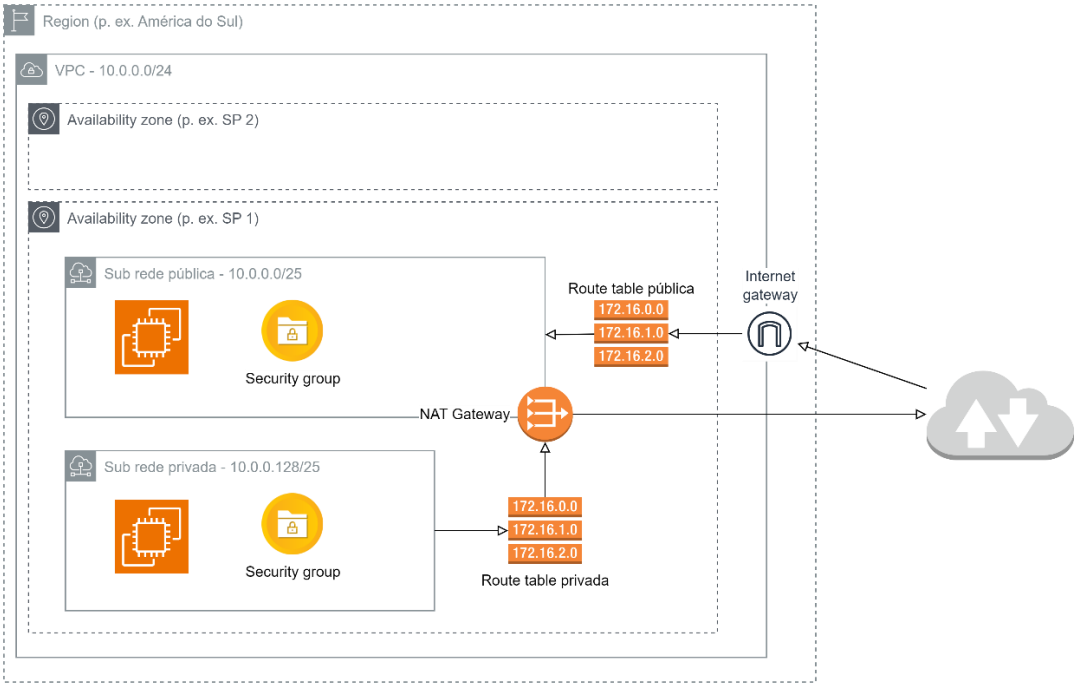
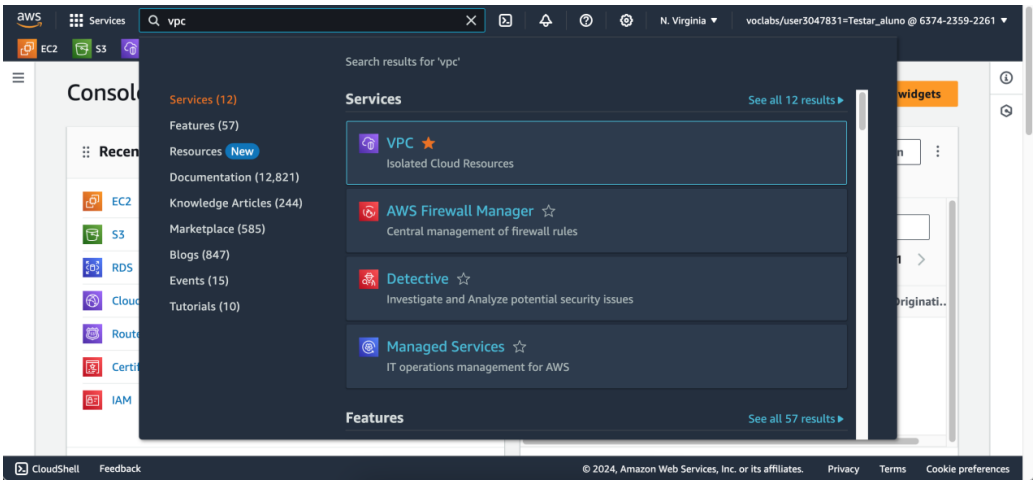
Sumário

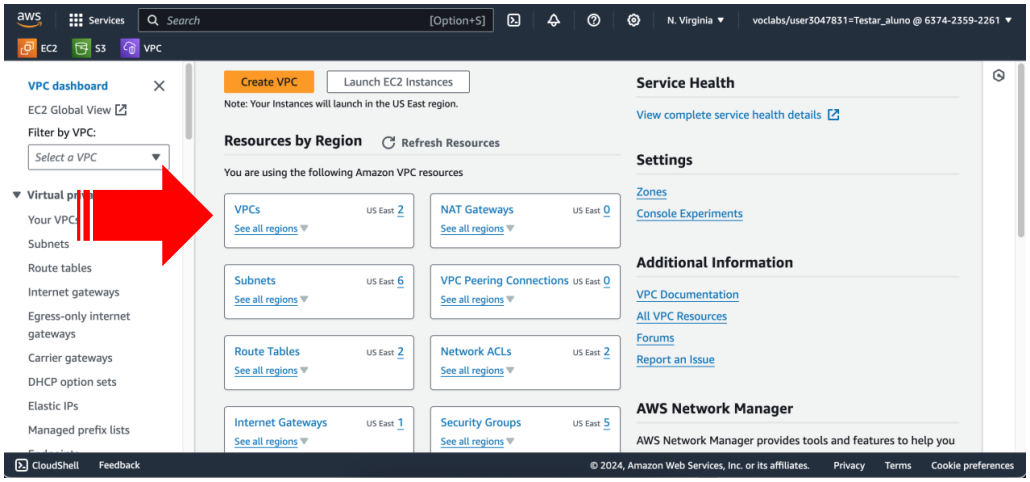
Arquitetura de referência



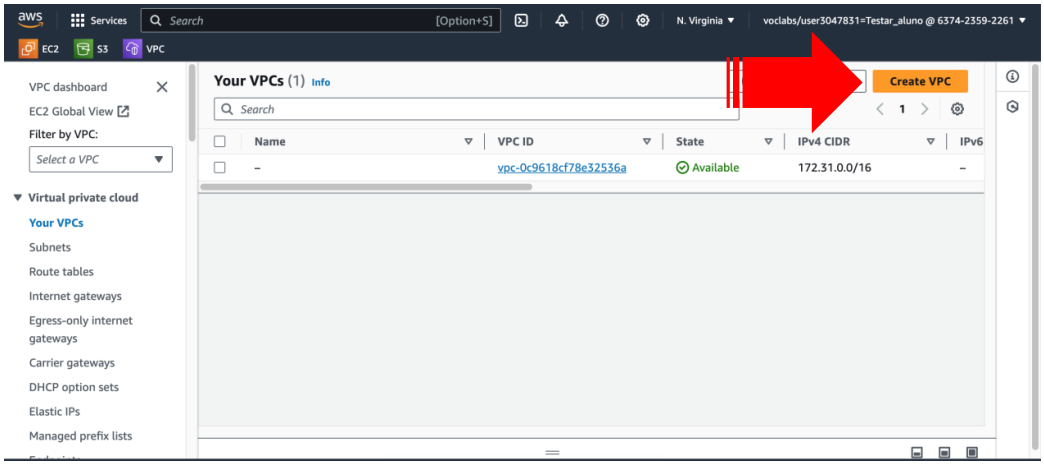
Configurando a VPC

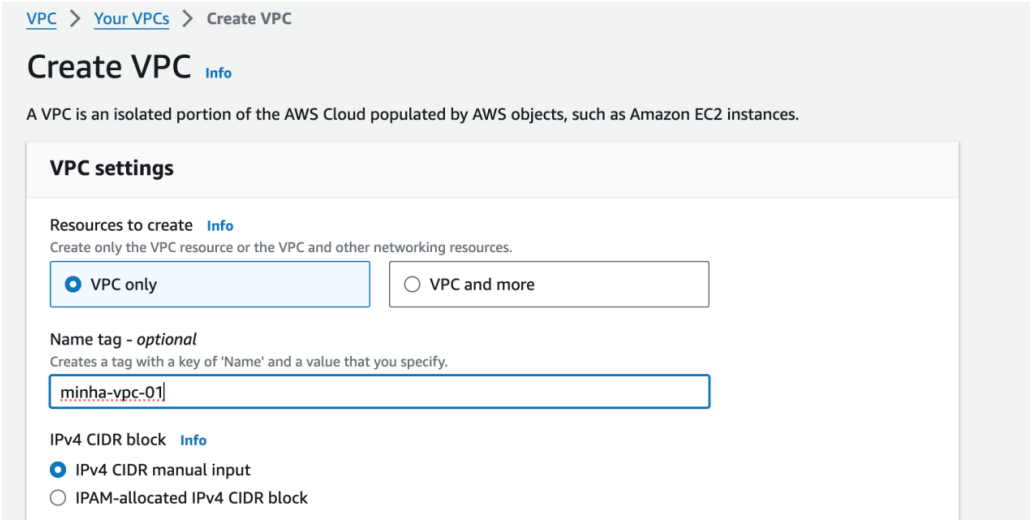
Acesse o console AWS e busque por VPC



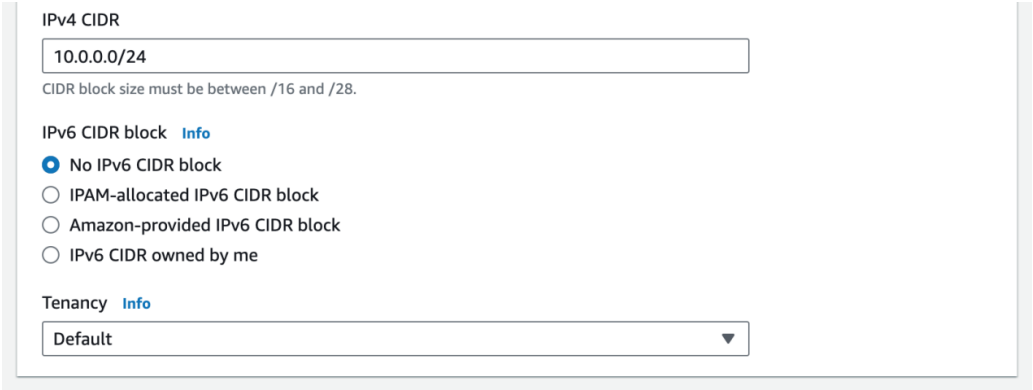


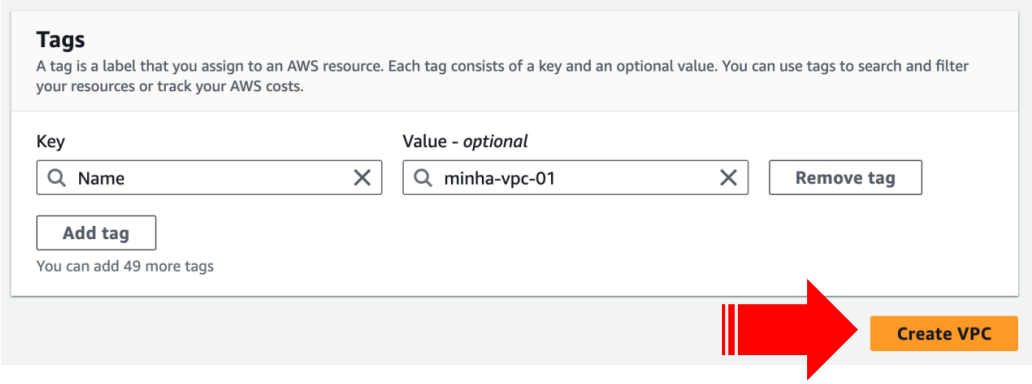
Por padrão, a AWS disponibiliza uma VPC por região, mas iremos criar uma VPC.

