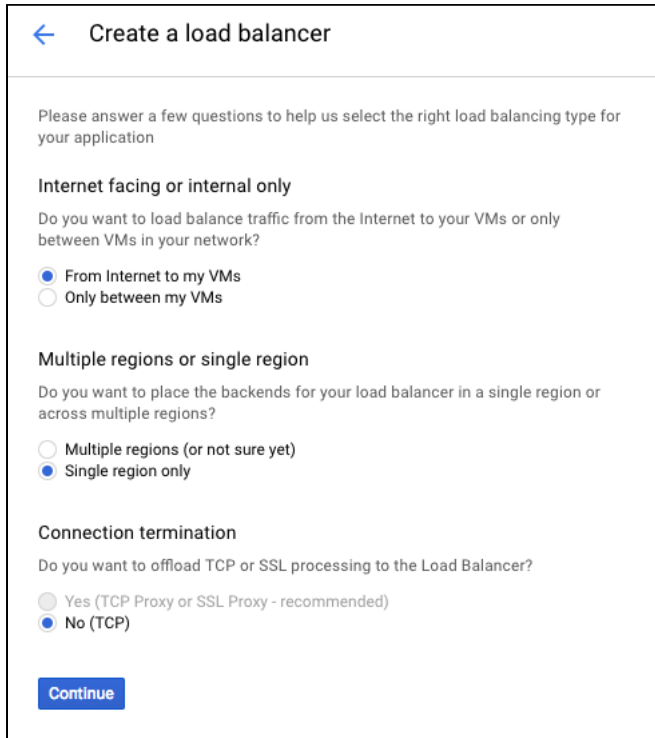
10. Clique em **Criar**.

## Etapa 11: criar o balanceador de carga para o roteador TCP

 **Nota:** Esta etapa é opcional e será necessária apenas se você ativar o roteamento TCP em sua implementação.

Para criar um balanceador de carga para o roteamento TCP no GCP, faça o seguinte:

1. No console do GCP, selecione **Serviços de rede** > **Balanceamento de carga** > **Criar balanceador de carga**.
2. Em **Balanceamento de carga TCP**, clique em **Iniciar configuração**.
3. Em **Terminação de conexão**, selecione **Não (TCP)**. Clique em **Continuar**.



**Create a load balancer**

Please answer a few questions to help us select the right load balancing type for your application

**Internet facing or internal only**  
Do you want to load balance traffic from the Internet to your VMs or only between VMs in your network?

☒ From Internet to my VMs  
☐ Only between my VMs

**Multiple regions or single region**  
Do you want to place the backends for your load balancer in a single region or across multiple regions?

☐ Multiple regions (or not sure yet)  
☒ Single region only

**Connection termination**  
Do you want to offload TCP or SSL processing to the Load Balancer?

☐ Yes (TCP Proxy or SSL Proxy - recommended)  
☒ No (TCP)

**Continue**

4. Na tela **Novo balanceador de carga TCP**, insira um nome exclusivo para o balanceador de carga no campo **Nome**. Por exemplo, `pcf-cf-tcp-lb`.

5. Selecione **Configuração de back-end** e insira os seguintes valores de campo:

- o **Região**: selecione a região usada para criar a rede em [Criar uma rede GCP com sub-rede](#).
- o Na lista suspensa **Verificação de saúde**, crie uma verificação de integridade com os seguintes detalhes:
  - **Nome**: `pcf-tcp-lb`
  - **Porta**: `80`
  - **Caminho de solicitação**: `/health`
  - **Verifique o intervalo**: `30`
  - **Timeout**: `5`
  - **Limiar saudável**: `10`
  - **Limiar insalubre**: `2`

- Clique em **Salvar e continue**.

## Backend configuration

---

**Name** ?

**Region** ?

**Backends** ?

**Backup pool** ? (Optional)

**Failover ratio** ?

%

**Health check** ?

port: 80, timeout: 5s, check interval: 30s, unhealthy threshold: 2 attempts

**Session affinity** ?

6. Selecione **Configuração de front-end** e adicione o IP de front end e a entrada de porta da seguinte maneira:

- **Protocolo** :
- **IP** : execute os seguintes passos:
  1. Selecione **Criar endereço IP**.
  2. Digite um **nome** para o novo endereço IP estático e uma descrição opcional. Por exemplo, .
  3. Clique em **Reservar**.
- **Porta** :

←

New TCP load balancer

Name ?

pcf-cf-tcp-lb

✓

Backend configuration

Your backend is configured

✓

Frontend configuration

Your frontend is configured

→

ⓘ

Review and finalize

Optional

Create

Cancel

Frontend configuration

Specify an IP address, port and protocol. This IP address is the frontend IP for your clients requests.

