

Gcloud - Módulo 3 - Estabelecendo uma conexão privada entre dois provedores de cloud (GCP e AWS)

terça-feira, 18 de junho de 2024 23:14

Configuração da KEY do GCP no ambiente do Terraform no Cloud Shell

```
ricoy sistemas@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-gcp-aws-426901)$ ls -l ~
total 36
drwxrwxr-x 3 ricoy sistemas ricoy sistemas 4096 Jun 29 2022 hands-on-tcb-bmc-gcp
-rw-rw-r-- 1 ricoy sistemas ricoy sistemas 22621 Jun 19 01:53 hands-on-tcb-bmc-gcp.zip
-rw-r--r-- 1 ricoy sistemas ricoy sistemas 913 Jun 19 02:00 README-cloudshell.txt
-rw-r--r-- 1 ricoy sistemas 1001 2362 Jun 19 02:07 tcb-gcp-aws-426901-7980501d30d4.json
ricoy sistemas@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-gcp-aws-426901)$ ls
aws_set_credentials.sh gcp_set_credentials.sh gcp_set_project.sh get_terraform.sh LICENSE README.md terraform
ricoy sistemas@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-gcp-aws-426901)$ ./gcp_set_credentials.sh ~/.
.bash_history .docker/ .sudo_as_admin_successful
.bash_logout hands-on-tcb-bmc-gcp/ tcb-gcp-aws-426901-7980501d30d4.json
.bashrc hands-on-tcb-bmc-gcp.zip .terraform.d/
.cache/ .npm/ .vscode/
.codeoss/ .profile
.config/ README-cloudshell.txt

ricoy sistemas@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-gcp-aws-426901)$ ./gcp_set_credentials.sh ~/tcb-gcp-aws-426901-7980501d30d4.json
Created /home/ricoy_sistemas/.config/gcloud/credentials_multiclouddeploy.json from /home/ricoy_sistemas/tcb-gcp-aws-426901-7980501d30d4.json.
Updated gcp_credentials file path in /home/ricoy_sistemas/hands-on-tcb-bmc-gcp/terraform/terraform.tfvars.
ricoy sistemas@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-gcp-aws-426901)$ cat ./aws_set_credentials.sh
aws_set_credentials.sh gcp_set_project.sh LICENSE terraform/
gcp_set_credentials.sh get_terraform.sh README.md
ricoy sistemas@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-gcp-aws-426901)$ cat ./gcp_set_credentials.sh
```

Configuração do access key da AWS no ambiente do Terraform no Cloud Shell

```
ricoy sistemas@cloudshell:~ (tcb-gcp-aws-426901)$ ls
hands-on-tcb-bmc-gcp README-cloudshell.txt tcb-gcp-aws-426901-7980501d30d4.json
hands-on-tcb-bmc-gcp.zip tcb-aws-gcp-automation_accessKeys.csv
ricoy sistemas@cloudshell:~ (tcb-gcp-aws-426901)$ cd hands-on-tcb-bmc-gcp/
ricoy sistemas@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-gcp-aws-426901)$ ls
aws_set_credentials.sh gcp_set_credentials.sh gcp_set_project.sh get_terraform.sh LICENSE README.md terraform
ricoy sistemas@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-gcp-aws-426901)$ ./aws_set_credentials.sh ../tcb-aws-gcp-automation_accessKeys.csv
cp: cannot stat '/home/ricoy_sistemas/.aws/credentials_multiclouddeploy': No such file or directory
Created backup (/home/ricoy_sistemas/.aws/credentials_multiclouddeploy.bak).
Created /home/ricoy_sistemas/.aws/credentials_multiclouddeploy.
Updated aws_credentials_file_path in /home/ricoy_sistemas/hands-on-tcb-bmc-gcp/terraform/terraform.tfvars.
ricoy sistemas@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-gcp-aws-426901)$ 
```

Explorando o script de instalação do Terraform pelo editor do Cloud Shell

The screenshot shows the Cloud Shell Editor interface with the following details:

- EXPLORER:** A sidebar on the left showing the project structure:
 - HANDS... (selected)
 - terraform
 - aws_set_credentials.sh
 - gcp_set_credentials.sh
 - gcp_set_project.sh
 - get_terraform.sh (highlighted)
 - LICENSE
 - README.md
- Code Editor:** The main area displays the content of the get_terraform.sh script:

```
$ get_terraform.sh x $ gcp_set_credentials.sh $ aws_set_credentials.sh
$ get_terraform.sh
17
18 # Download Terraform utility.
19
20 # Download and extract Terraform utility in the terraform directory.
21 function getTerraform() {
22     # Places terraform in ~/terraform dir.
23     local T_VERSION='0.12.4/terraform_0.12.4_linux_amd64'
24     local T_URL="https://releases.hashicorp.com/terraform/${T_VERSION}.zip"
25     # ~ only expands when NOT quoted (below).
26     local T_DIR=~/terraform
27     local T_ZIP="${T_DIR}/terraform.zip"
28     local T_EXE="${T_DIR}/terraform"
29
30     if [ ! -e ${T_EXE} ]; then
31         echo "${T_EXE} already exists. Exiting."
32         echo ''
```
- Status Bar:** Shows the current file is Cloud Code - Sign in, and the status bar indicates Ln 1, Col 1, Spaces: 2, UTF-8 LF, Shell Script, Layout: Portuguese (Brazilian ABNT).

Instalação do Terraform através do script

```
(tcb-gcp-aws-426901) ricoy_sistemas@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-gcp-aws-426901)$ ./get_terraform.sh
% Total    % Received % Xferd  Average Speed   Time     Time      Current
          Dload  Upload Total   Spent   Left  Speed
100 15.2M  100 15.2M    0     0  24.4M  0:--:-- --:--:-- --:--:-- 24.4M
Successfully retrieved /home/ricoy_sistemas/terraform/terraform.

To adjust your path: export PATH=/home/ricoy_sistemas/terraform:${PATH}
ricoy_sistemas@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-gcp-aws-426901)$ terraform
Usage: terraform [global options] <subcommand> [args]

The available commands for execution are listed below.
The primary workflow commands are given first, followed by
less common or more advanced commands.

Main commands:
  init      Prepare your working directory for other commands
  validate  Check whether the configuration is valid
  plan     Show changes required by the current configuration
```

Execução do script de definição do project_id do Google Cloud

```
(tcb-gcp-aws-426901) ricoy_sistemas@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-gcp-aws-426901)$ ./gcp_set_project.sh
Updated gcp_project_id in /home/ricoy_sistemas/hands-on-tcb-bmc-gcp/terraform/terraform.tfvars.
ricoy_sistemas@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-gcp-aws-426901)$ cat /home/ricoy_sistemas/hands-on-tcb-bmc-gcp/terraform/ter
raform.tfvars
/*
 * Initialized Terraform variables.
 */

gcp_credentials_file_path = "/home/ricoy_sistemas/.config/gcloud/credentials_multiclouddeploy.json"
aws_credentials_file_path = "/home/ricoy_sistemas/.aws/credentials_multiclouddeploy"
gcp_project_id = "tcb-gcp-aws-426901"
ricoy_sistemas@cloudshell:~/hands-on-tcb-bmc-gcp (tcb-gcp-aws-426901)$
```

Geração da chave ssh no CloudShell

```
(tcb-gcp-aws-426901) ricoy_sistemas@cloudshell:~ (tcb-gcp-aws-426901)$ ssh-keygen -t rsa -f ~/.ssh/vm-ssh-key -C ricoy_sistemas
Generating public/private rsa key pair.
Created directory '/home/ricoy_sistemas/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ricoy_sistemas/.ssh/vm-ssh-key
Your public key has been saved in /home/ricoy_sistemas/.ssh/vm-ssh-key.pub
The key fingerprint is:
SHA256:RSyrW57SqQEjrSkRm6ZI4ZtC6fWmbeLW0uB2/kHrcTo ricoy sistemas
```

