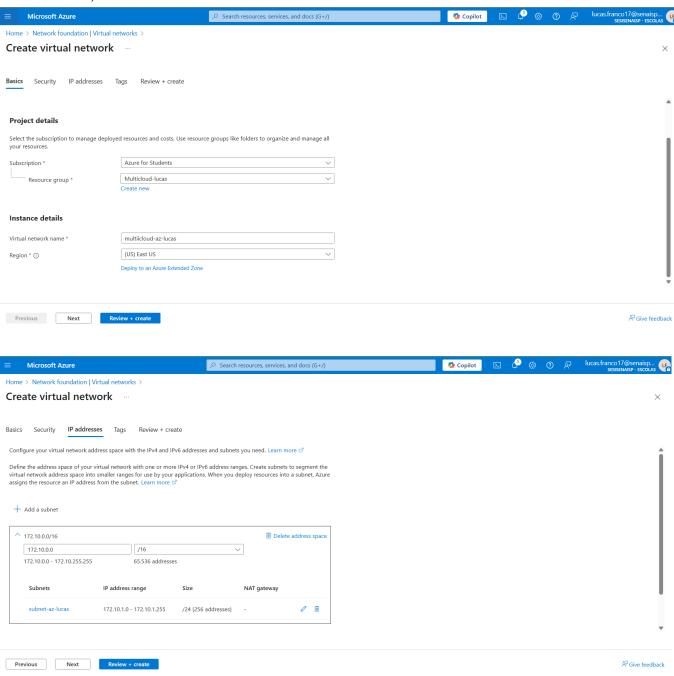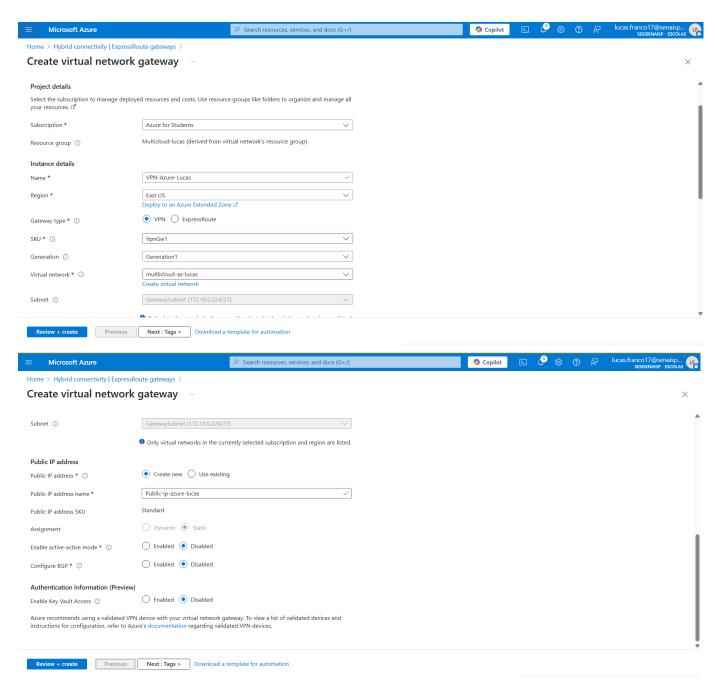# Criação e integração de ambiente multicloud entre Azure e AWS
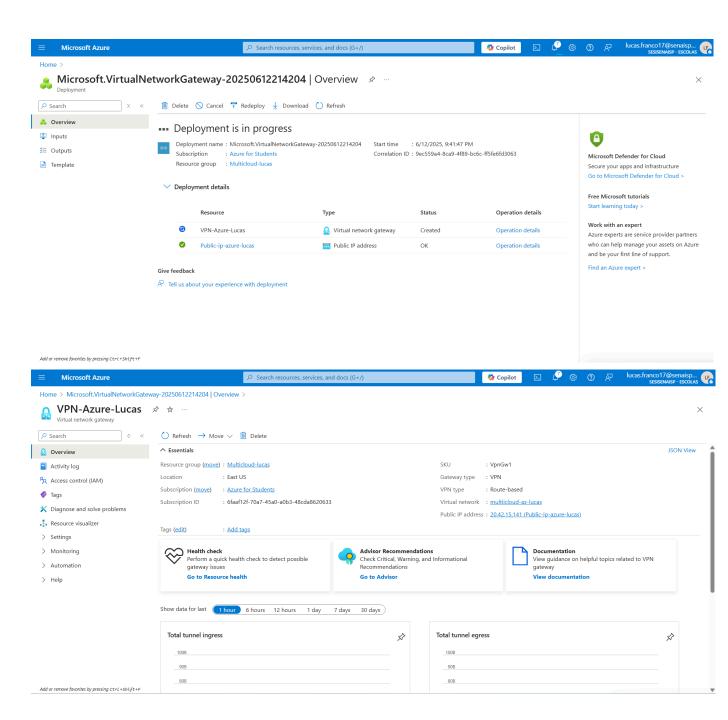
Primeiramente, criar a Virtual Network na Azure
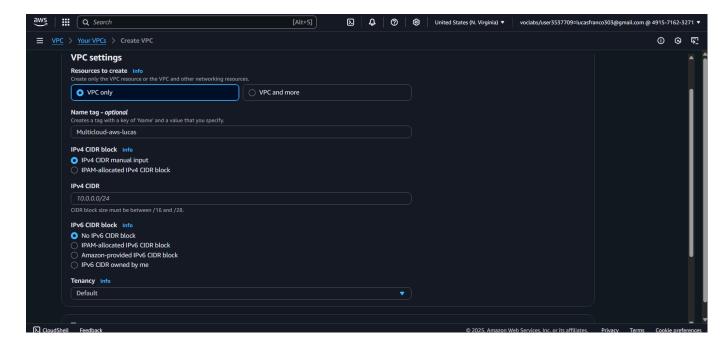