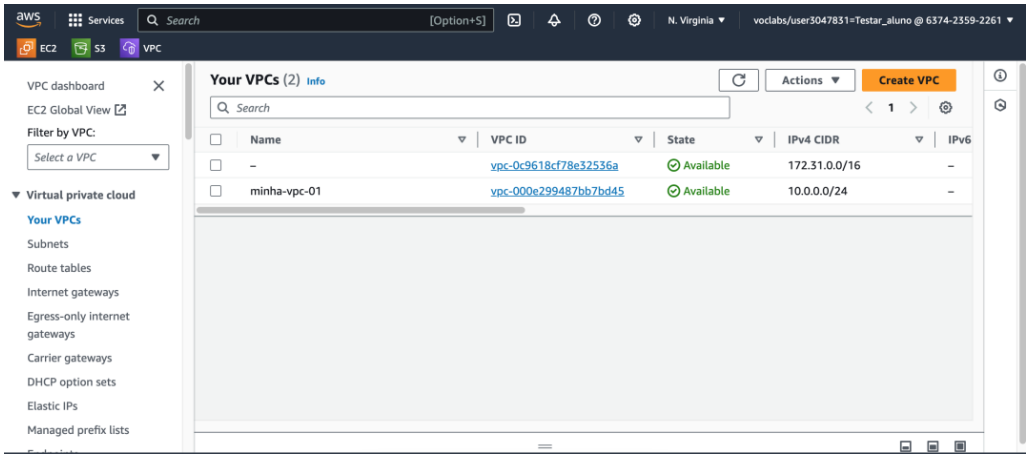




Utilizaremos um endereçamento padrão de classe A, com uma máscara de sub rede /24 o que nos permite criar 128 IPs. Note que a AWS limita entre uma faixa de /16 e /28







Agora, criaremos algumas sub redes para associar à essa VPC. Lembrando que para a divisão dos IPs podemos usar uma calculadora de sub redes

Visual Subnet Calculator

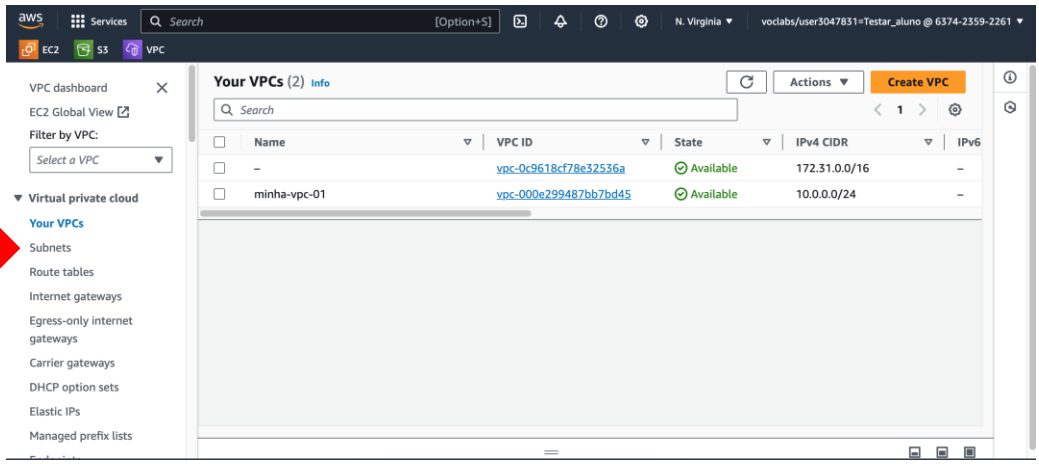
Enter the network you wish to subnet:

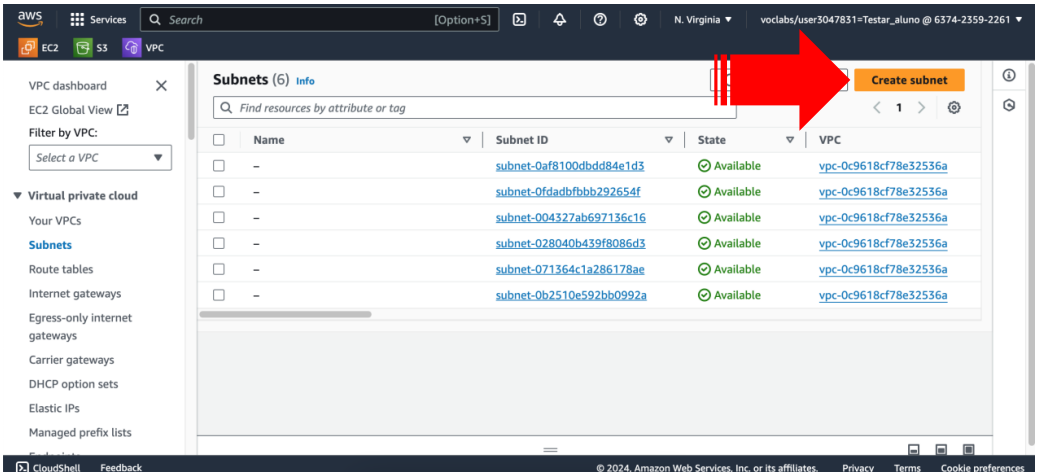
Network Address: 10.0.0.0 / Mask bits: 24 — Update — Reset

Show columns: Subnet address, Netmask, Range of addresses, Useable IPs, Hosts, Divide, Join

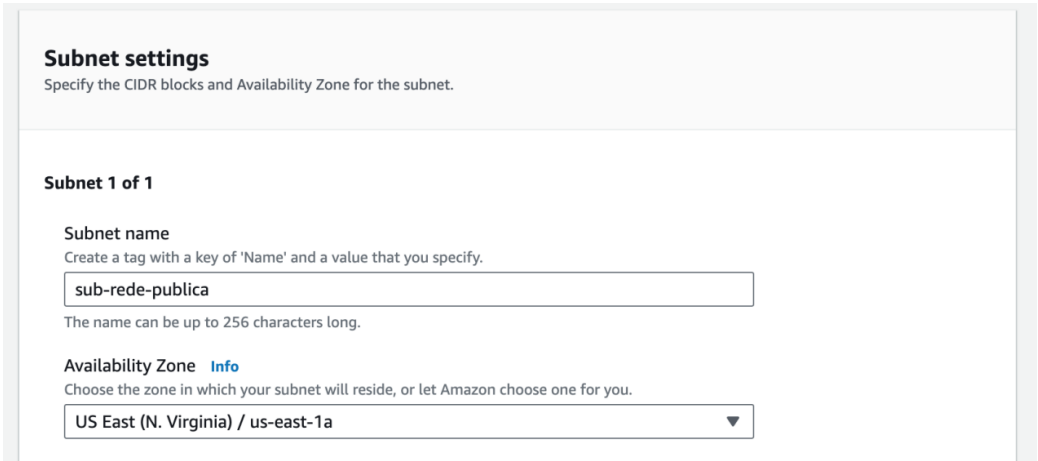
Click below to split and join subnets.
If you wish to save this subnetting for later, bookmark this hyperlink.

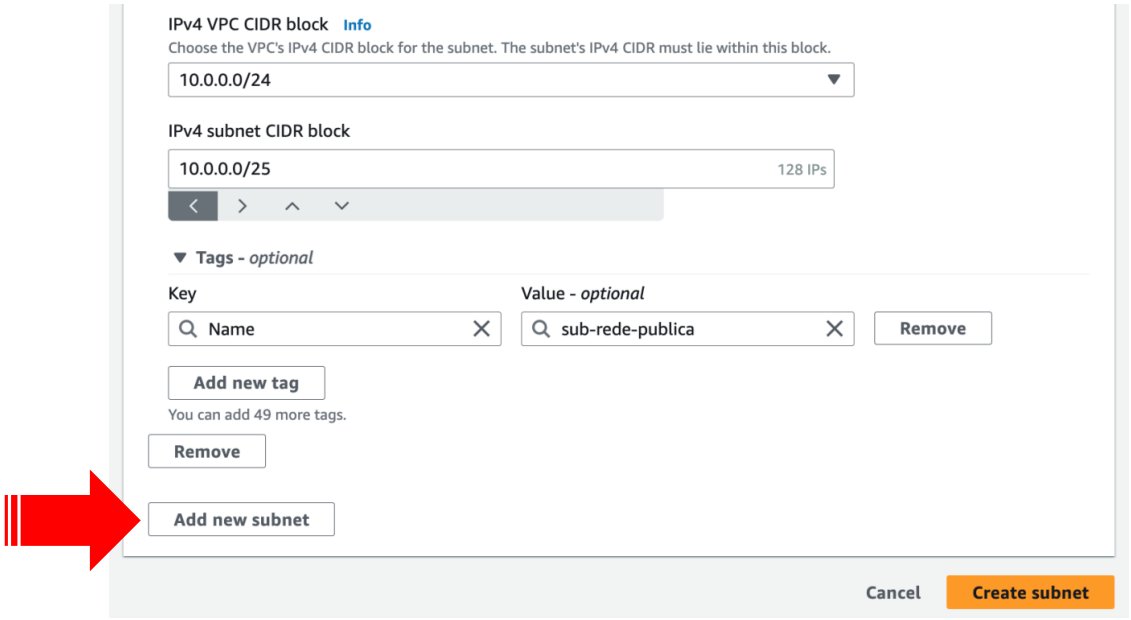
Subnet address	Range of addresses	Useable IPs	Hosts	Divide	Join
10.0.0.0/25	10.0.0.0 - 10.0.0.127	10.0.0.1 - 10.0.0.126	126	Divide	/25 /24
10.0.0.128/25	10.0.0.128 - 10.0.0.255	10.0.0.129 - 10.0.0.254	126	Divide	/25

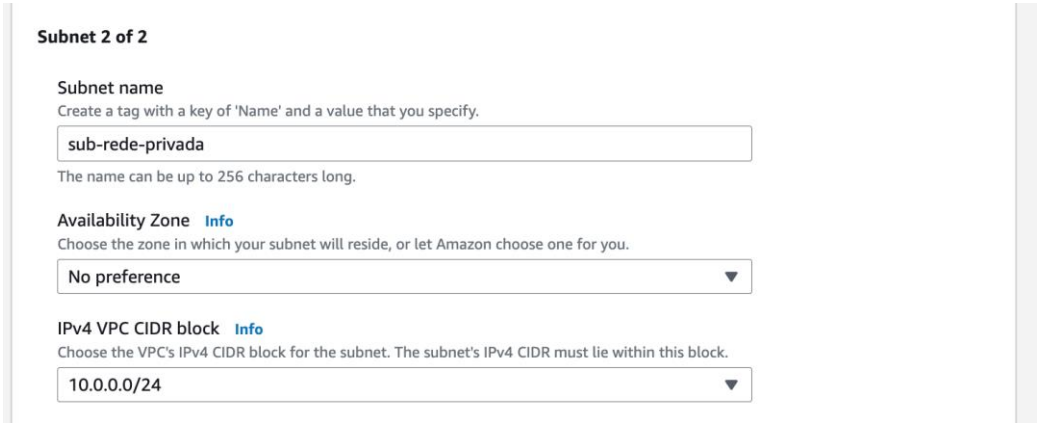


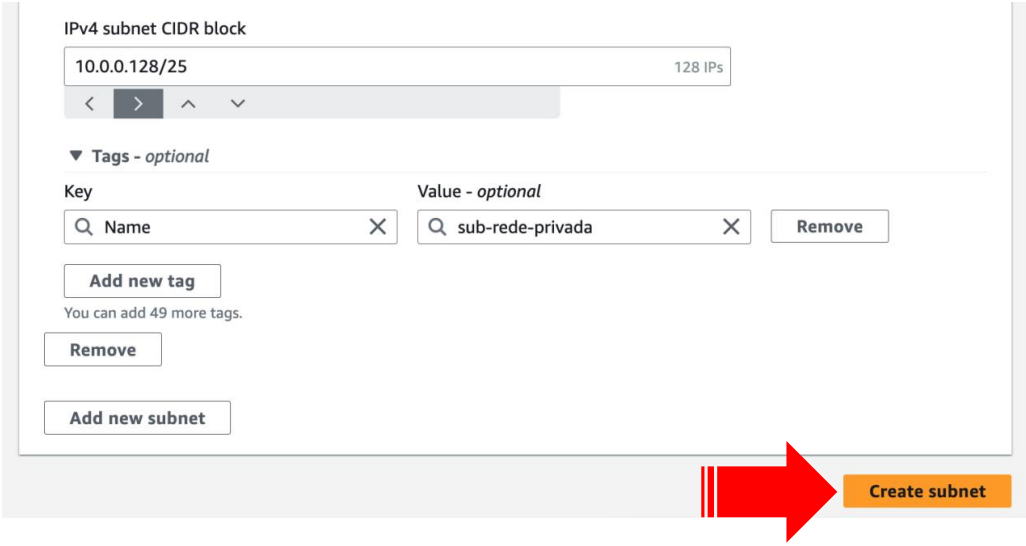

Services
Search
[Option+S]
N. Virginia
EC2
S3
VPC
VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Subnets (6) Info
Find resources by attribute or tag
Create subnet
Name
Subnet ID
State
VPC
subnet-0af8100dbdd84e1d3
subnet-0fdadbfbbb292654f
subnet-004327ab697136c16
subnet-028040b439f8086d3
subnet-071364c1a286178ae
subnet-0b2510e592bb0992a
Available
vpc-0c9618cf78e32536a
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