Importação da chave SSH para a Gcloud

```
(tcb-gcp-aws-426901) ricoy_sistemas@cloudshell:~/.ssh (tcb-gcp-aws-426901)$ gcloud compute config-ssh --ssh-key-file=~/ssh/vm-ssh-key
Updating project ssh metadata...working..Updated [https://www.googleapis.com/compute/v1/projects/tcb-gcp-aws-426901].
Updating project ssh metadata...done.
WARNING: No host aliases were added to your SSH configs because you do not have any running instances. Try running this command again after running some instances.
ricoy_sistemas@cloudshell:~/.ssh (tcb-gcp-aws-426901)$
```

Google Cloud tcb-gcp-aws ssh

Compute Engine Metadata EDIT REFRESH LEARN

Virtual machines VM instances Instance templates Sole-tenant nodes Machine images TPUs Committed use discounts Reservations

All instances in this project inherit these SSH keys. [Learn more](#)

METADATA SSH KEYS

Username ↑	Key
ricoy_sistemas	ssh-rsa...

EQUIVALENT REST

Importação da chave ssh na AWS

AWS Services Search [Alt+S] N. Virginia aws-admin @ 6050-9227-3258

EC2 VPC RDS CloudFront Elastic Beanstalk S3 DynamoDB Simple Notification Service

EC2 Dashboard EC2 Global View Events Console-to-Code [Preview](#)

Instances Instances Instance Types Launch Templates Spot Requests Savings Plans

Successfully imported key pair

Key pairs (1/1) Info

Name	Type	Created	Fingerprint	ID
vm-ssh-key	rsa	2024/06/20 22:15 GMT-3	7d:70:51:2d:91:11:dc:df:3c:5a:c6:2...	key-0c6...

Execução do "terraform plan" para pré-visualizar os recursos que serão criados na AWS e GCP

(tcb-gcp-aws-426901) +

The connection to your Google Cloud Shell was lost.

Plan: 41 to add, 0 to change, 0 to destroy.

Changes to Outputs:

```
+ aws_instance_external_ip = (known after apply)
+ aws_instance_internal_ip = "172.16.0.100"
+ gcp_instance_external_ip = (known after apply)
+ gcp_instance_internal_ip = "10.88.0.100"
```

Note: You didn't use the -out option to save this plan, so Terraform can't guarantee to take exactly these actions if you run "terraform apply" now.

ricoy_sistemas@cloudshell:~/hands-on-tcb-bmc-gcp/terraform (tcb-gcp-aws-426901) \$

Execução do comando "terraform apply" para provisionamento dos recursos na AWS e GCP

```

Enter a value: yes

aws_instance.tcb-aws-vm-01: Creating...
aws_instance.tcb-aws-vm-01: Still creating... [10s elapsed]
aws_instance.tcb-aws-vm-01: Creation complete after 13s [id=i-08d99e8f2e136302f]
aws_eip.aws-ip: Creating...
aws_eip.aws-ip: Creation complete after 2s [id=eipalloc-0b9cab56d3654eda3]
google_compute_instance.tcb-gcp-vm-01: Creating...
google_compute_instance.tcb-gcp-vm-01: Still creating... [10s elapsed]
google_compute_instance.tcb-gcp-vm-01: Creation complete after 13s [id=projects/tcb-gcp-aws-426901/zones/us-west1-a/instances/tcb-gcp-vm-01]

Apply complete! Resources: 3 added, 0 changed, 0 destroyed.

Outputs:

aws_instance_external_ip = "35.95.231.24"
aws_instance_internal_ip = "172.16.0.100"
gcp_instance_external_ip = "34.82.218.132"
gcp_instance_internal_ip = "10.88.0.100"
ricoy sistemas@cloudshell:~/hands-on-tcb-bmc-gcp/terraform (tcb-gcp-aws-426901)§

```

Recursos criados na GCP

The screenshot shows the Google Cloud Platform Compute Engine VM instances page. The sidebar on the left is titled 'Virtual machines' and has a 'VM instances' section selected. The main table lists one instance:

Status	Name	Zone	Recommendations	In use by	Internal IP	External IP	Connect
<input checked="" type="checkbox"/>	tcb-gcp-vm-01	us-west1-a			10.88.0.100 (nic0)	34.82.218.132 (nic0)	SSH

Below the table, there are 'Related actions' buttons for 'Explore Backup and DR', 'View billing report', and 'Monitor VMs'.