Agora, criar a Virtual network gateway

Home > Hybrid connectivity | ExpressRoute gateways >

Create virtual network gateway   ...

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	Azure for Students
Resource group ⓘ	Multicloud-lucas (derived from virtual network's resource group)

Instance details

Name *	VPN-Azure-Lucas
Region *	East US

Deploy to an Azure Extended Zone

Gateway type * ⓘ	⦿ VPN ○ ExpressRoute
SKU * ⓘ	VpnGw1
Generation ⓘ	Generation1
Virtual network * ⓘ	multiicloud-az-lucas

Create virtual network

Subnet ⓘ	GatewaySubnet (172.10.0.224/27)

[Review + create] [Previous] [Next : Tags >] Download a template for automation

---

Home > Hybrid connectivity | ExpressRoute gateways >

Create virtual network gateway   ...

Subnet ⓘ	GatewaySubnet (172.10.0.224/27)

ⓘ Only virtual networks in the currently selected subscription and region are listed.

Public IP address

Public IP address * ⓘ	⦿ Create new ○ Use existing
Public IP address name *	Public-ip-azure-lucas
Public IP address SKU	Standard
Assignment	○ Dynamic ⦿ Static
Enable active-active mode * ⓘ	○ Enabled ⦿ Disabled
Configure BGP * ⓘ	○ Enabled ⦿ Disabled

Authentication Information (Preview)

Enable Key Vault Access ⓘ	○ Enabled ⦿ Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's documentation regarding validated VPN devices.

[Review + create] [Previous] [Next : Tags >] Download a template for automation
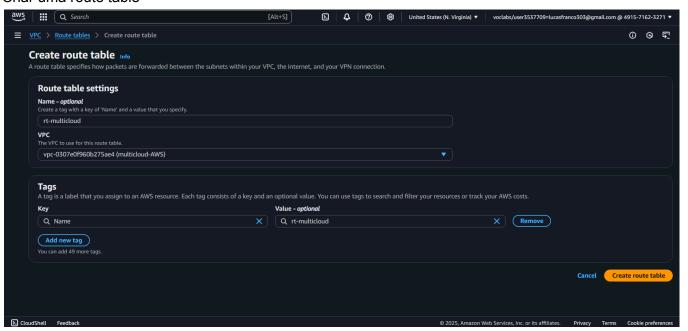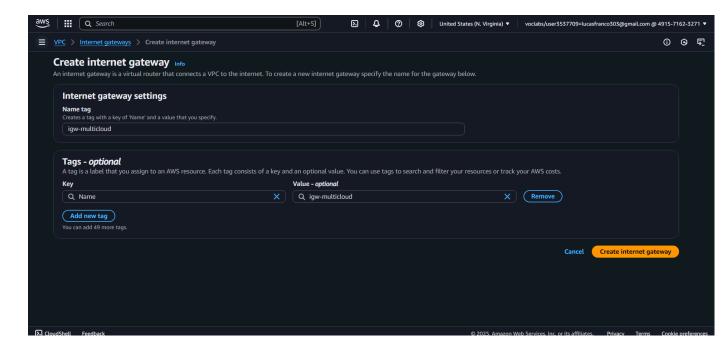
Aguardar um tempinho para ser criado

