

# 14 - CONFIGURANDO VPC ENDPOINT

- Cria uma ponte entra a VPC e os serviços AWS

- Existe Dois tipos de ENDPOINT :

- INTERFACE ENDPOINT

- GATEWAY ENDPOINT


- vpc>ENDPOINT>CREATE ENDPOINT

## Create Endpoint

A VPC endpoint allows you to securely connect your VPC to another service.  
An interface endpoint is powered by [PrivateLink](#), and uses an elastic network interface (ENI) as an entry point for traffic destined to the service.  
A gateway endpoint serves as a target for a route in your route table for traffic destined for the service.

Service category ☒ AWS services  
☐ Find service by name  
☐ Your AWS Marketplace services

Service Name Select a service ⓘ



Service Name	Owner	Type
<input type="radio"/> aws.sagemaker.us-west-2.notebook	amazon	Interface
<input type="radio"/> com.amazonaws.us-west-2.cloudformation	amazon	Interface
<input type="radio"/> com.amazonaws.us-west-2.cloudtrail	amazon	Interface
<input type="radio"/> com.amazonaws.us-west-2.codebuild	amazon	Interface
<input type="radio"/> com.amazonaws.us-west-2.codebuild-fips	amazon	Interface
<input type="radio"/> com.amazonaws.us-west-2.codecommit	amazon	Interface
<input type="radio"/> com.amazonaws.us-west-2.codecommit-fips	amazon	Interface
<input type="radio"/> com.amazonaws.us-west-2.codepipeline	amazon	Interface
<input type="radio"/> com.amazonaws.us-west-2.config	amazon	Interface
<input type="radio"/> com.amazonaws.us-west-2.dynamodb	amazon	Gateway
<input type="radio"/> com.amazonaws.us-west-2.ec2	amazon	Interface
<input type="radio"/> com.amazonaws.us-west-2.ec2messages	amazon	Interface
<input type="radio"/> com.amazonaws.us-west-2.ecr.api	amazon	Interface
<input type="radio"/> com.amazonaws.us-west-2.ecr.dkr	amazon	Interface

- vAMOS CRIAR ESSE TUNEL ENTRA NOSSA vpc E O SERVIÇO DE AWS PARA O S3


VPC\* vpc-9eb410f5 ⓘ

Configure route tables A rule with destination `ip-4ba540d1 (com.amazonaws.us-west-2.s3)` and a target with this endpoint's ID (e.g. vpc-12345678) will be added to the route tables you select below.

Subnets associated with selected route tables will be able to access this endpoint.

ⓘ

No route tables selected



Route Table ID	Main	Associated With
<input checked="" type="checkbox"/> rtb-7636b00d	Yes	4 subnets

### Warning

When you use an endpoint, the source IP addresses from your instances in your affected subnets for accessing the AWS service in the same region will be private IP addresses, not public IP addresses. Existing connections from your affected subnets to the AWS service that use public IP addresses may be dropped. Ensure that you don't have critical tasks running when you create or modify an endpoint.

Policy\* ⓘ ☒ Full Access - Allow access by any user or service within the VPC using credentials from any AWS accounts to any resources in this AWS service. All policies — IAM user policies, VPC endpoint policies, and AWS service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.

☐ Custom

Use the [policy creation tool](#) to generate a policy, then paste the generated policy below.