The screenshot shows the Google Cloud Platform VPC networks page. The sidebar on the left is titled 'VPC network' and has a 'VPC networks' section selected. The main table lists one VPC network:

Name	Subnets	MTU	Mode	IPv6 ULA range	Gateways	Firewall rules	Global dynamic routing
default	41	1460	Auto			4	Off
tcb-gcp-network	1	1460	Custom			4	Off

Google Cloud tcb-gcp-aws VPN Search 1 ? ...

Network Connectivity Center

VPN

Cloud VPN Tunnels CLOUD VPN GATEWAYS PEER VPN GATEWAYS

CREATE VPN TUNNEL

Filter Enter property name or value

<input type="checkbox"/>	Name ▲	Cloud VPN gateway (IP)	Peer VPN gateway (IP)	Cloud Router BGP IP address	Peer BGP IP address	VPN tu	Actions
<input type="checkbox"/>	gcp-tunnel1	gcp-vpn-gw-us-west1 35.242.48.219	aws-gateway 44.233.23.99	169.254.21.218	169.254.21.217	✓ Est	⋮
<input type="checkbox"/>	gcp-tunnel2	gcp-vpn-gw-us-west1 35.242.48.219	aws-gateway 44.236.182.114	169.254.138.198	169.254.138.197	✓ Est	⋮
<input type="checkbox"/>	gcp-tunnel3	gcp-vpn-gw-us-west1 34.157.246.153	aws-gateway 54.68.142.18	169.254.122.158	169.254.122.157	✓ Est	⋮
<input type="checkbox"/>	gcp-tunnel4	gcp-vpn-gw-us-west1 34.157.246.153	aws-gateway 54.186.240.158	169.254.168.250	169.254.168.249	✓ Est	⋮

Google Cloud tcb-gcp-aws VPN Search 1 ? ...

Network Connectivity Center

Cloud Router

Routers **CREATE ROUTER** **REFRESH**

Filter

<input type="checkbox"/>	Name ▲	Network	Region	Interconnect encryption	Google ASN	Interconnect / VPN gateway	Connection	BG
<input type="checkbox"/>	gcp-router1	tcb-gcp-network	us-west1	Unencrypted	65000	gcp-vpn-gw-us-west1	gcp-tunnel1	✓ aw
<input type="checkbox"/>	gcp-router2	tcb-gcp-network	us-west1	Unencrypted	65000	gcp-vpn-gw-us-west1	gcp-tunnel2	✓ aw
<input type="checkbox"/>	gcp-router3	tcb-gcp-network	us-west1	Unencrypted	65000	gcp-vpn-gw-us-west1	gcp-tunnel3	✓ aw
<input type="checkbox"/>	gcp-router4	tcb-gcp-network	us-west1	Unencrypted	65000	gcp-vpn-gw-us-west1	gcp-tunnel4	✓ aw

Recursos criados na AWS

aws Services Search [Alt+S] Oregon aws-admin @ 6050-9227-3258

EC2 VPC RDS CloudFront Elastic Beanstalk S3 DynamoDB Simple Notification Service

EC2 Dashboard EC2 Global View Events Instances Instances Instance Types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts

Instances (1) Info

Find Instance by attribute or tag (case-sensitive)

All states

<input type="checkbox"/>	Name ▲	Instance ID	Instance state	Instance type	Status check	Alarm status
<input type="checkbox"/>	tcb-aws-vm-01	i-08d99e8f2e136302f	Running	t3.micro	2/2 checks passed	View alarms +

Select an instance

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Your VPCs (2) Info

Last updated less than a minute ago

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
-	vpc-0541ba805dbe3f361	Available	172.31.0.0/16	-
tcb-aws-vpc	vpc-09c2ec308eaa195e1	Available	172.16.0.0/16	-