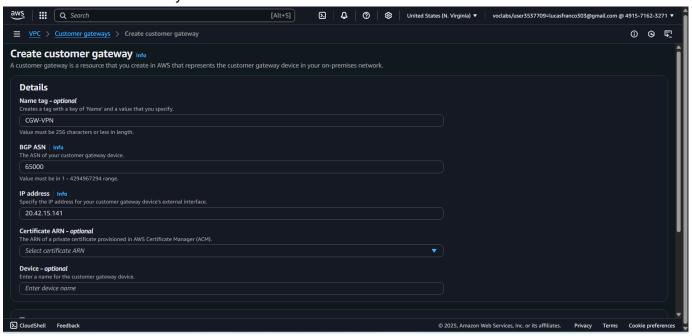Após o deploy ficar completo, criar a VPC na AWS
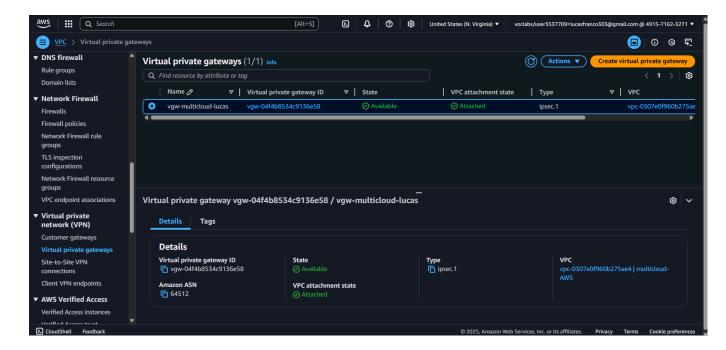
Criar uma route table
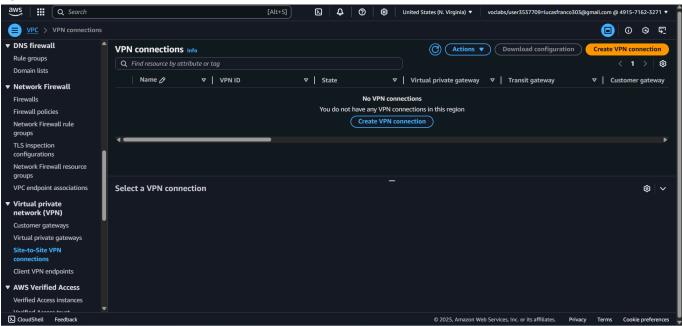

Criar um internet gateway

Agora criar o Customer Gateway (IMPORTANTE: na parte de especificar o ip, colocar o ip do Virtual Network Gateway da Azure
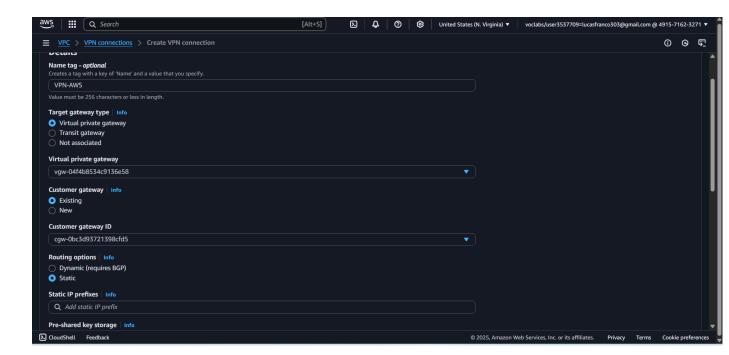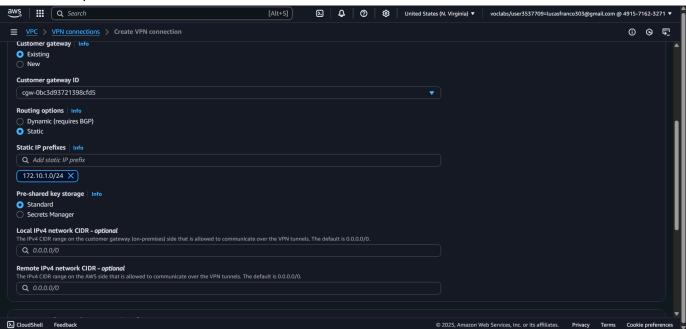