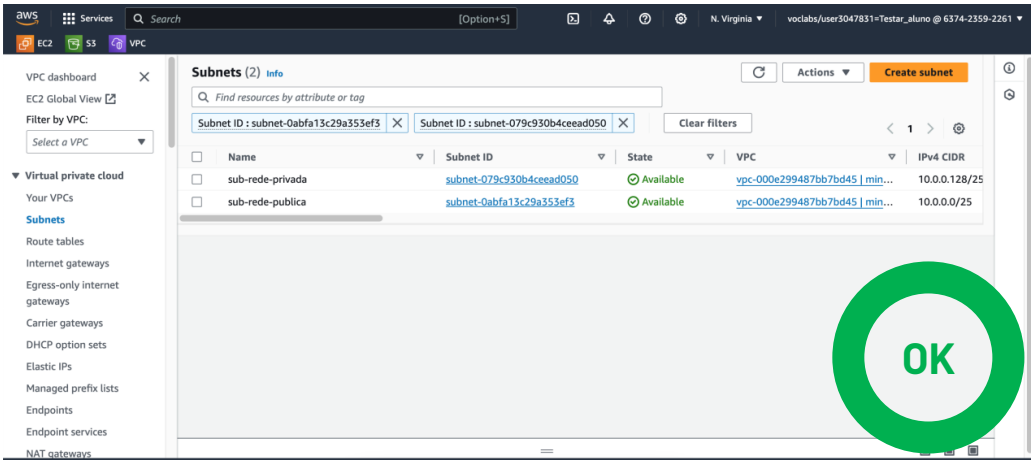

VPC > Subnets > Create subnet
Create subnet Info
VPC
VPC ID
Create subnets in this VPC.
vpc-000e299487bb7bd45 (minha-vpc-01)
Associated VPC CIDRs
IPv4 CIDRs
10.0.0.0/24


Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.
Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
sub-rede-publica
The name can be up to 256 characters long.
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1a


IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/24
IPv4 subnet CIDR block
10.0.0.0/25
128 IPs
Tags - optional
Key
Value - optional
Name
sub-rede-publica
Remove
Add new tag
You can add 49 more tags.
Remove
Add new subnet
Cancel
Create subnet

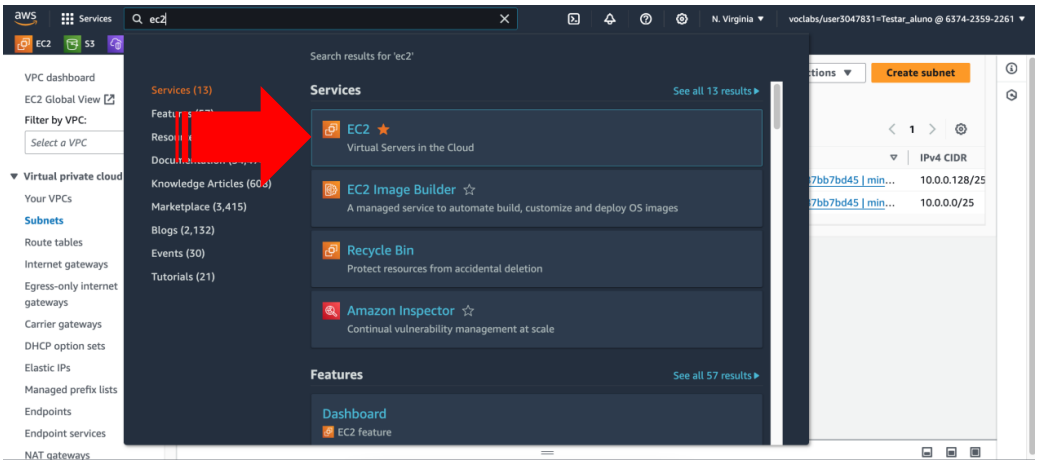

Subnet 2 of 2
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
sub-rede-privada
The name can be up to 256 characters long.
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/24

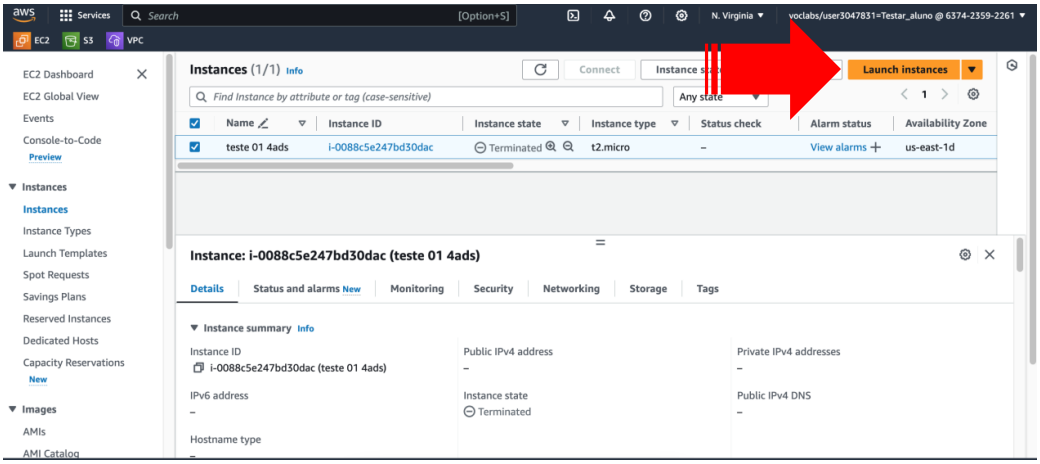

IPv4 subnet CIDR block
10.0.0.128/25
128 IPs
Tags - optional
Key
Value - optional
Name
sub-rede-privada
Remove
Add new tag
You can add 49 more tags.
Remove
Add new subnet
Create subnet



Provisionamento instância em sub redes

Agora temos duas sub redes, uma privada e uma pública. Podemos então provisionar duas instâncias, uma em cada sub rede para que possamos realizar os testes de acesso





EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

ec2-pública

Add additional tags

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux | macOS | Ubuntu | Windows | Red Hat | SUSE Li

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type — Free tier eligible

ami-0c7217cdde317cfec (64-bit (x86)) / ami-05d47d29a4c2d19e1 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-12-07

Architecture: 64-bit (x86)

AMI ID: ami-0c7217cdde317cfec — Verified provider

Instance type Info | Get advice

Instance type

t2.micro — Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true

On-Demand Windows base pricing: 0.0162 USD per Hour

On-Demand SUSE base pricing: 0.0116 USD per Hour

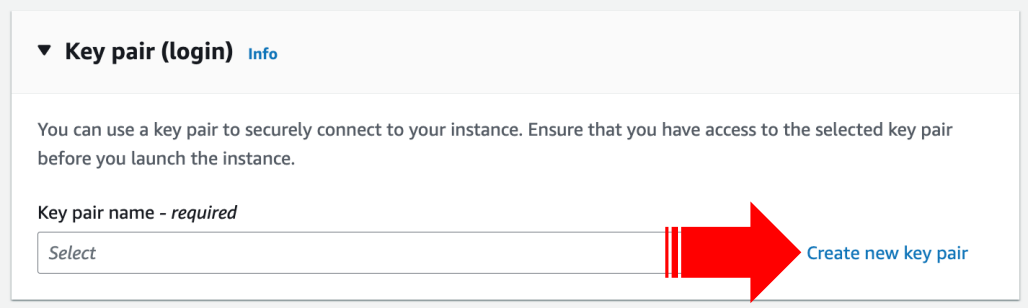
On-Demand RHEL base pricing: 0.0716 USD per Hour

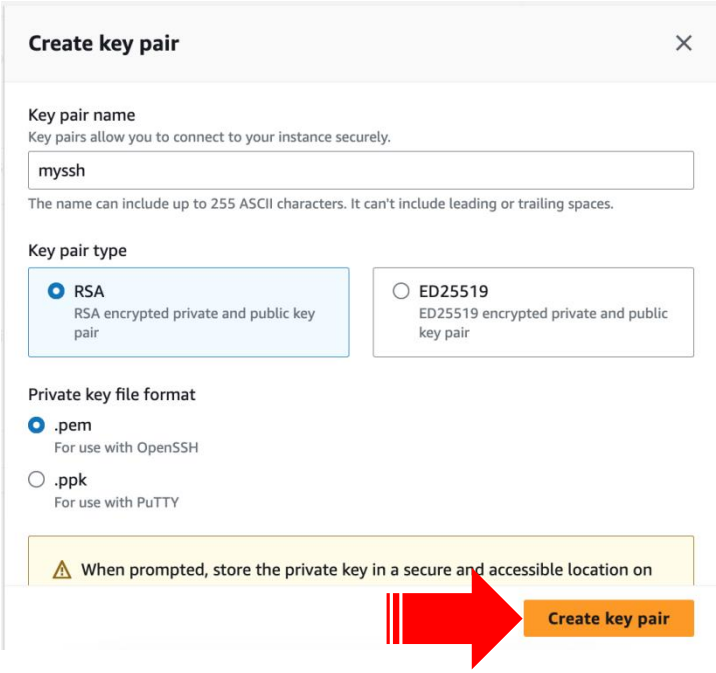
On-Demand Linux base pricing: 0.0116 USD per Hour