Select a VPC above

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Subnets (5) Info

Last updated 1 minute ago

Name	Subnet ID	State	VPC
-	subnet-0cd35d57cc12c5c41	Available	vpc-0541ba805dbe3f361
-	subnet-06efccd55fa28c694	Available	vpc-0541ba805dbe3f361
-	subnet-038006a173590c54d	Available	vpc-0541ba805dbe3f361
-	subnet-0c95dff4ce93f1049	Available	vpc-0541ba805dbe3f361
tcb-aws-subnet1	subnet-014916e7b59fd8b30	Available	vpc-09c2ec308eaa195e1 tcb-a..

Select a subnet

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private network (VPN)

Customer gateways

Virtual private gateways

Site-to-Site VPN connections

Customer gateways (2) info

Last updated 1 minute ago

Name	Customer gateway ID	State	BGP ASN	IP address
aws-customer-gw	cgw-08905d18096cf0abf	Available	65000	34.157.246.15
aws-customer-gw	cgw-05bf12a9402cd9fb	Available	65000	35.242.48.219

Select a customer gateway

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private network (VPN)

Site-to-Site VPN connections

Client VPN endpoints

AWS Verified Access

Verified Access

VPN connections (2) Info

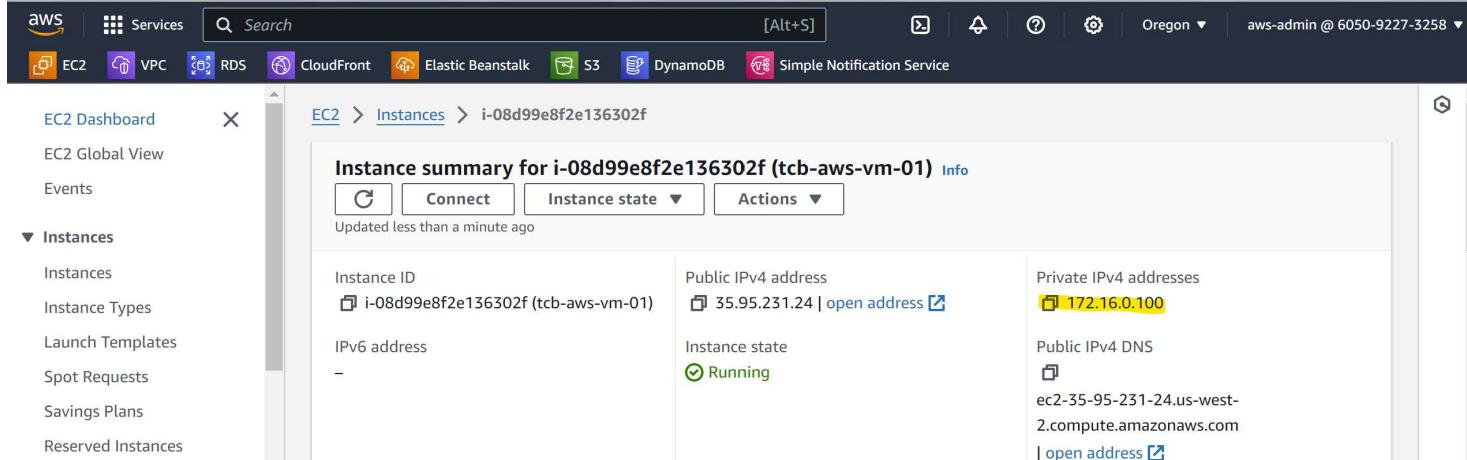
Last updated 1 minute ago

Name	VPN ID	State	Virtual private gateway	Transit gateway
aws-vpn-connection1	vpn-08bc86e8094e935c7	Available	vgw-09dfac39511bce325	-
aws-vpn-connection2	vpn-08f5009058a12c708	Available	vgw-09dfac39511bce325	-

Select a VPN connection

Teste de comunicação da VPN entre GCP e AWS

1. Obtenção do IP privado da instância criada na AWS



EC2 Dashboard X EC2 > Instances > i-08d99e8f2e136302f (tcb-aws-vm-01) [Info](#)