Criar o Virtual private gateway

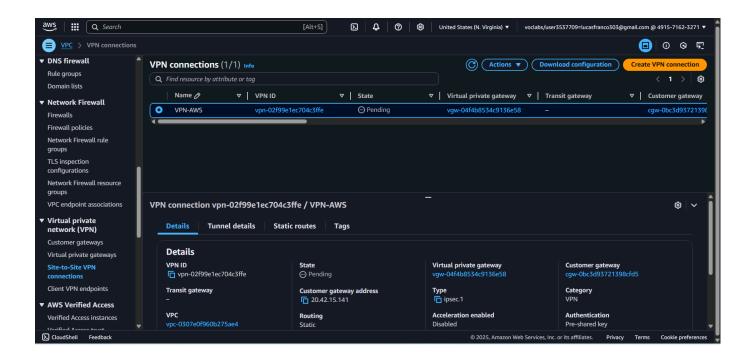Agora criar um site-to-site VPN connections

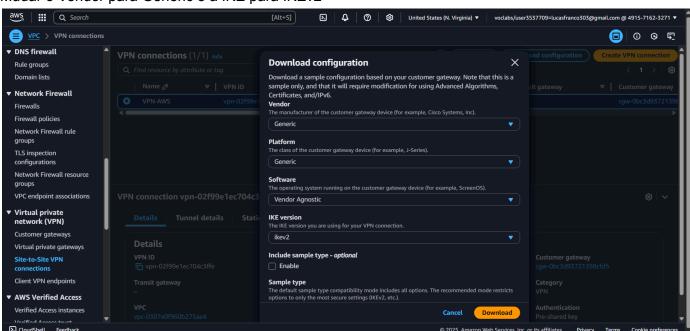Selecionar os recursos que foram criados

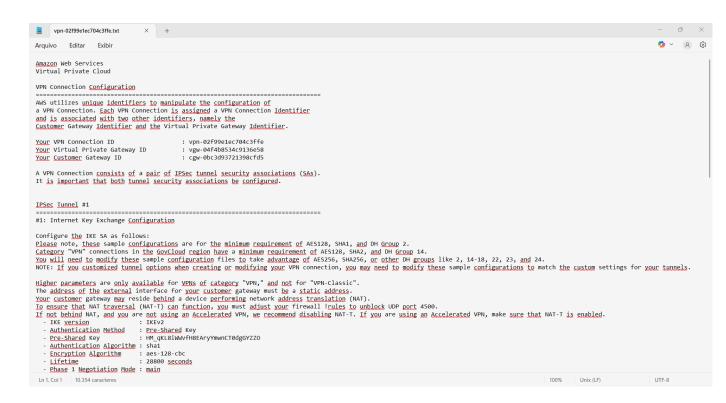Em Static IP prefixes, colocar a rede da Azure

Após criar a VPN Connections, baixar as configurações para que a AWS confie na Azure, clicar na opção Download configuration
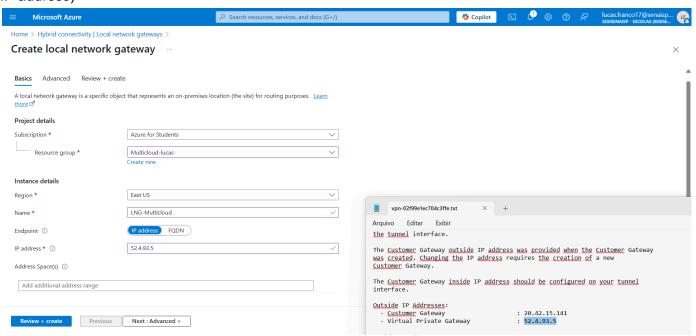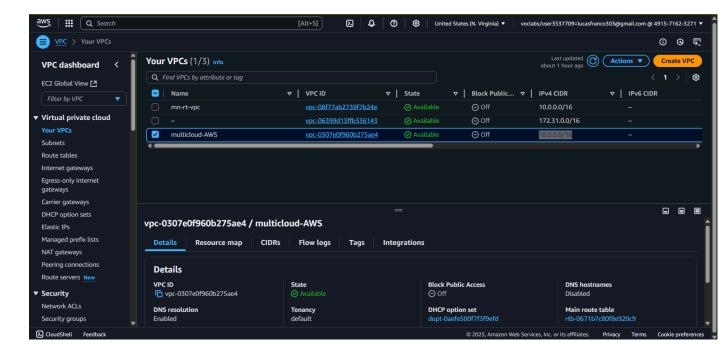
Mudar o Vendor para Generic e a IKE para IKEv2

