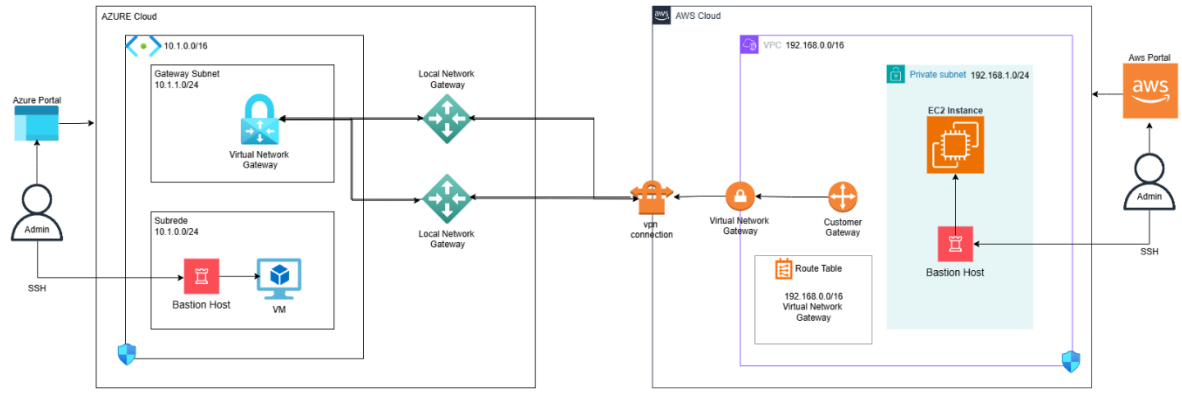
# Lucas Duarte Pires

## Projeto Multi-Cloud Azure & Aws

### Integração Multi-Cloud Azure + AWS via VPN Site-to-Site

Criar um ambiente multi-cloud entre Microsoft Azure e Amazon Web Services (AWS), estabelecendo uma VPN site-to-site que permita a comunicação entre máquinas virtuais usando apenas endereços IP privados.

## Topologia




## Tabela de IPs

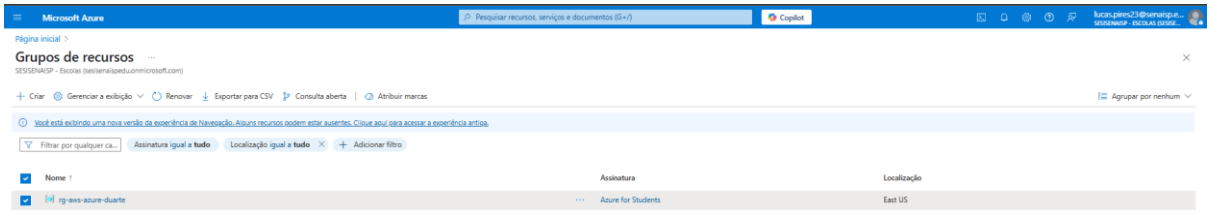
| Multi-Cloud Tabela | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Nuvem** | **Rede** | **Sub-rede** | **Nome-VM** | **IP-Público** | **IP-Privado** | **Função-Vm** | **Tipo-Vm** |
| Azure | 10.1.0.0/16 | 10.1.0.0/24 | bastion-host | 52.226.121.135 | 10.1.0.7 | Bastion-Host | Standard_B2s |
| Azure | 10.1.0.0/16 | 10.1.0.0/24 | vm-azure | ----- | 10.1.0.4 | Internal VM | Standard_B2s |
| Aws | 192.168.0.0/16 | 192.168.1.0/24 | bastion-host | 204.236.248.28 | 192.168.1.50 | Bastion-Host | t2.micro |
| Aws | 192.168.0.0/16 | 192.168.1.0/24 | vm-duarte | ----- | 192.168.1.116 | Internal EC2 | t2.micro |