Instances

Instance ID: i-08d99e8f2e136302f (tcb-aws-vm-01)

Public IPv4 address: 35.95.231.24 | [open address](#)

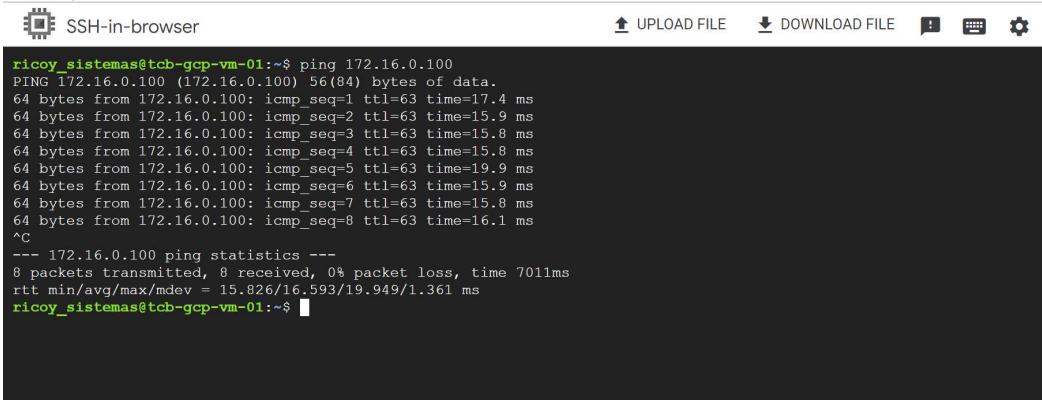
Private IPv4 addresses: 172.16.0.100

IPv6 address: -

Instance state: Running

Public IPv4 DNS: ec2-35-95-231-24.us-west-2.compute.amazonaws.com | [open address](#)

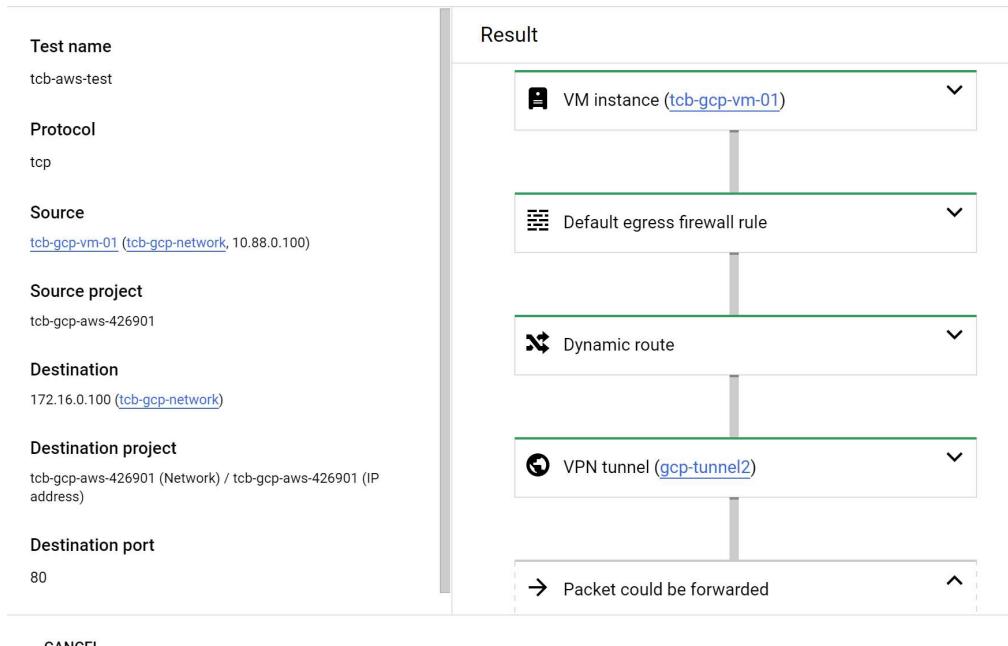
2. Conexão ssh na instância criada no GCP e execução do comando ping para validar a comunicação entre as duas redes



```
ricoy_sistemas@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=17.4 ms
64 bytes from 172.16.0.100: icmp_seq=2 ttl=63 time=15.9 ms
64 bytes from 172.16.0.100: icmp_seq=3 ttl=63 time=15.8 ms
64 bytes from 172.16.0.100: icmp_seq=4 ttl=63 time=15.8 ms
64 bytes from 172.16.0.100: icmp_seq=5 ttl=63 time=19.9 ms
64 bytes from 172.16.0.100: icmp_seq=6 ttl=63 time=15.9 ms
64 bytes from 172.16.0.100: icmp_seq=7 ttl=63 time=15.8 ms
64 bytes from 172.16.0.100: icmp_seq=8 ttl=63 time=16.1 ms
^C
--- 172.16.0.100 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 701ms
rtt min/avg/max/mdev = 15.826/16.593/19.949/1.361 ms
ricoy_sistemas@tcb-gcp-vm-01:~$
```