Baixar e abrir o arquivo para prosseguir

```
vpn-02f99e1ec704c3ffe.txt

Arquivo   Editar   Exibir

Amazon Web Services
Virtual Private Cloud

VPN Connection Configuration
================================================================
AWS utilizes unique identifiers to manipulate the configuration of
a VPN Connection. Each VPN Connection is assigned a VPN Connection Identifier
and is associated with two other identifiers, namely the
Customer Gateway Identifier and the Virtual Private Gateway Identifier.

Your VPN Connection ID              : vpn-02f99e1ec704c3ffe
Your Virtual Private Gateway ID     : vgw-04f4b8534c9136e58
Your Customer Gateway ID            : cgw-0bc3d93721398cfd5

A VPN Connection consists of a pair of IPSec tunnel security associations (SAs).
It is important that both tunnel security associations be configured.


IPSec Tunnel #1
================================================================
#1: Internet Key Exchange Configuration

Configure the IKE SA as follows:
Please note, these sample configurations are for the minimum requirement of AES128, SHA1, and DH Group 2.
Category "VPN" connections in the GovCloud region have a minimum requirement of AES128, SHA2, and DH Group 14.
You will need to modify these sample configuration files to take advantage of AES256, SHA256, or other DH groups like 2, 14-18, 22, 23, and 24.
NOTE: If you customized tunnel options when creating or modifying your VPN connection, you may need to modify these sample configurations to match the custom settings for your tunnels.

Higher parameters are only available for VPNs of category "VPN," and not for "VPN-Classic".
The address of the external interface for your customer gateway must be a static address.
Your customer gateway may reside behind a device performing network address translation (NAT).
To ensure that NAT traversal (NAT-T) can function, you must adjust your firewall !rules to unblock UDP port 4500.
If not behind NAT, and you are not using an Accelerated VPN, we recommend disabling NAT-T. If you are using an Accelerated VPN, make sure that NAT-T is enabled.
  - IKE version                    : IKEv2
  - Authentication Method          : Pre-Shared Key
  - Pre-Shared Key                 : HM_qKL8iWWvfH8EAryYmwnCT0dgGYZZO
  - Authentication Algorithm       : sha1
  - Encryption Algorithm           : aes-128-cbc
  - Lifetime                       : 28800 seconds
  - Phase 1 Negotiation Mode       : main

Ln 1, Col 1    10.354 caracteres                         100%    Unix (LF)          UTF-8
```
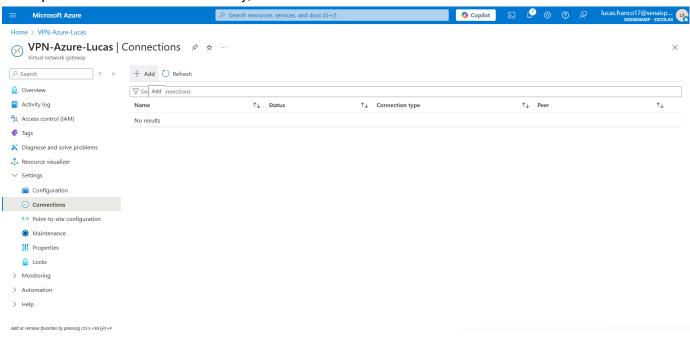
Voltar na Azure e criar um Local Network Gateway
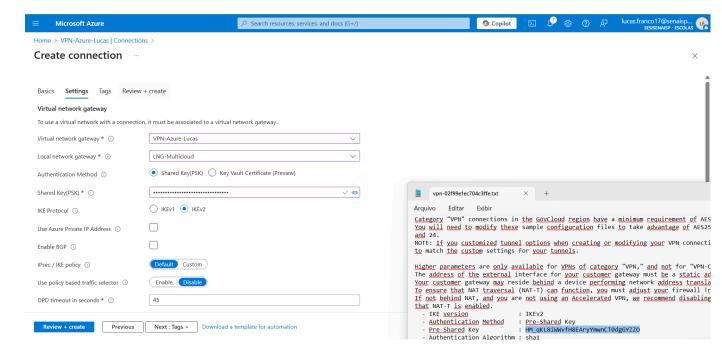na parte de IP address, colocar o IP que está no arquivo de configuração da AWS (Outside IP address)

