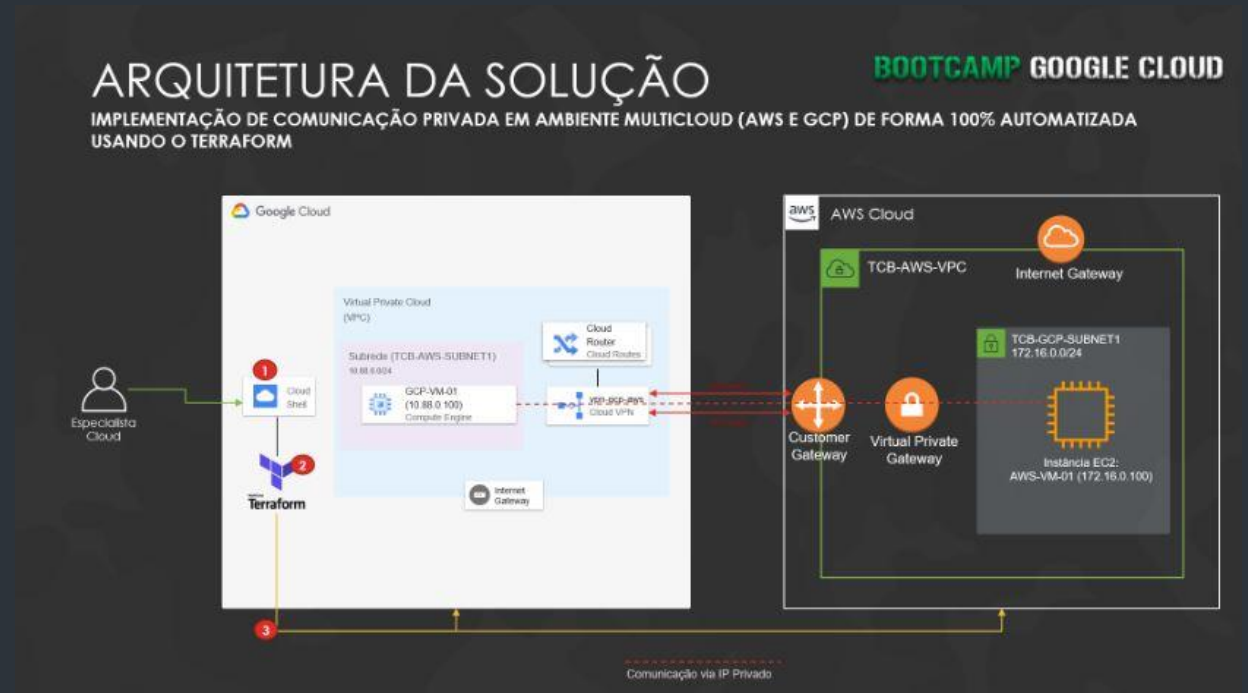




#pracima

Hands on – GCP | Network

- Implementação de Comunicação privada em ambiente MultiCloud (AWS e GCP) de forma 100% automatizada usando Terraform-infraestrutura as code



- Imagina que você trabalha em uma empresa que utiliza os serviços da Google Cloud e AWS, porém, no momento, em Arquiteturas separadas.
- Foi apresentado uma necessidade de interconectar as duas Arquiteturas, de forma completamente privada, fazendo uso do Virtual Private Gateway, Customer Gateway, Cloud Routers, Cloud VPN, entre outros serviços.
- Além disso, os recursos precisam estar em produção o mais breve possível, estipulando o prazo de uma semana. Visando ganhar tempo, se decidiu fazer a preparação de contas na GCP e AWS, para realizar a implementação de forma 100% automatizada utilizando o Terraform.

- ▶ Para solução deste hands-on foi utilizado necessário criar uma conta de serviço no GCP IAM e gerado a chave JSON que foi exportada e armazenada localmente.
- ▶ Os arquivos de configuração .sh e código declarativo para provisionar os recursos de infraestrutura (.tf) pode ser encontrado no [GitHub](#).
- ▶ Setando o service account do Google Cloud Platform.

```
lenowds@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-thecloudbootcamp)$ ./gcp_set_credentials.sh ~/developer.gserviceaccount.com.json
Created /home/lenowds/.config/gcloud/credentials_multiclouddeploy.json from /home/lenowds/developer.gserviceaccount.com.json.
Updated gcp_credentials_file_path in /home/lenowds/hands-on-tcb-bmc-gcp/terraform/terraform.tfvars.
lenowds@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-thecloudbootcamp)$
```