Teste de conectividade via Connectivity Test da GCP

Connectivity test result



Test name: tcb-aws-test

Protocol: tcp

Source: tcb-gcp-vm-01 (tcb-gcp-network, 10.88.0.100)

Source project: tcb-gcp-aws-426901

Destination: 172.16.0.100 (tcb-gcp-network)

Destination project: tcb-gcp-aws-426901 (Network) / tcb-gcp-aws-426901 (IP address)

Destination port: 80

Result:

- VM instance (tcb-gcp-vm-01)
- Default egress firewall rule
- Dynamic route
- VPN tunnel (gcp-tunnel2)
- Packet could be forwarded

Desprovisionando os recursos criados com o comando "terraform destroy"

```
[tcb-gcp-aws-426901] +   
lapsed]  
google_compute_network.tcb-gcp-network: Destruction complete after 21s  
aws_internet_gateway.aws-vpc-igw: Still destroying... [id=igw-03b3cffd46440737d, 1m40s elapsed]  
aws_internet_gateway.aws-vpc-igw: Destruction complete after 1m40s  
aws_instance.tcb-aws-vm-01: Still destroying... [id=i-08d99e8f2e136302f, 50s elapsed]  
aws_instance.tcb-aws-vm-01: Destruction complete after 51s  
google_compute_address.gcp-ip: Destroying... [id=projects/tcb-gcp-aws-426901/regions/us-west1/addresses/gcp-vm-ip]  
aws_security_group.aws-allow-icmp: Destroying... [id=sg-031f0ced29dbf079f]  
aws_security_group.aws-allow-internet: Destroying... [id=sg-040adf765c9696515]  
aws_security_group.aws-allow-ssh: Destroying... [id=sg-0a8819cf3a7df8950]  
aws_subnet.tcb-aws-subnet1: Destroying... [id=subnet-014916e7b59fd8b30]  
aws_security_group.aws-allow-vpn: Destroying... [id=sg-018b43264e94dd7bd]  
aws_security_group.aws-allow-vpn: Destruction complete after 0s  
aws_security_group.aws-allow-ssh: Destruction complete after 0s  
aws_subnet.tcb-aws-subnet1: Destruction complete after 0s  
aws_security_group.aws-allow-internet: Destruction complete after 0s  
aws_security_group.aws-allow-icmp: Destruction complete after 0s  
aws_vpc.tcb-aws-vpc: Destroying... [id=vpc-09c2ec308eaa195e1]  
aws_vpc.tcb-aws-vpc: Destruction complete after 1s  
google_compute_address.gcp-ip: Still destroying... [id=projects/tcb-gcp-aws-426901/regions/us-west1/addresses/gcp-vm-ip, 10s elapsed]  
google_compute_address.gcp-ip: Destruction complete after 11s  
  
Destroy complete! Resources: 41 destroyed.  
ricoy_sistemas@cloudshell:~/hands-on-tcb-bmc-gcp/terraform (tcb-gcp-aws-426901)$ █
```