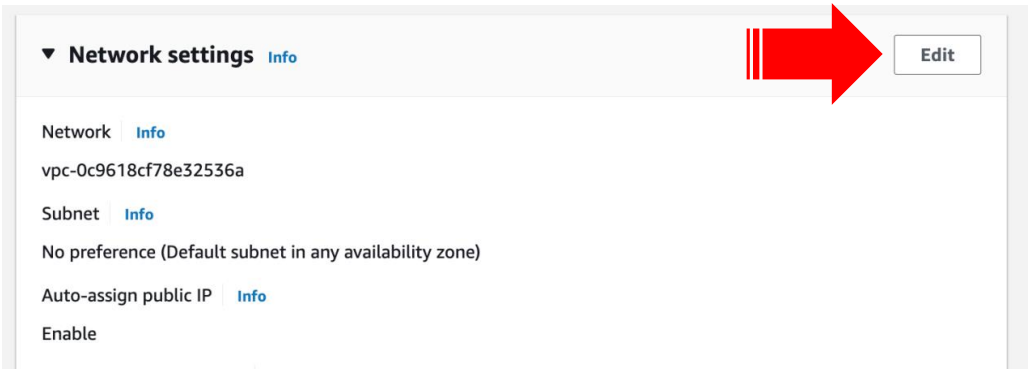
All generations

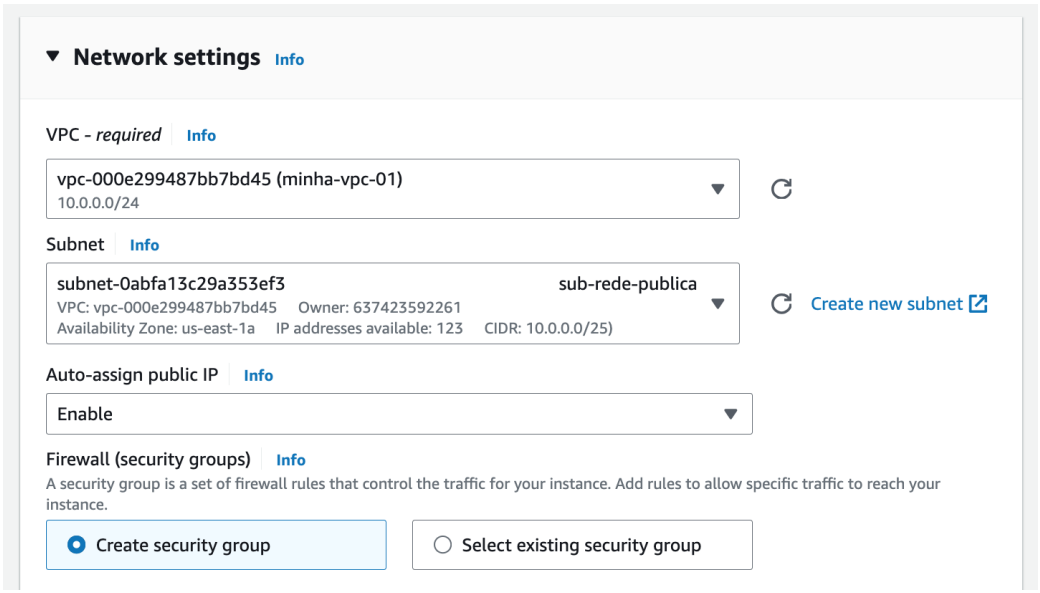
Compare instance types

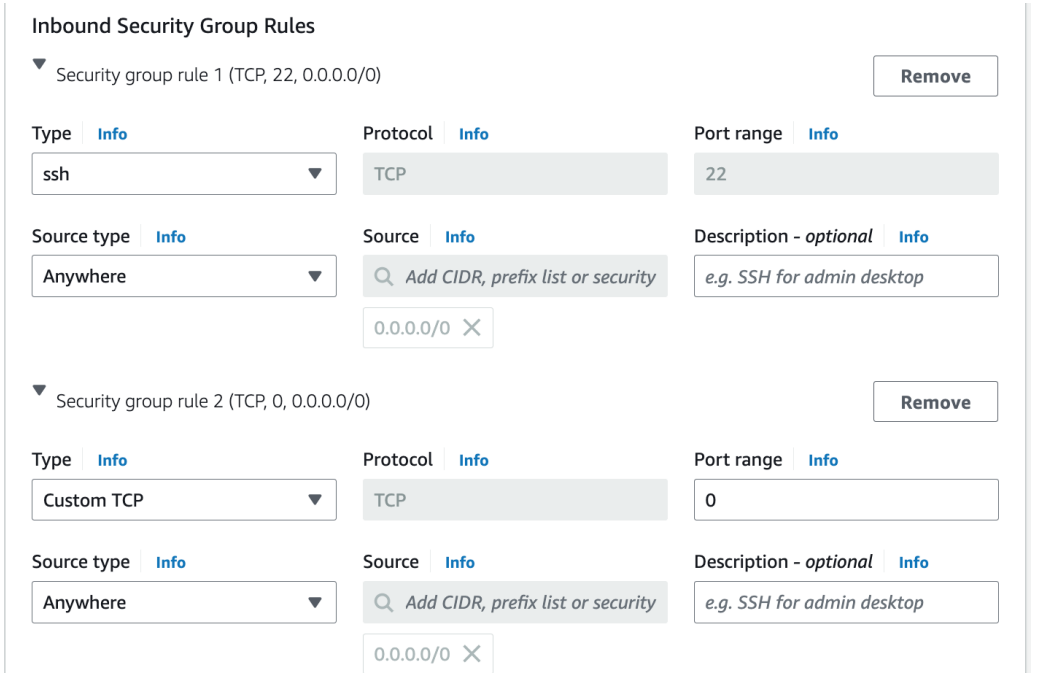
Additional costs apply for AMIs with pre-installed software

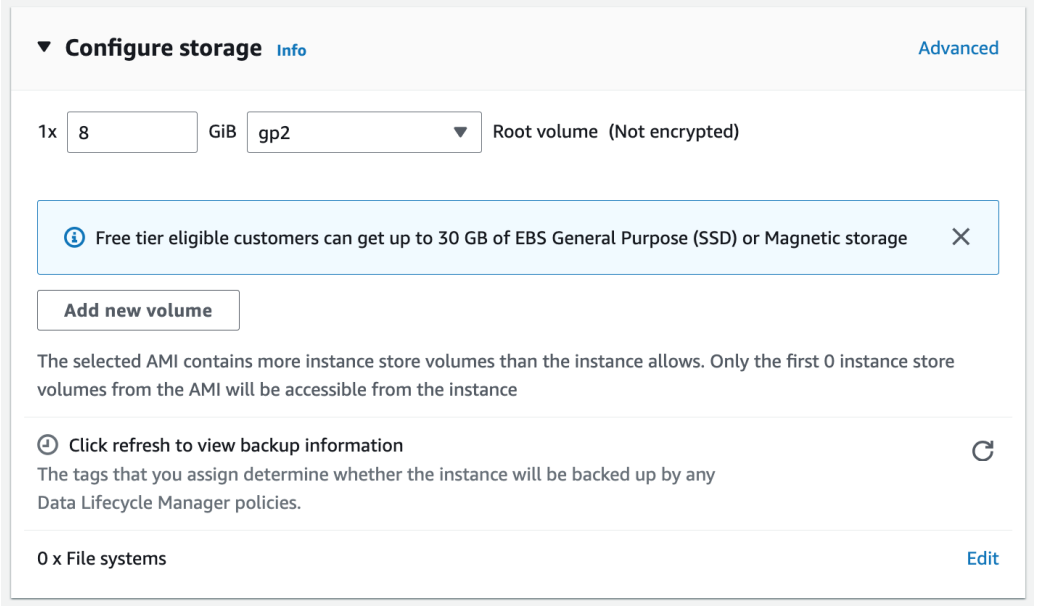

Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
Select
Create new key pair

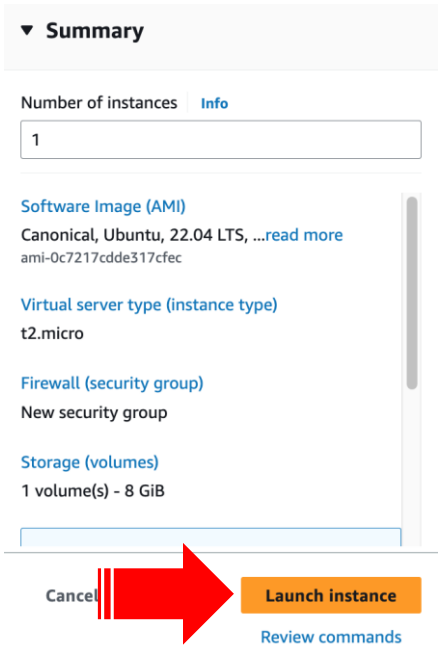

Create key pair
Key pair name
Key pairs allow you to connect to your instance securely.
mykey
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.
Key pair type
RSA
RSA encrypted private and public key pair
ED25519
ED25519 encrypted private and public key pair
Private key file format
.pem
For use with OpenSSH
.ppk
For use with PuTTY
When prompted, store the private key in a secure and accessible location on
Create key pair


Network settings Info
Edit
Network Info
vpc-0c9618cf78e32536a
Subnet Info
No preference (Default subnet in any availability zone)
Auto-assign public IP Info
Enable

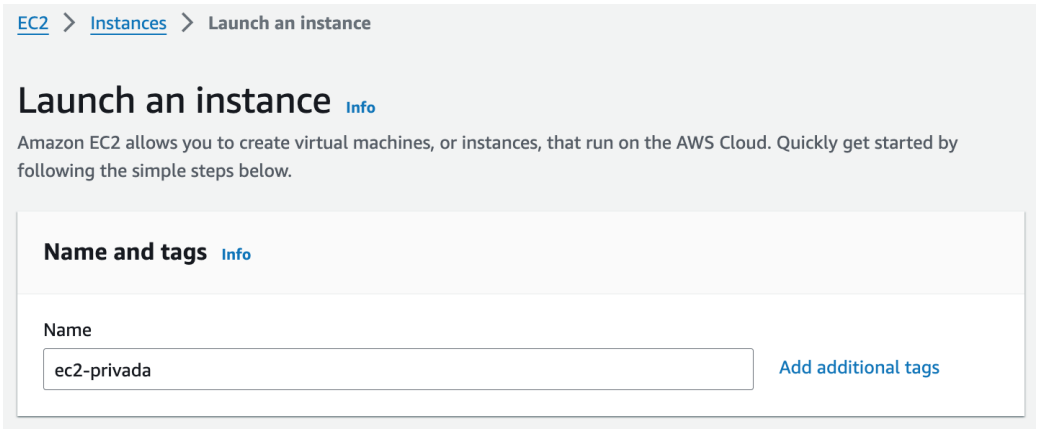

Network settings Info
VPC - required Info
vpc-000e299487bb7bd45 (minha-vpc-01)
10.0.0.0/24
Subnet Info
subnet-0abfa13c29a353ef3 sub-rede-publica
VPC: vpc-000e299487bb7bd45 Owner: 637423592261
Availability Zone: us-east-1a IP addresses available: 123 CIDR: 10.0.0.0/25)
Create new subnet
Auto-assign public IP Info
Enable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group

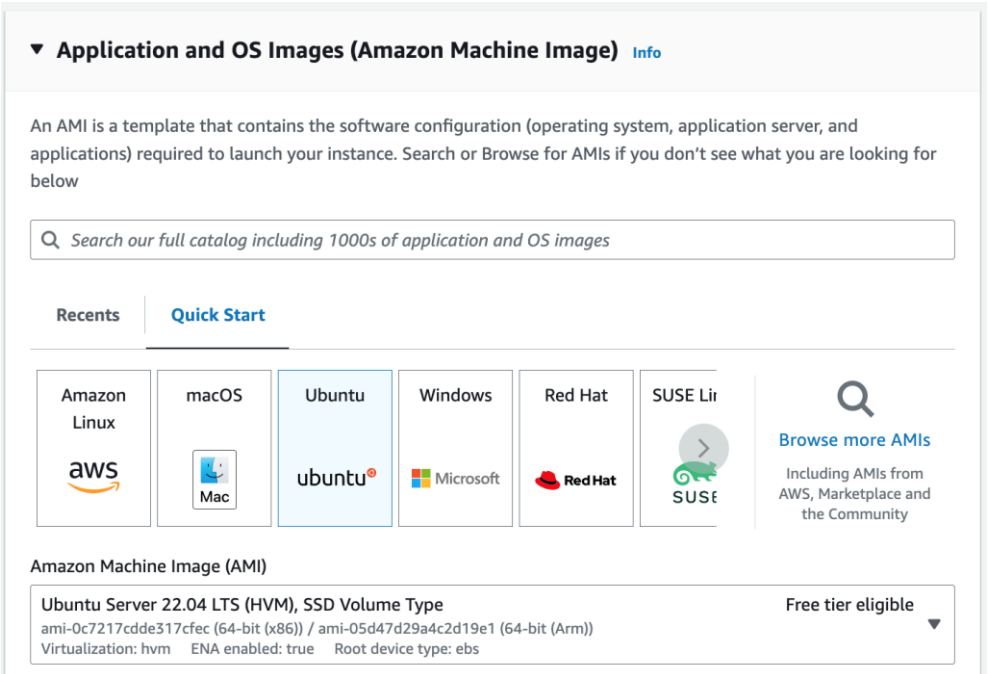

Inbound Security Group Rules
Security group rule 1 (TCP, 22, 0.0.0.0/0)
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or security
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop
Security group rule 2 (TCP, 0, 0.0.0.0/0)
Remove
Type Info
Custom TCP
Protocol Info
TCP
Port range Info
0
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or security
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop


Configure storage Info
Advanced
1x 8 GiB gp2 Root volume (Not encrypted)
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage
Add new volume
The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance
Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.
0 x File systems
Edit



Provisionamos a instância que estará na sub rede pública, agora provisionaremos a máquina que ficará em uma sub rede privada





Description

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-12-07

Architecture

64-bit (x86)

AMI ID

ami-0c7217cdde317cfec

Verified provider

Instance type Info | Get advice

Instance type

t2.micro — Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.0716 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

myssh

Create new key pair

Network settings Info

VPC - *required* Info

vpc-000e299487bb7bd45 (minha-vpc-01)
10.0.0.0/24

Subnet Info

subnet-079c930b4ceead050 — sub-rede-privada
VPC: vpc-000e299487bb7bd45 Owner: 637423592261
Availability Zone: us-east-1a IP addresses available: 123 CIDR: 10.0.0.128/25)