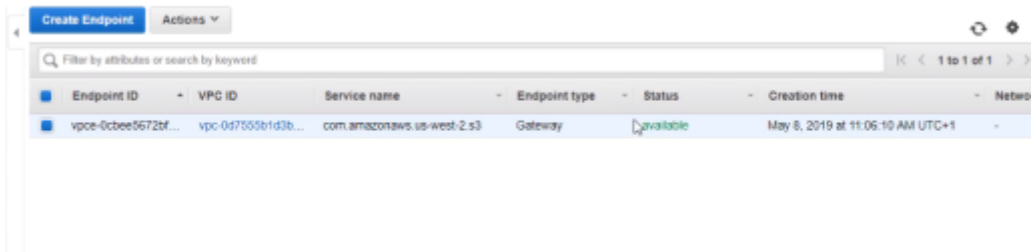
```
{
  "Statement": [
    {

```

- ELE IRÁ PERGUNTAR O VPC E A TABELA DE ROTEAMENTO

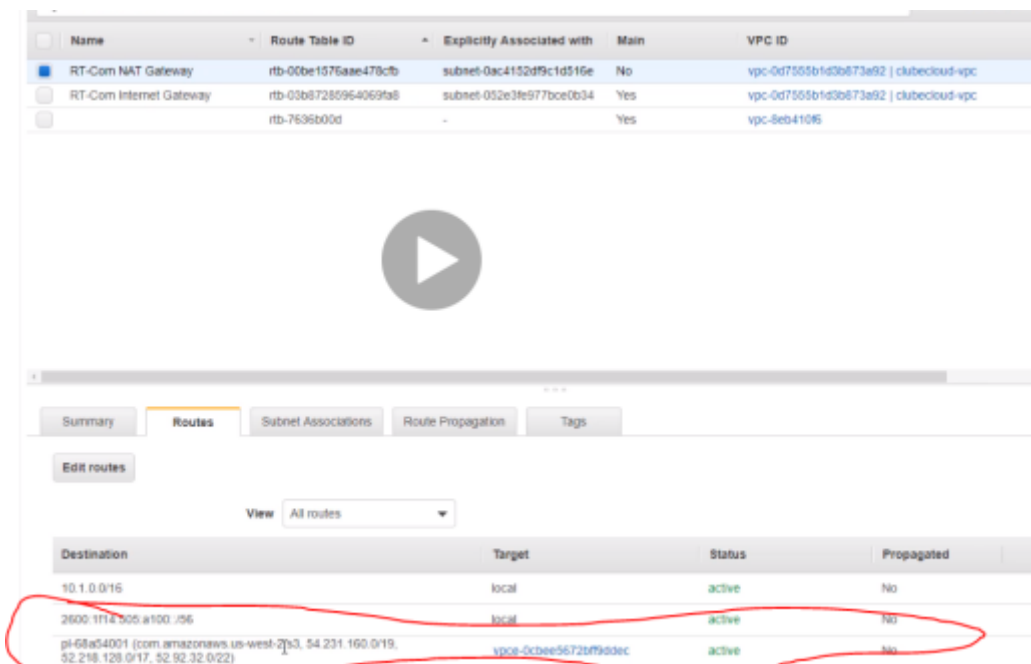
- EM QUAL LUGAR DA TOPOLOGIA IREMOS USAR ESSE TUNNEL, SUBNET B - FINANCE

- PODEMOS DAR FULLACCESS OU ACESSO PARCIAL



Endpoint ID	VPC ID	Service name	Endpoint type	Status	Creation time
vpc-e0cbee5672bf...	vpc-d7555b1d3b...	com.amazonaws.us-west-2.s3	Gateway	available	May 5, 2019 at 11:05:10 AM UTC+1

- O ENDPOINT VAI NA TABELA DE ROTEAMENTO > NAT GATEWAY E CRIA UMA ROTA



Name	Route Table ID	Explicitly Associated with	Main	VPC ID
RT-Com NAT Gateway	rtb-00be1576aee478c9b	subnet-0ac4152d9c1d516e	No	vpc-d7555b1d3b673e92   clubecloud-vpc
RT-Com Internet Gateway	rtb-03b67285964069fa8	subnet-032e3fe977bce0634	Yes	vpc-d7555b1d3b673e92   clubecloud-vpc
	rtb-7636b00d	-	Yes	vpc-8eb41065

Destination	Target	Status	Propagated
10.1.0.0/16	local	active	No
2600:1114:505:a100::/56	local	active	No
pl-68a54001 (com.amazonaws.us-west-2/s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpc-e0cbee5672bf99ddec	active	No