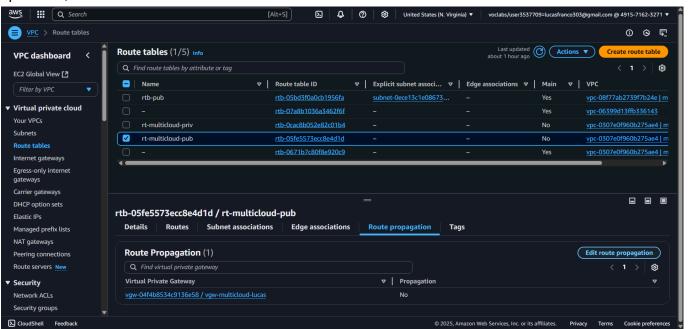**Na parte de range colocar o range da rede da AWS**

Voltar para o Virtual Network Gateway, ir em connections e add connections
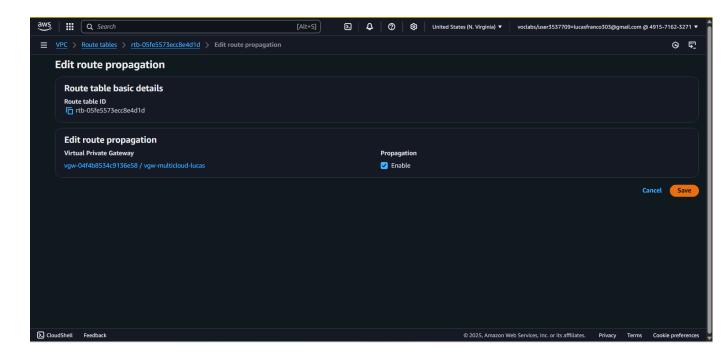

Adicionar as informações e na hora do PSK, pegar no arquivo de configuração da AWS
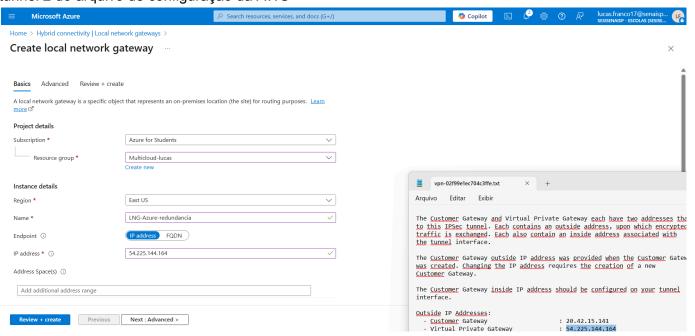
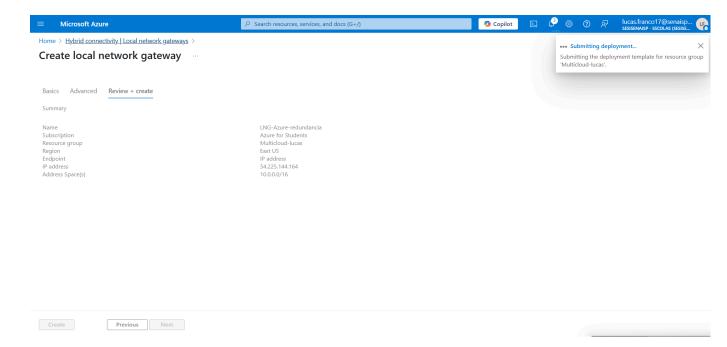Após criar, voltar na AWS e atrelar a rede na route table
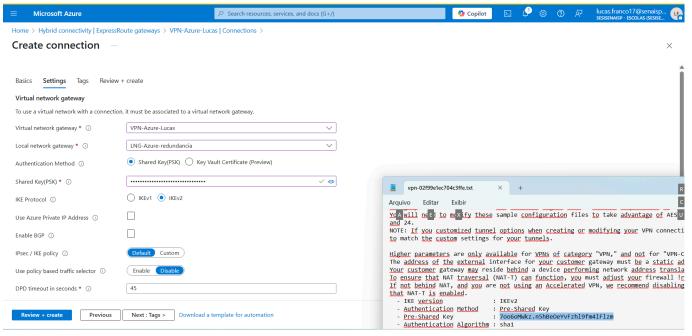