Create new subnet

Auto-assign public IP Info

Disable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

Common security groups Info

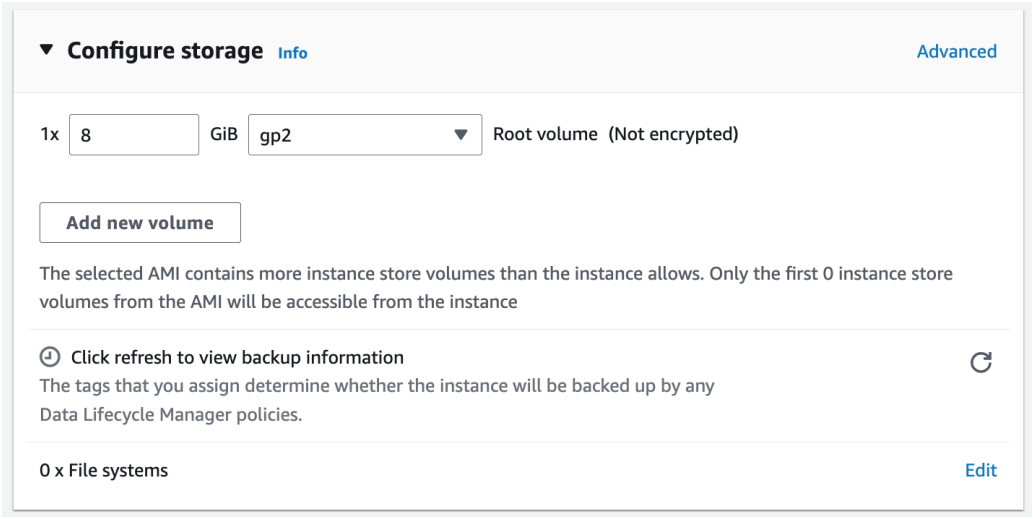
Select security groups

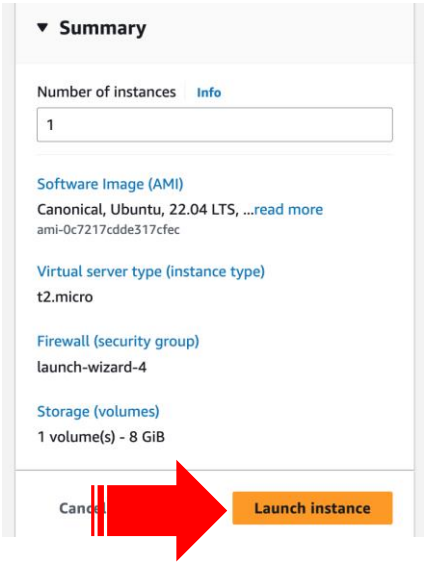
launch-wizard-4 sg-096bec2517d868b00
VPC: vpc-000e299487bb7bd45

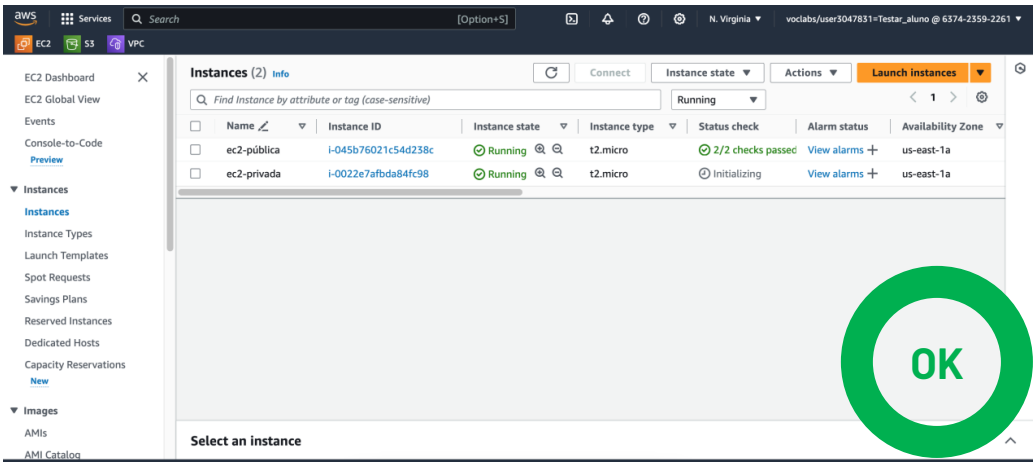
Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

Advanced network configuration

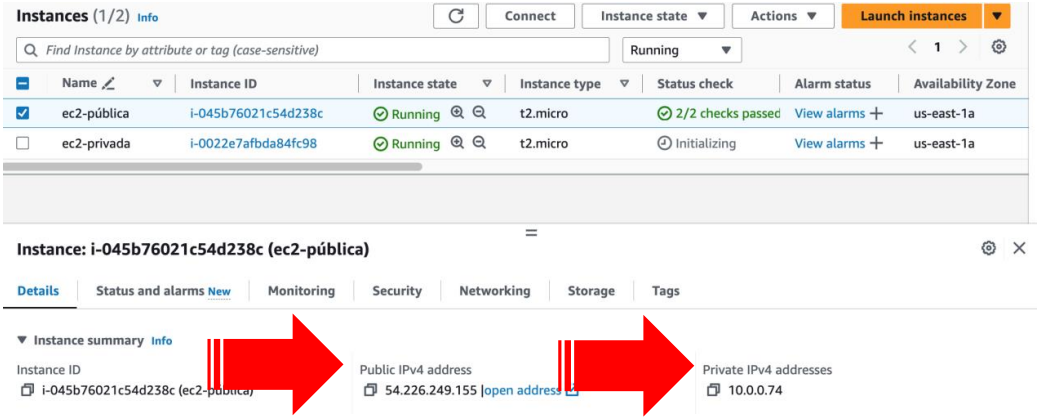




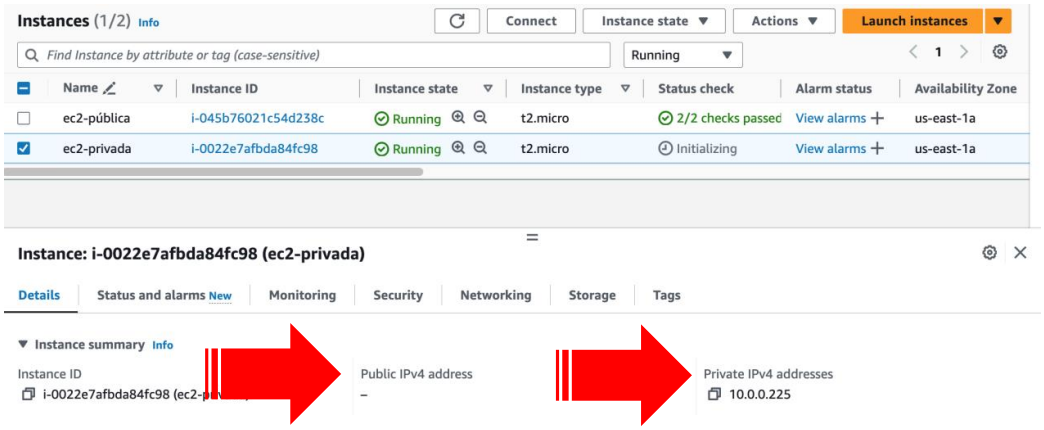


Vamos observar os IPv4 de cada uma das máquinas

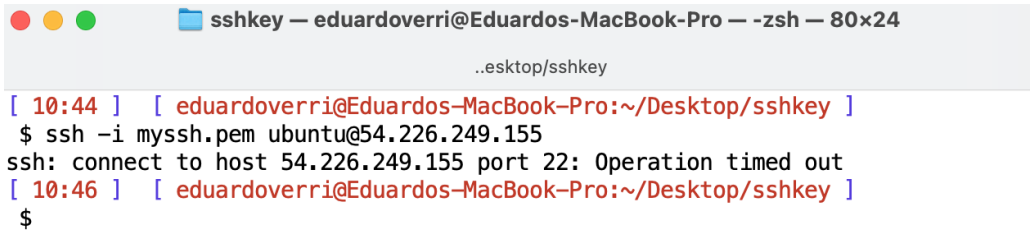
Para a EC2 pública



Para a EC2 privada



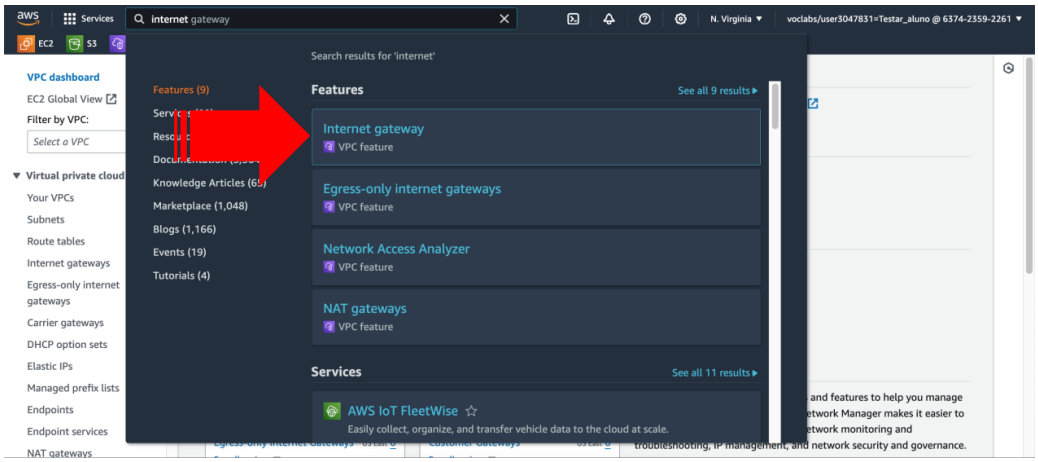
Como habilitamos um IP de saída, a EC2 pública poderá ter um acesso à internet, vamos testá-lo com a conexão SSH

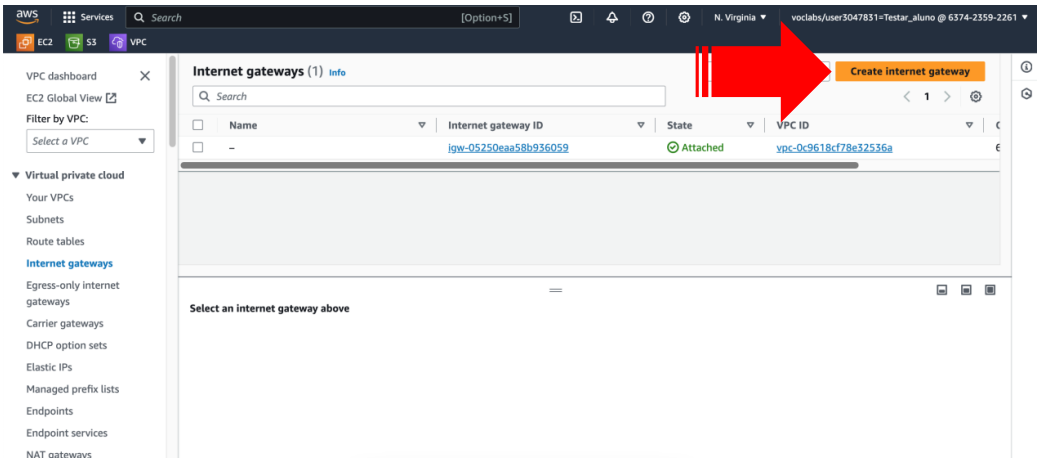


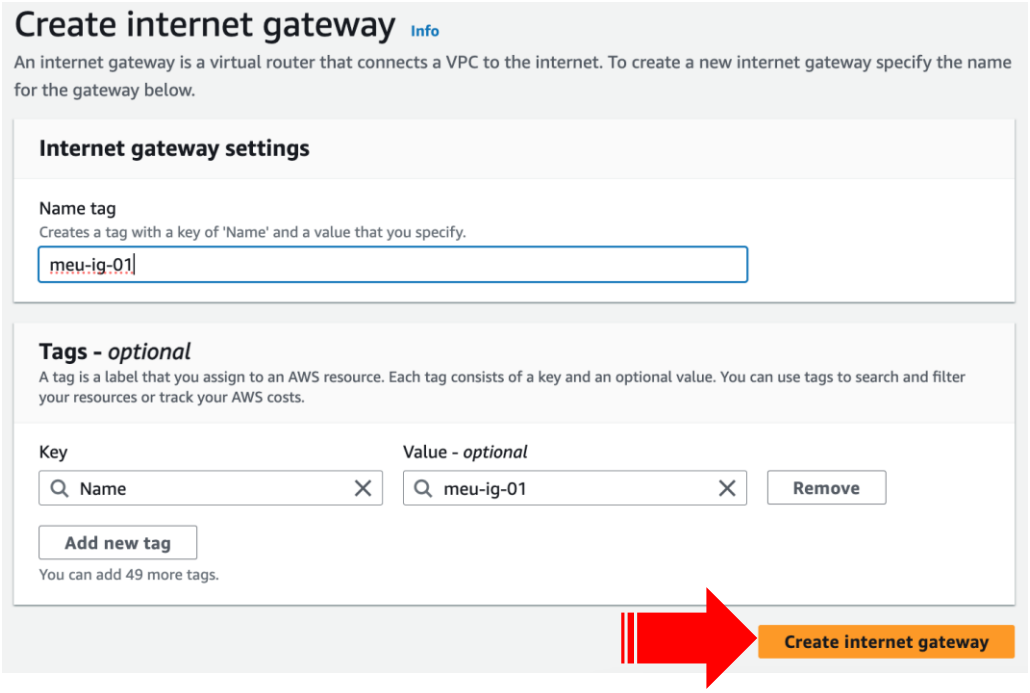
Ele não cria acesso à EC2! Por que isso?