- ▶ Ativando a credencial do service account, checando a configuração de conta e validando a ativação do service account.

```
lenowds@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-thecloudbootcamp)$ gcloud auth activate-service-account --key-file ~/.config/gcloud/credentials_multiclouddeploy.json
Activated service account credentials for: [879989001652-compute@developer.gserviceaccount.com]
lenowds@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-thecloudbootcamp)$
```

```
lenowds@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-thecloudbootcamp)$ cat ~/.config/gcloud/credentials_multiclouddeploy.json | grep client_email
"client_email": "879989001652-compute@developer.gserviceaccount.com",
lenowds@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-thecloudbootcamp)$
```

```
lenowds@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-thecloudbootcamp)$ gcloud auth list
Credentialed Accounts

ACTIVE  ACCOUNT
*       879989001652-compute@developer.gserviceaccount.com
        lenowds@gmail.com
```

```
To set the active account, run:
$ gcloud config set account `ACCOUNT`
```

```
lenowds@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-thecloudbootcamp)$
```

- Setando o service account da AWS.

```
lenowds@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-thecloudbootcamp)$ ./aws_set_credentials.sh ~/accessKeys.csv
Created backup (/home/lenowds/.aws/credentials_multiclouddeploy.bak).
Created /home/lenowds/.aws/credentials_multiclouddeploy.
Updated aws_credentials_file_path in /home/lenowds/hands-on-tcb-bmc-gcp/terraform/terraform.tfvars.
lenowds@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-thecloudbootcamp)$
```

- Preparando o Terraform para provisionar o recursos.

```
lenowds@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-thecloudbootcamp)$ ./get_terraform.sh
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           % Done    Dload  Upload   Total   Spent    Left  Speed
100 15.2M  100 15.2M    0     0  71.8M      0 --:--:-- --:--:-- --:--:-- 71.8M
Successfully retrieved /home/lenowds/terraform/terraform.

To adjust your path: export PATH=/home/lenowds/terraform:${PATH}
lenowds@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-thecloudbootcamp)$
```

- Após, executar o comando ./gcp_set_project.sh no Cloud Shell.

- Verificar no Cloud Shell o usuário conectado no projeto, utilize o comando **whoami**.
- Gerar um par de chaves para o usuário conectado no projeto e restringir o acesso a chave privada.

```
lenowds@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-thecloudbootcamp)$ ssh-keygen -t rsa -f ~/.ssh/vm-ssh-key -C lenowds
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/lenowds/.ssh/vm-ssh-key.
Your public key has been saved in /home/lenowds/.ssh/vm-ssh-key.pub.
The key fingerprint is:
SHA256:a81tEENMiS1OLC83pEcsBH9oJbbZEb+ijGTVEkPu+Vk lenowds
The key's randomart image is:
+---[RSA 2048]-----+
|  .+Bo+*o.  |
|  +o@O++    |
|  XX+.+     |
|  +o+*  +   |
|  o o+S.E    |
|  o o o B o  |
|  . o = o o  |
|  . .       |
|             |
+---[SHA256]-----+
lenowds@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-thecloudbootcamp)$ chmod 400 ~/.ssh/vm-ssh-key
lenowds@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-thecloudbootcamp)$
```


- Importar a chave para o Google Cloud Plataform.

```
lenowds@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-thecloudbootcamp)$ gcloud compute config-ssh --ssh-key-file=~/.ssh/vm-ssh-key
Updating project ssh metadata...Updated [https://www.googleapis.com/compute/v1/projects/tcb-thecloudbootcamp].
Updating project ssh metadata...done.
You should now be able to use ssh/scp with your instances.
For example, try running:

$ ssh eua-app01.us-west1-b.tcb-thecloudbootcamp

lenowds@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-thecloudbootcamp)$
```

- No Google Shell executar o download da chave pública, armazenando localmente e na console da AWS importar dentro EC2 >> Network & Security >> Key Pairs.
- Provisionar os recursos utilizando terraform apply.

```
Apply complete! Resources: 34 added, 0 changed, 0 destroyed.

Outputs:

aws_instance_external_ip = "35.85.134.109"
aws_instance_internal_ip = "172.16.0.100"
gcp_instance_external_ip = <<EOT
34.105.121.236

EOT
gcp_instance_internal_ip = "10.88.0.100"
lenowds@cloudshell:~/hands-on-tcb-bmc-gcp/terraform (tcb-thecloudbootcamp)$
```

- Informações da VM Instance provisionada na GCP. Além da VM foi provisionado uma infraestrutura de rede e subrede, e, túnel vpc.