enable

Agora, criar para criar o tunnel 2, precisa criar um outro local network gateway, com o ip do tunnel 2 do arquivo de configuração da AWS
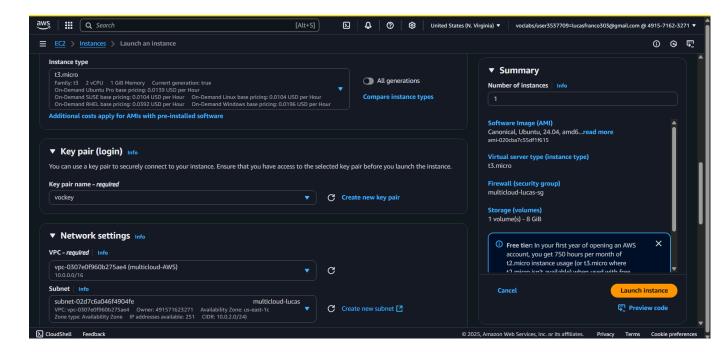

Criar o recurso

Home > Hybrid connectivity | Local network gateways >

Create local network gateway

Submitting deployment...
Submitting the deployment template for resource group 'Multicloud-lucas'.

Basics   Advanced   Review + create

Summary

Name	LNG-Azure-redundancia
Subscription	Azure for Students
Resource group	Multicloud-lucas
Region	East US
Endpoint	IP address
IP address	54.225.144.164
Address Space(s)	10.0.0.0/16

Create   Previous   Next

Criar a conexão na Virtual network gateway

Home > Hybrid connectivity | ExpressRoute gateways > VPN-Azure-Lucas | Connections >

Create connection

Basics   Settings   Tags   Review + create

Virtual network gateway

To use a virtual network with a connection, it must be associated to a virtual network gateway.

Virtual network gateway *   VPN-Azure-Lucas

Local network gateway *   LNG-Azure-redundancia

Authentication Method   ● Shared Key(PSK)   ○ Key Vault Certificate (Preview)

Shared Key(PSK) *   ••••••••••••••••••••••••••••••

IKE Protocol   ○ IKEv1   ● IKEv2

Use Azure Private IP Address   ☐

Enable BGP   ☐

IPsec / IKE policy   [Default] [Custom]

Use policy based traffic selector   [Enable] [Disable]

DPD timeout in seconds *   45

Review + create   Previous   Next : Tags >   Download a template for automation

vpn-02f99e1ec704c3ffe.txt

Arquivo   Editar   Exibir

You will need to modify these sample configuration files to take advantage of AES
and 24.
NOTE: If you customized tunnel options when creating or modifying your VPN connecti
to match the custom settings for your tunnels.

Higher parameters are only available for VPNs of category "VPN," and not for "VPN-C
The address of the external interface for your customer gateway must be a static ad
Your customer gateway may reside behind a device performing network address transla
To ensure that NAT traversal (NAT-T) can function, you must adjust your firewall !r
If not behind NAT, and you are not using an Accelerated VPN, we recommend disabling
that NAT-T is enabled.
  - IKE version   : IKEv2
  - Authentication Method   : Pre-Shared Key
  - Pre-Shared Key   : 7oo6oMWkz.n5hBeOeYvFzhl9fm4lFlzm
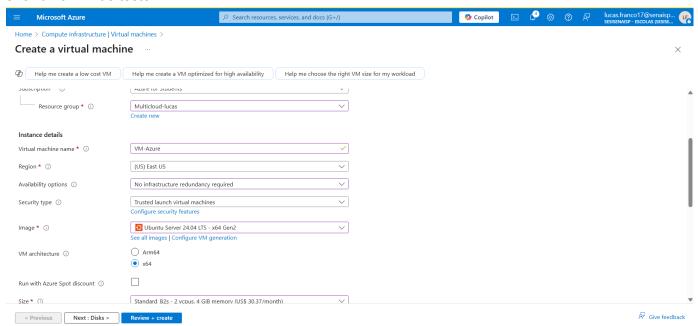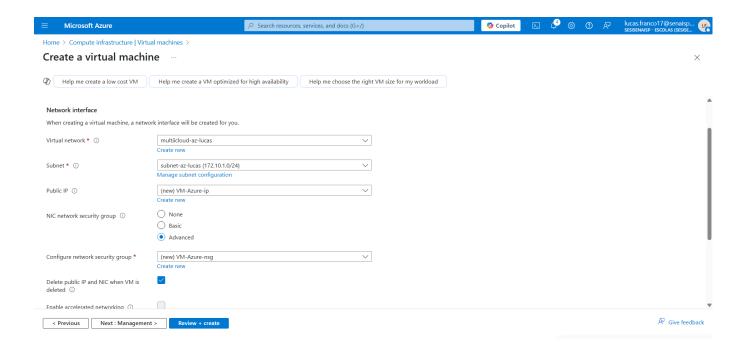 - Authentication Algorithm   : sha1