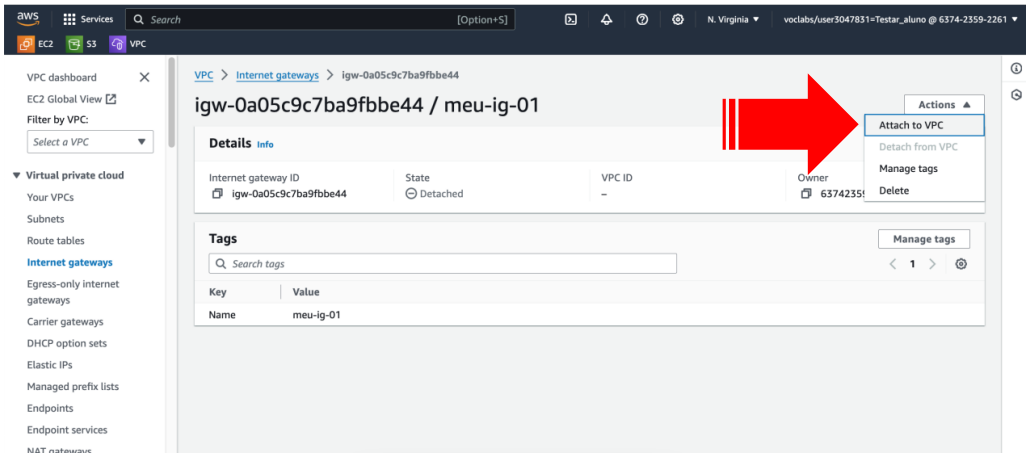
Porque, apesar desta máquina ter um IP público, a minha sub rede não tem acesso à internet, ela não está exposta à internet. Para isso precisaremos configurar um elemento de rede que expõem a rede, que é o internet gateway!

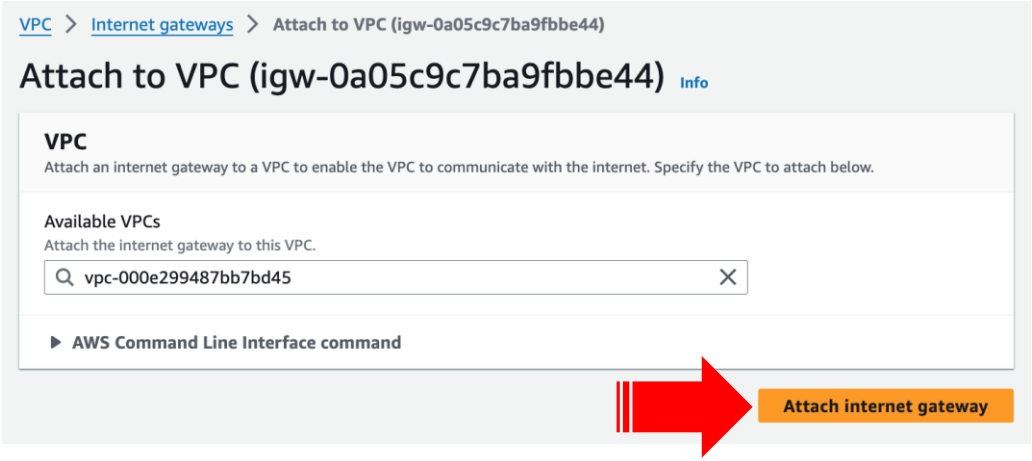
Configurando Internet Gateway e Route Table

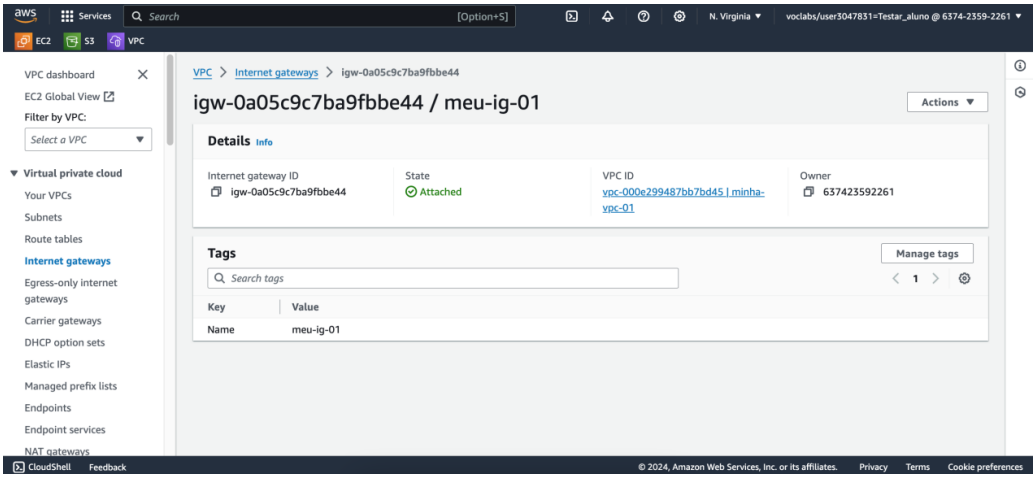






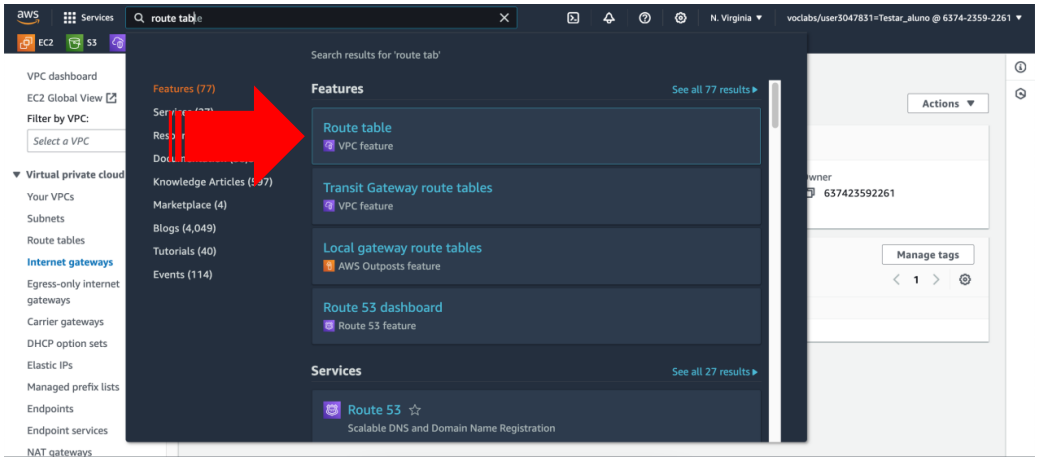


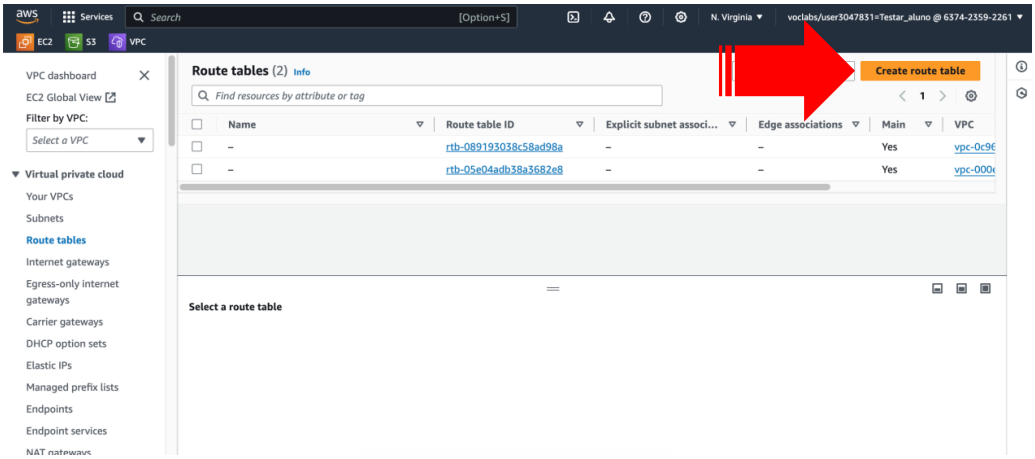


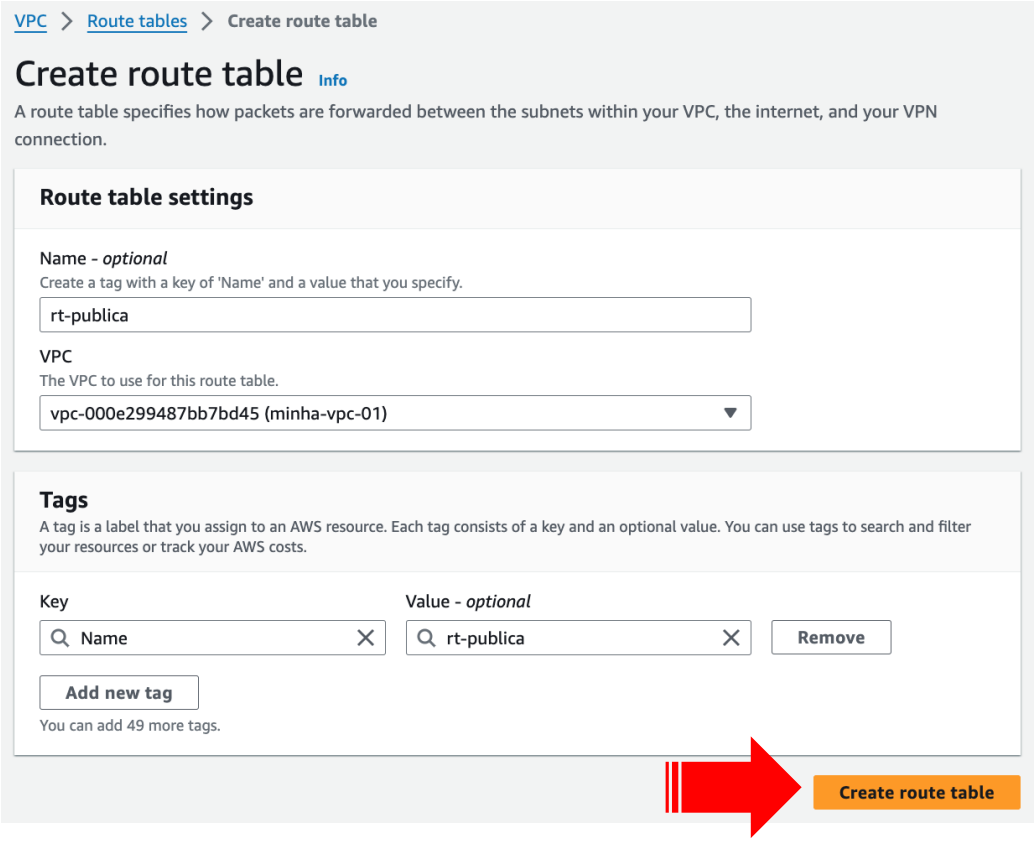


Vamos testar novamente. Continua não indo!

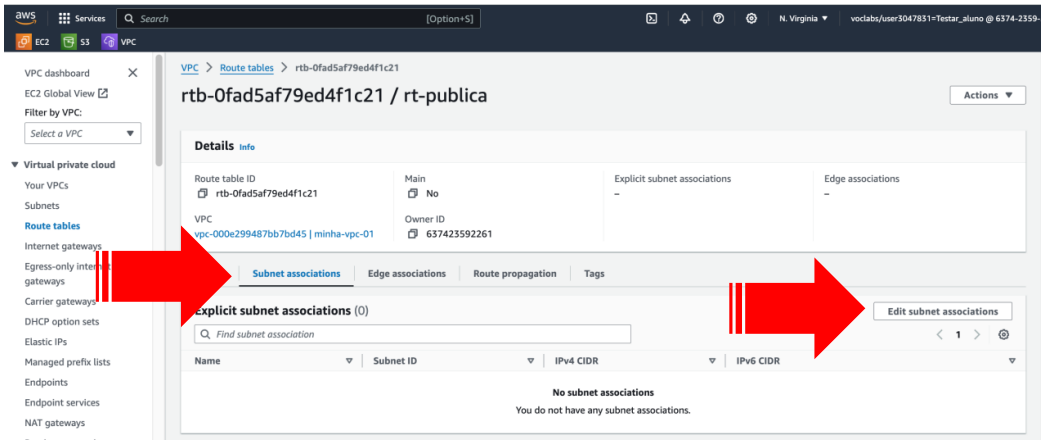
Falta eu "ensinar" a rota da minha sub rede para o internet gateway, fazemos isso com uma tabela de rota (route table).