Protocol:TCP, IP:35.235.110.100, Port:1024-65535

Not saved

+ Add Frontend IP and port

7. Clique em **Revisar e finalize** para verificar sua configuração.

8. Clique em **Criar** .

## Etapa 12: adicionar registros DNS para seus balanceadores de carga

Nesta etapa, você redireciona as consultas do seu domínio para os endereços IP de seus balanceadores de carga.

1. Localize os endereços IP estáticos dos balanceadores de carga que você criou em [Preparando para implantar o Gerenciador de operações no GCP manualmente](#) :

Um balanceador de carga HTTP (S) chamado `pcf-global-pcf`

Um balanceador de carga TCP para WebSockets chamado `pcf-wss-logs`

Um balanceador de carga TCP chamado `pcf-ssh-proxy`

Um balanceador de carga TCP chamado `pcf-cf-tcp-lb`

💡

**Nota:** Você pode localizar o endereço IP estático de cada balanceador de carga clicando em seu nome em **Serviços de rede> Balanceamento de carga** no console do GCP.

2. Faça login no registrador DNS que hospeda seu domínio. Exemplos de registradores DNS incluem Network Solutions, GoDaddy e Register.com.

3. Crie **registros** com seu registrador DNS que mapeiam nomes de domínio para os endereços IP estáticos públicos dos balanceadores de carga localizados acima:

Crie e mapeie este registro ...	Para o IP deste balanceador de carga	Requeridos
<code>*.sys.MY-DOMAIN</code> Exemplo: <code>*.sys.example.com</code>	<code>pcf-global-pcf</code>	sim
<code>*.apps.MY-DOMAIN</code> Exemplo: <code>*.apps.example.com</code>	<code>pcf-global-pcf</code>	sim
<code>doppler.sys.MY-DOMAIN</code> Exemplo: <code>doppler.sys.example.com</code>	<code>pcf-wss-logs</code>	sim
<code>loggregator.sys.MY-DOMAIN</code> Exemplo: <code>loggregator.sys.example.com</code>	<code>pcf-wss-logs</code>	sim

<https://docs.pivotal.io/pivotalcf/2-4/om/gcp/prepare-env-manual.html>

21/22

ssh.sys.MY-DOMAIN Exemplo: ssh.sys.example.com	pcf-ssh-proxy	Sim, para permitir o acesso SSH a aplicativos
tcp.MY-DOMAIN Exemplo: tcp.example.com	pcf-cf-tcp-lb	Não, apenas configure se você ativou o recurso de roteamento TCP

4. Salve as alterações na interface da Web do seu registrador de DNS.

5. Em uma janela de terminal, execute o seguinte `dig` comando para confirmar que você criou seu registro A com sucesso:

```
cavar SUBDOMAIN.EXAMPLE-URL.com
```

Onde `SUBDOMAIN.EXAMPLE-URL` está o subdomínio do seu balanceador de carga.

Você deve ver o registro que você acabou de criar:

```
;; SEÇÃO DE RESPOSTA:
xyz.EXAMPLE.COM. 1767 EM A 203.0.113.1
```

## Próximos passos

- (Opcional) Para se preparar para implantar um bloco PAS ou PKS no GCP, você pode fazer o download do bloco de tempo de execução necessário antecipadamente:
  - Para baixar o PAS, efetue login na [Rede Pivotal](#), selecione a versão de lançamento desejada e faça o download do **Serviço de Aplicativo Dinâmico**.
  - Para fazer o download do PKS, efetue login na [Rede Pivotal](#), selecione a versão de lançamento desejada e faça o download do **Pivotal Container Service**.
- Depois de iniciar o download do bloco, prossiga para a próxima etapa, [Implantando o Gerenciador de Ops no GCP Manualmente](#).