PRONTO
Teste
Criar uma instancia para teste

Criar uma VM de teste

Criar regras para conexão no security group

Teste de ping


```
System load:    0.0              Temperature:           -273.1 C
Usage of /:     25.7% of 6.71GB  Processes:             109
Memory usage:   24%              Users logged in:       1
Swap usage:     0%               IPv4 address for ens5: 10.0.2.213


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


Last login: Fri Jun 13 03:45:17 2025 from 177.181.0.99
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-2-213:~$ ping 172.10.1.4
PING 172.10.1.4 (172.10.1.4) 56(84) bytes of data.
64 bytes from 172.10.1.4: icmp_seq=1 ttl=64 time=5.74 ms
64 bytes from 172.10.1.4: icmp_seq=2 ttl=64 time=5.46 ms
64 bytes from 172.10.1.4: icmp_seq=3 ttl=64 time=5.21 ms
64 bytes from 172.10.1.4: icmp_seq=4 ttl=64 time=5.27 ms
64 bytes from 172.10.1.4: icmp_seq=5 ttl=64 time=5.12 ms
^C
--- 172.10.1.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 5.122/5.359/5.737/0.218 ms
ubuntu@ip-10-0-2-213:~$
```

```
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.

lucas@VM-Azure:~$
lucas@VM-Azure:~$
lucas@VM-Azure:~$
lucas@VM-Azure:~$
lucas@VM-Azure:~$
lucas@VM-Azure:~$
lucas@VM-Azure:~$ ping 10.0.2.213
PING 10.0.2.213 (10.0.2.213) 56(84) bytes of data.
64 bytes from 10.0.2.213: icmp_seq=1 ttl=64 time=6.07 ms
64 bytes from 10.0.2.213: icmp_seq=2 ttl=64 time=5.69 ms
64 bytes from 10.0.2.213: icmp_seq=3 ttl=64 time=5.07 ms
64 bytes from 10.0.2.213: icmp_seq=4 ttl=64 time=5.74 ms
64 bytes from 10.0.2.213: icmp_seq=5 ttl=64 time=5.86 ms
64 bytes from 10.0.2.213: icmp_seq=6 ttl=64 time=5.90 ms
64 bytes from 10.0.2.213: icmp_seq=7 ttl=64 time=5.12 ms
64 bytes from 10.0.2.213: icmp_seq=8 ttl=64 time=5.00 ms
64 bytes from 10.0.2.213: icmp_seq=9 ttl=64 time=5.18 ms
^C
--- 10.0.2.213 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8012ms
rtt min/avg/max/mdev = 5.003/5.514/6.072/0.392 ms
lucas@VM-Azure:~$
```

Teste de SSH


```
7 packets transmitted, 7 received, 0% packet loss, time 6010ms
rtt min/avg/max/mdev = 4.873/5.265/5.601/0.209 ms
ubuntu@ip-10-0-2-213:~$ ssh lucas@172.10.1.4
The authenticity of host '172.10.1.4 (172.10.1.4)' can't be established.
ED25519 key fingerprint is SHA256:skC2oQxUrx329sAvNYsXYk3nU0/AYbQUxA2UIlyLaCM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.10.1.4' (ED25519) to the list of known hosts.
lucas@172.10.1.4's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-1015-azure x86_64)

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

 System information as of Fri Jun 13 04:20:14 UTC 2025

  System load:  0.0              Processes:             120
  Usage of /:   5.6% of 28.02GB  Users logged in:       1
  Memory usage: 6%               IPv4 address for eth0: 172.10.1.4
  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: Fri Jun 13 03:51:47 2025 from 177.181.0.99
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

lucas@VM-Azure:~$
```