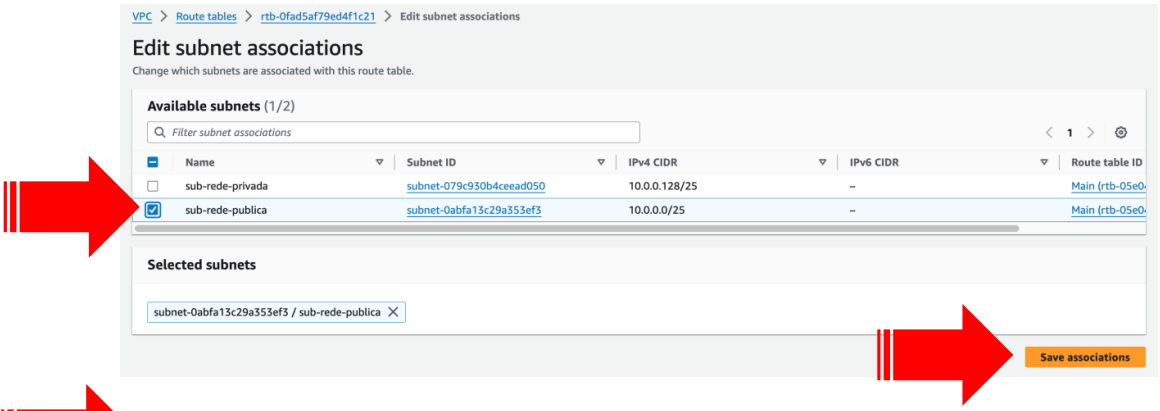


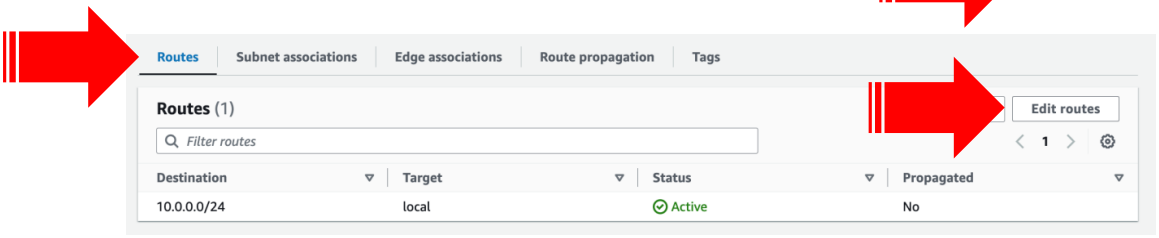


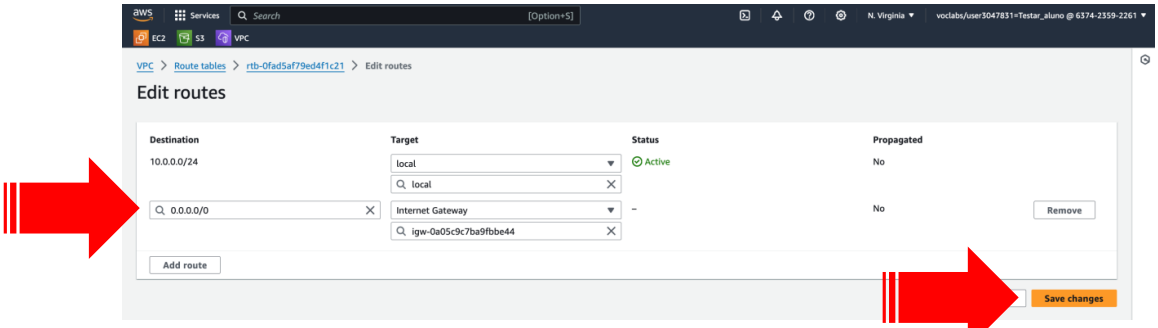


Como essa tabela de rota vai apontar para a internet eu vou associá-la à minha rede pública









Pronto, agora minha tabela de rotas determinou que qualquer IP fora do range de 10.0.0.0/24 será resolvido na Internet! Vamos testar, e vemos que agora temos acesso SSH à máquina!!

```
[ 11:06 ]  [ eduardoverri@Eduardos-MacBook-Pro:~/Desktop/sshkey ]
 $ ssh -i myssh.pem ubuntu@54.226.249.155
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1017-aws x86_64)

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

  System information as of Sun Feb 25 14:06:16 UTC 2024

  System load:  0.0               Processes:             96
  Usage of /:   20.5% of 7.57GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for eth0: 10.0.0.74
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


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.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-0-74:~$
```

Mas este acesso é a máquina pública, como podemos acessar a máquina privada? Iremos fazer uma cópia de segurança com o comando **scp**

```
scp -i chave_pem <arquivo_origem> <local_destino>
```

```
sshkey — eduardoverri@Eduardos-MacBook-Pro — -zsh — 67×27
...untu@54.226.249.155   ..esktop/sshkey   ..esktop/sshkey
[ 11:51 ]  [ eduardoverri@Eduardos-MacBook-Pro:~/Desktop/sshkey ]
 $ scp -i ./myssh.pem /Users/eduardoverri/Desktop/sshkey/myssh.pem
ubuntu@54.226.249.155:/home/ubuntu/.ssh/myssh.pem
myssh.pem                                     100% 1674    11.7KB/s   00:00
[ 11:51 ]  [ eduardoverri@Eduardos-MacBook-Pro:~/Desktop/sshkey ]
 $
```

Acessando a EC2 na rede pública (*tag*: ec2-pública)

```
sshkey — ubuntu@ip-10-0-0-74: ~/.ssh — ssh -i myssh.pem ubuntu@54...
...untu@54.226.249.155   ..esktop/sshkey   ..esktop/sshkey
ubuntu@ip-10-0-0-74:~/.ssh$ ll
total 16
drwx------ 2 ubuntu ubuntu 4096 Feb 25 14:51 ./
drwxr-x--- 5 ubuntu ubuntu 4096 Feb 25 14:40 ../
-rw------- 1 ubuntu ubuntu  387 Feb 25 13:31 authorized_keys
-r-------- 1 ubuntu ubuntu 1674 Feb 25 14:51 myssh.pem
ubuntu@ip-10-0-0-74:~/.ssh$
```

Se quisermos conectar na instância privada, podemos através da pública com ssh! Conceito de jump server ou bastião (bastion host)

```
sshkey — ubuntu@ip-10-0-0-225: ~ —
...@ip-10-0-0-225: ~ — ssh -i myssh.pem ubuntu@54.226.249.155
ubuntu@ip-10-0-0-74:~/.ssh$ ssh -i myssh.pem ubuntu@10.0.0.225
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1017-aws x86_64)

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

  System information as of Sun Feb 25 14:58:17 UTC 2024

  System load:  0.0               Processes:             94
  Usage of /:   20.5% of 7.57GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for eth0: 10.0.0.225
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Sun Feb 25 14:58:18 2024 from 10.0.0.74
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-0-225:~$
```

Mas temos um problema, bloqueamos o acesso à essa VM de fora da rede, mas e para atualizar os pacotes de nossa instância? E criarmos um CI/CD? Precisaremos acessar a internet, de dentro, mas não permitir que de fora seja acessada. Nesses casos precisaremos de um NAT Gateway, que permite a saída para a Internet, mas bloqueia a entrada da Internet.

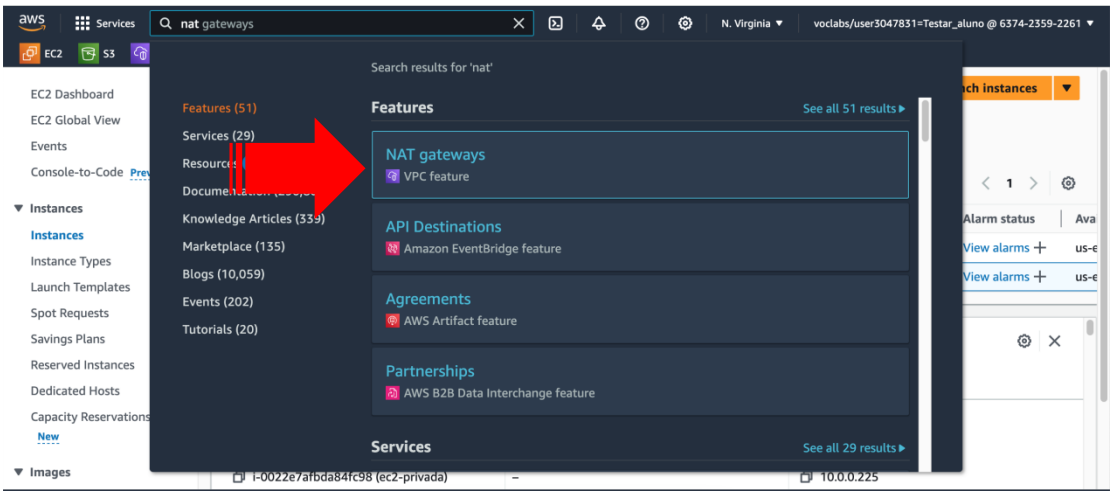
Ao tentar acessar de fora não temos acesso

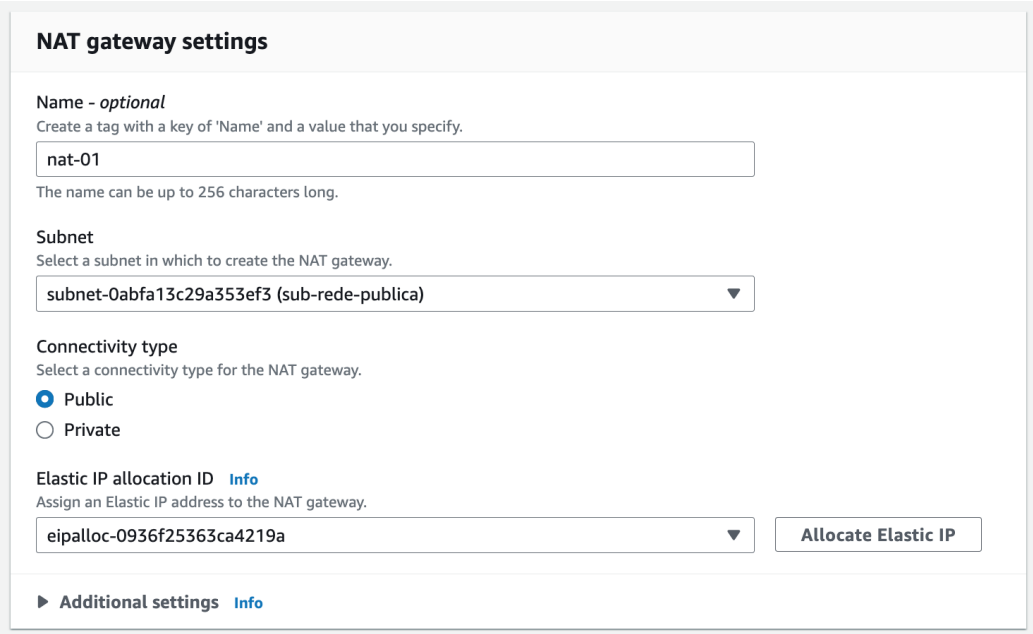
```
sshkey — eduardoverri@Eduardos-MacBook-Pro — -zsh — 104×25
...h -i myssh.pem ubuntu@54.226.249.155   ..esktop/sshkey   ..esktop/sshkey
[ 12:00 ]  [ eduardoverri@Eduardos-MacBook-Pro:~/Desktop/sshkey ]
 $ ssh -i myssh.pem ubuntu@10.0.0.225
ssh: connect to host 10.0.0.225 port 22: Operation timed out
[ 12:02 ]  [ eduardoverri@Eduardos-MacBook-Pro:~/Desktop/sshkey ]
 $
```

Ao tentar realizar um `sudo apt update`, não funciona!