Creation time
Sep 14, 2021, 9:10:44 PM

Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	tcb-gcp-network	tcb-gcp-subnet1	10.88.0.100	—	gcp-vm-ip (34.105.121.236)	Premium	Off	View details

Public DNS PTR Record
None

Firewalls

- ☐ Allow HTTP traffic
- ☐ Allow HTTPS traffic

Network tags
None

Deletion protection

- ☐ Enable deletion protection

When deletion protection is enabled, instance cannot be deleted. [Learn more](#)

Confidential VM service

Disabled

Boot disk


Name	Image	Size (GB)	Device name	Type	Encryption	Mode	When deleting it
tcb-gcp-vm-01	ubuntu-1604-xenial-v20210429	10	persistent-disk-0	Standard persistent disk	Google managed	Boot, read/write	Delete disk
















➤ Informações da VM Instance provisionada na AWS.

Resumo da instância para i-04fb18ae942144cd7 (tcb-aws-vm-01)

Atualizado há less than a minute

[Informações](#)

 [Conectar](#) [Estado da instância ▼](#) [Ações ▼](#)

ID de instância  i-04fb18ae942144cd7 (tcb-aws-vm-01)	Endereço IPv4 público  35.85.134.109 endereço aberto 	Endereços IPv4 privados  172.16.0.100
Endereço IPv6 –	Estado da instância  Executando	DNS IPv4 público  ec2-35-85-134-109.us-west-2.compute.amazonaws.com endereço aberto 
DNS IPv4 privado  ip-172-16-0-100.us-west-2.compute.internal	Tipo de instância t3.micro	Endereços IP elásticos  35.85.134.109 [IP público]
ID da VPC  vpc-09743ee8a38eac22f (tcb-aws-vpc) 	Descoberta do AWS Compute Optimizer  Opte por participar do AWS Compute Optimizer para obter recomendações. Saiba mais 	Função do IAM –
ID da sub-rede  subnet-0ab42cad9277e6d75 (tcb-aws-subnet1) 		

➤ Conectivity test result.

☒ [test-hands-on-vpn](#) tcp 10.88.0.100 ([tcb-gcp-network](#)) 172.16.0.100 80 2021-09-14 (21:23:02) ✓ Reachable [VIEW](#)

Connected, host fingerprint: ssh-rsa 0 F5:3E:F2:51:02:70:50:09:C0:B6:77:CC:8C:AF:75:01:59:2F:0C:9B:CC:68:D8:00:8F:4B:A6:04:07:07:CE:B1

Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-1098-gcp x86_64)

* Documentation: <https://help.ubuntu.com>
 * Management: <https://landscape.canonical.com>
 * Support: <https://ubuntu.com/advantage>

39 packages can be updated.
 20 of these updates are security updates.
 To see these additional updates run: apt list --upgradable

The programs included with the Ubuntu system are free software;
 the exact distribution terms for each program are described in the
 individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
 applicable law.

```
lenowds@tcb-gcp-vm-01:~$ ping 172.16.0.100
PING 172.16.0.100 (172.16.0.100) 56(84) bytes of data.
64 bytes from 172.16.0.100: icmp_seq=1 ttl=63 time=16.5 ms
64 bytes from 172.16.0.100: icmp_seq=2 ttl=63 time=15.2 ms
64 bytes from 172.16.0.100: icmp_seq=3 ttl=63 time=15.2 ms
64 bytes from 172.16.0.100: icmp_seq=4 ttl=63 time=15.1 ms
64 bytes from 172.16.0.100: icmp_seq=5 ttl=63 time=15.1 ms
```

Connectivity test result

Test name
test-hands-on-vpn

Protocol
tcp

Source
10.88.0.100 ([tcb-gcp-network](#))

Source project
tcb-thecloudbootcamp (Network) / tcb-thecloudbootcamp (IP address)

Destination
172.16.0.100

Destination project
-

Destination port
80

Result

- Default egress network rule**
Network: [tcb-gcp-network](#)
Action: ALLOW
Priority: 65535
- Dynamic route**
Network: [tcb-gcp-network](#)
Destination IP range: 172.16.0.0/16
Priority: 100
Next hop: VPN tunnel
- VPN tunnel ([gcp-tunnel1](#))**
Cloud VPN gateway: [gcp-vpn-gw-us-west1](#)
Cloud VPN gateway IP address: 34.127.87.27
Remote peer gateway: -
Remote peer gateway IP address: 34.213.252.19
VPC network: [tcb-gcp-network](#)
Region: us-west1

CANCEL

➤ Destruindo os recursos provisionados, terraform destroy.

```
Destroy complete! Resources: 34 destroyed.
lenowds@cloudshell:~/hands-on-tcb-bmc-gcp/terraform (tcb-thecloudbootcamp) $
```



- Author: Leniel dos Santos
- Linkedin: <https://www.linkedin.com/in/leniel-dos-santos-7813a924/>