- APONTANDO PARA O ENDPOINT

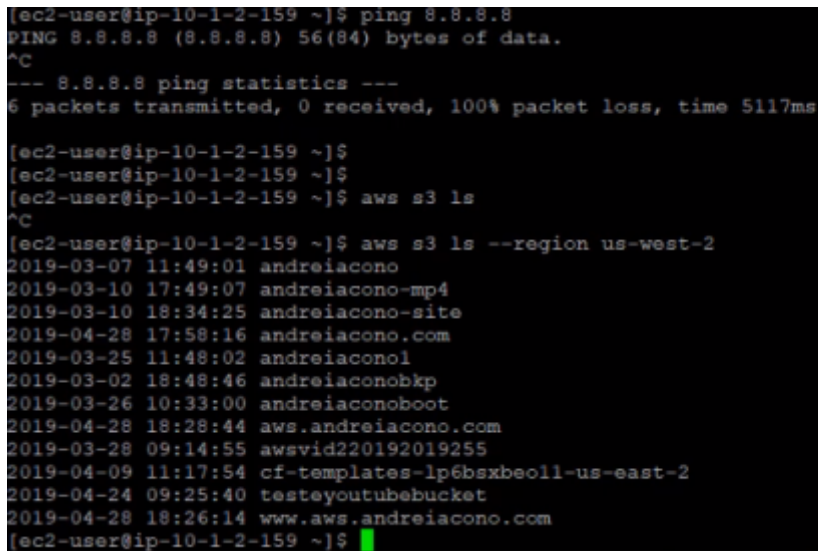
- CONSEQUENTEMENTE DEVEMOS NÃO CONSEGUIR SAIR PARA A INTERNET MAS DEVEMOS CONSEGUIR VISUALIZAR AS BUCKETS .

PARA ISSO NÃO É SOMENTE UTILIZAR O COMANDO

aws s3 ls

e sim

```
aws s3 ls --region us-west-2
```



```
[ec2-user@ip-10-1-2-159 ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5117ms

[ec2-user@ip-10-1-2-159 ~]$
[ec2-user@ip-10-1-2-159 ~]$
[ec2-user@ip-10-1-2-159 ~]$ aws s3 ls
^C
[ec2-user@ip-10-1-2-159 ~]$ aws s3 ls --region us-west-2
2019-03-07 11:49:01 andreiacono
2019-03-10 17:49:07 andreiacono-mp4
2019-03-10 18:34:25 andreiacono-site
2019-04-28 17:58:16 andreiacono.com
2019-03-25 11:48:02 andreiaconol
2019-03-02 18:48:46 andreiaconobkp
2019-03-26 10:33:00 andreiaconoboot
2019-04-28 18:28:44 aws.andreiacono.com
2019-03-28 09:14:55 awsvid220192019255
2019-04-09 11:17:54 cf-templates-lp6bsxbo11-us-east-2
2019-04-24 09:25:40 testyoutubebucket
2019-04-28 18:26:14 www.aws.andreiacono.com
[ec2-user@ip-10-1-2-159 ~]$
```

- Ou seja, tiramos o acesso web dessa maquina so para provar que por dentro da topologia aws conseguimos chegar nos serviços que a propria aws disponibiliza.
- As vezes muitos engenheiros não prestam atenção em qual que é o fluxo em que suas maquinas estão chegando aos serviços aws.
- Pois se a maquina possui acesso a internet e ela esta dentro de um VPC ela precisa tecnicamente ir para a internet para acessar um serviço (nada segura) criando o endpoint estamos fazendo como se fosse uma porta numa caixa com acesso direto aos serviços da aws.
- Para o vpc voltar a ter acesso a internet basta:

Edit routes

Destination	Target	Status	Propagated
10.1.0.0/16	local	active	No
2600:1f14:505:a100::/56	local	active	No
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.216.128.0/17, 52.92.39.0/22)	vpc-e0c0ee5672b0ff9ddec	active	No
0.0.0.0/0	nat-02b07449e229b35ef		No

Add route

\* Required

Cancel

Save routes