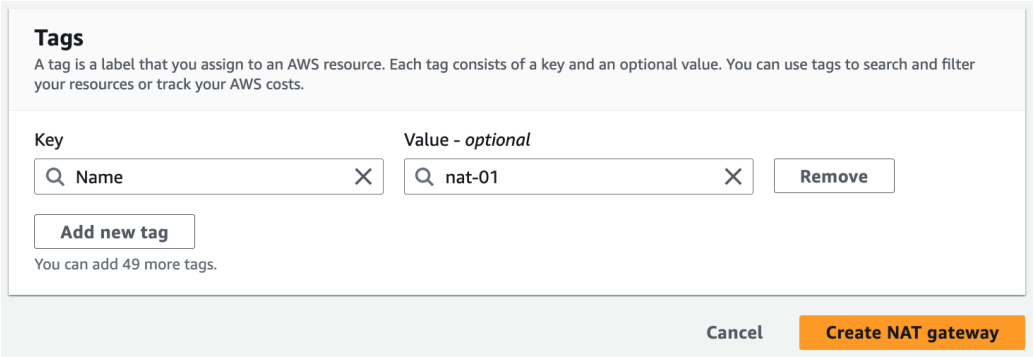
```
sshkey — ubuntu@ip-10-0-0-225: ~ — ssh -i myssh.pem ubuntu@54.226.249.155 — 104×25
...h -i myssh.pem ubuntu@54.226.249.155   ..esktop/sshkey   ..esktop/sshkey
iate the connection to us-east-1.ec2.archive.ubuntu.com:80 (2600:1f18:5c55:4c04:b8fe:122c:bb55:6b84). - connect (101: Network is unreachable) Cannot initiate the connection to us-east-1.ec2.archive.ubuntu.com:80 (2600:1f18:5c55:4c05:17c8:ad29:43bf:eb48). - connect (101: Network is unreachable) Cannot initiate the connection to us-east-1.ec2.archive.ubuntu.com:80 (2600:1f18:5c55:4c00:2637:a32b:ccef:30d5). - connect (101: Network is unreachable) Cannot initiate the connection to us-east-1.ec2.archive.ubuntu.com:80 (2600:1f18:5c55:4c00:7447:9a97:fa56:cd92). - connect (101: Network is unreachable) Cannot initiate the connection to us-east-1.ec2.archive.ubuntu.com:80 (2600:1f18:5c55:4c00:e093:e2e5:23b4:529f). - connect (101: Network is unreachable) Cannot initiate the connection to us-east-1.ec2.archive.ubuntu.com:80 (2600:1f18:5c55:4c01:32a9:41b2:cfa3:904a). - connect (101: Network is unreachable) Cannot initiate the connection to us-east-1.ec2.archive.ubuntu.com:80 (2600:1f18:5c55:4c01:ed0c:fdfa:1470:afc0). - connect (101: Network is unreachable) Cannot initiate the connection to us-east-1.ec2.archive.ubuntu.com:80 (2600:1f18:5c55:4c02:b55:260f:8030:b812). - connect (101: Network is unreachable)
W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/jammy-security/InRelease  Cannot initiate the connection to security.ubuntu.com:80 (2620:2d:4002:1::102). - connect (101: Network is unreachable) Cannot initiate the connection to security.ubuntu.com:80 (2620:2d:4002:1::103). - connect (101: Network is unreachable) Cannot initiate the connection to security.ubuntu.com:80 (2620:2d:4000:1::16). - connect (101: Network is unreachable) Cannot initiate the connection to security.ubuntu.com:80 (2620:2d:4000:1::19). - connect (101: Network is unreachable) Cannot initiate the connection to security.ubuntu.com:80 (2620:2d:4002:1::101). - connect (101: Network is unreachable) Could not connect to security.ubuntu.com:80 (185.125.190.39), connection timed out Could not connect to security.ubuntu.com:80 (91.189.91.81), connection timed out Could not connect to security.ubuntu.com:80 (91.189.91.82), connection timed out Could not connect to security.ubuntu.com:80 (91.189.91.83), connection timed out Could not connect to security.ubuntu.com:80 (185.125.190.36), connection timed out
W: Some index files failed to download. They have been ignored, or old ones used instead.
ubuntu@ip-10-0-0-225:~$
```

Configurando NAT Gateway e Route Table

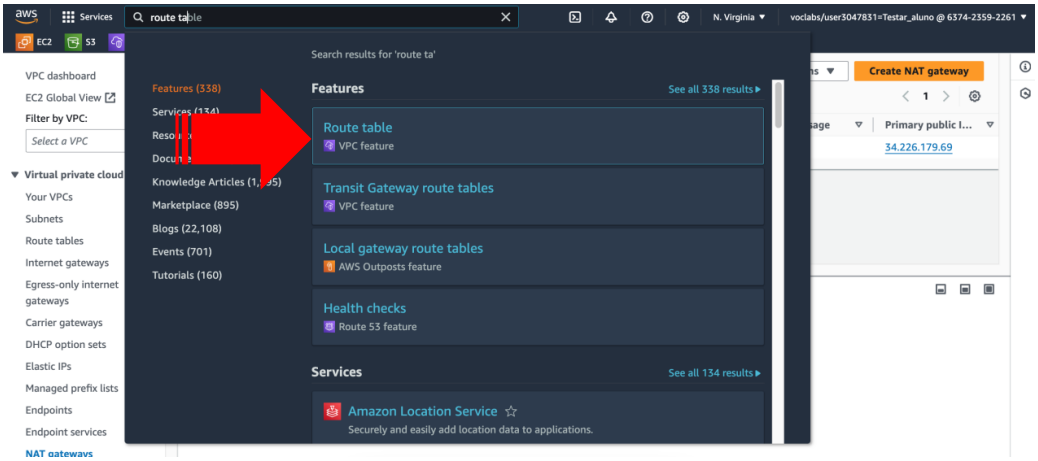


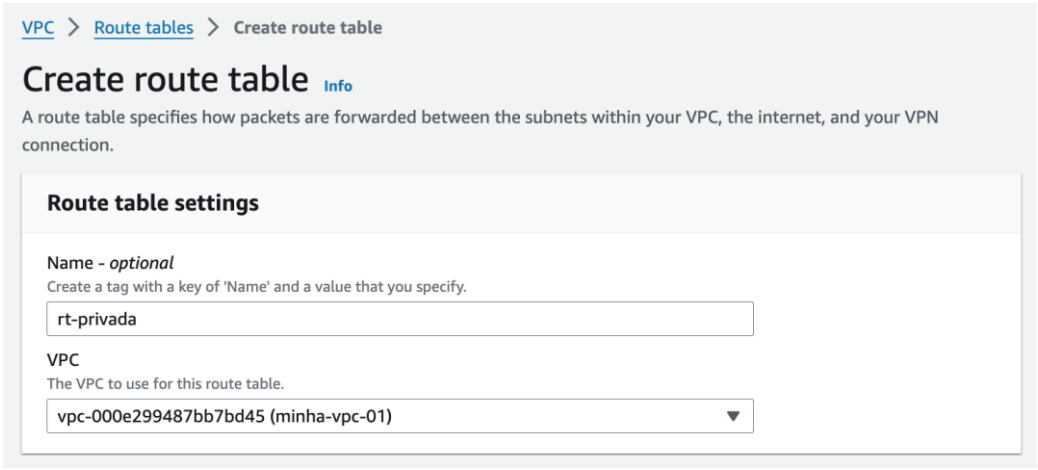


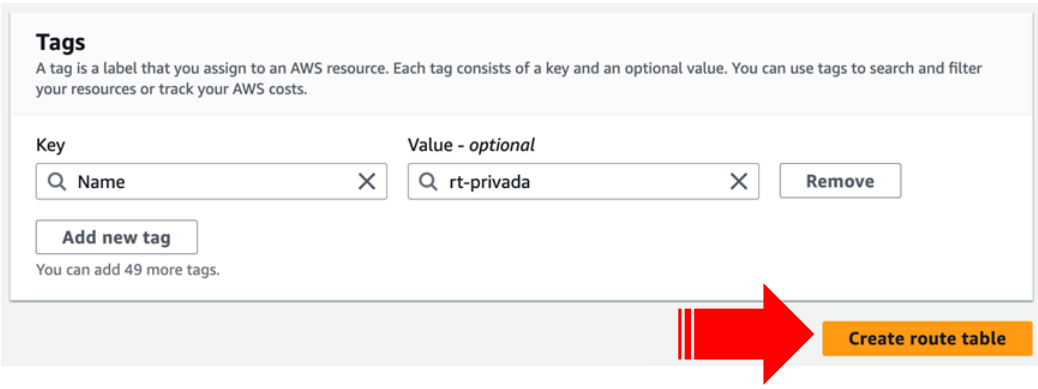
Vamos alocar o NAT gateway na sub rede pública, pois ele terá acesso à Internet. Iremos também alocar um IP elástico para ele, caso tivéssemos criado um IP elástico poderíamos alocar o criado. Ao final clicamos em **Create NAT gateway**.



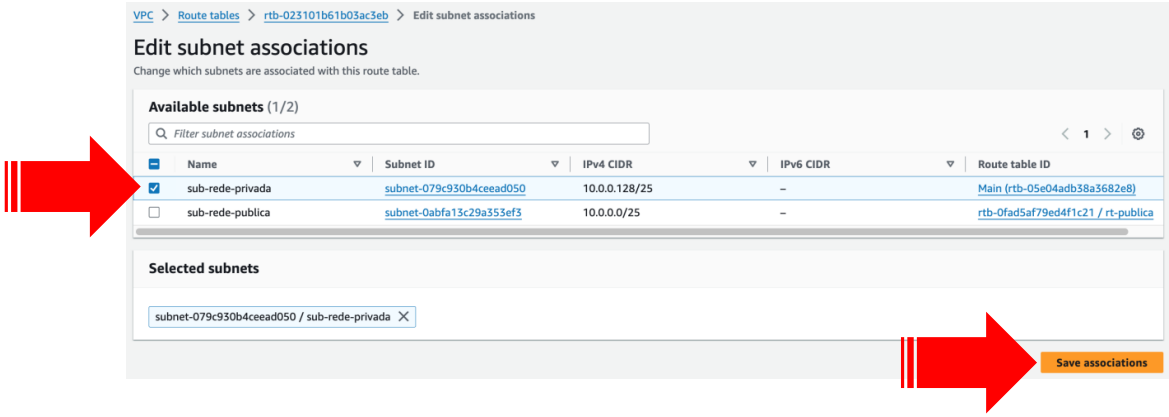
Só que da mesma forma que criamos um tabela de rota entre a sub rede pública e o Internet Gateway, precisaremos criar uma tabela de rota entre a sub rede privada e o NAT gateway!

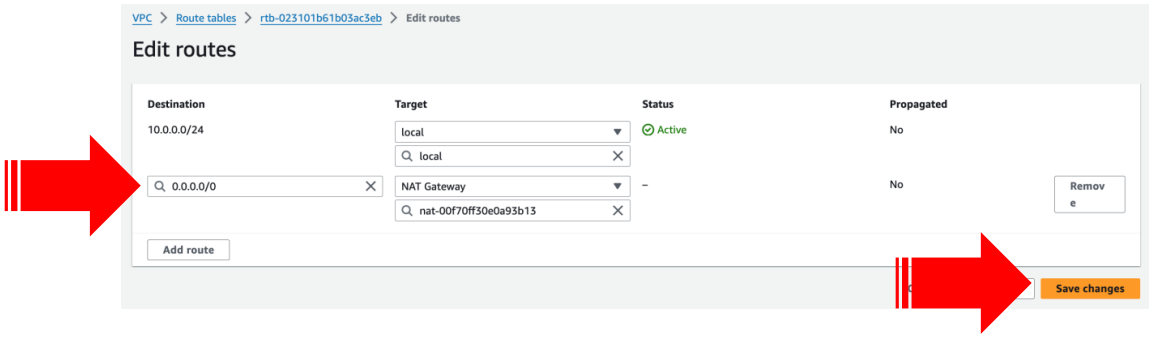






Da mesma forma com o Internet Gateway, preciso associar as sub redes e definir as rotas!





E agora ao rodar `sudo apt update` minha máquina que está numa sub rede privada tem acesso à Internet! O NAT Gateway permite o tráfego outbound, bloqueando o tráfego inbound de Internet à nossa VM. Mas colocamos ele na sub rede pública pois ele tem acesso à Internet.