| Legenda da Tabela | |
|---|---|
| **Nuvem** | Nome da provedora de nuvem utilizada (ex: AWS, Azure). |
| **Rede** | Endereço da rede principal (ex: 10.1.0.0/16), também chamada de VNet (Azure) ou VPC (AWS). |
| **Sub-rede** | Intervalo de IPs atribuído à sub-rede (ex: 10.1.0.0/24), onde a VM está alocada. |
| **Nome-VM** | Nome da máquina virtual definido durante sua criação (ex: vm-duarte). |
| **IP-Público** | Endereço IP acessível pela internet. Pode mudar se for dinâmico (não estático). |
| **IP-Privado** | Endereço IP interno atribuído à VM na rede/sub-rede. Usado para comunicação interna. |
| **Função-VM** | Tipo/tamanho da VM, que define seus recursos de hardware (ex: t2.micro, Standard_B2s). |
| **Tipo-VM** | Finalidade da máquina na arquitetura. |

# Azure

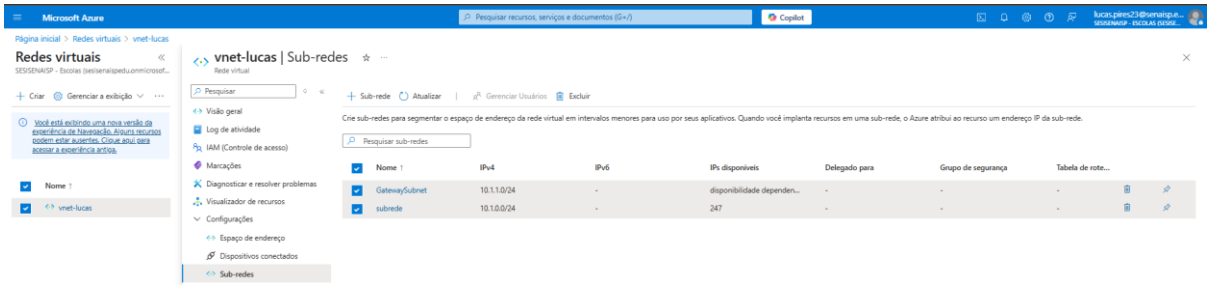
## 1º Passo – Criar o Grupo de Recursos

A criação do grupo de recursos é o ponto de partida para organizar e gerenciar todos os serviços que serão utilizados no Azure. Ele serve como um contêiner lógico para manter os recursos relacionados em um único local.



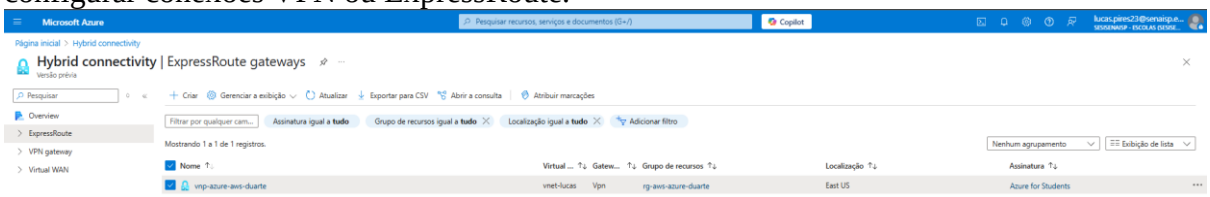

## 2º Passo – Criar a Rede Virtual

A rede virtual (VNet) é fundamental para a comunicação entre os recursos no Azure. Ela permite definir um espaço de endereçamento IP, sub-redes e configurações de segurança, funcionando como a base da infraestrutura em nuvem.




## 3º Passo – Criar o Virtual Network Gateway

O Virtual Network Gateway é responsável por estabelecer a comunicação segura entre a rede virtual do Azure e outras redes, como ambientes locais ou outras VNets. Ele é essencial para configurar conexões VPN ou ExpressRoute.

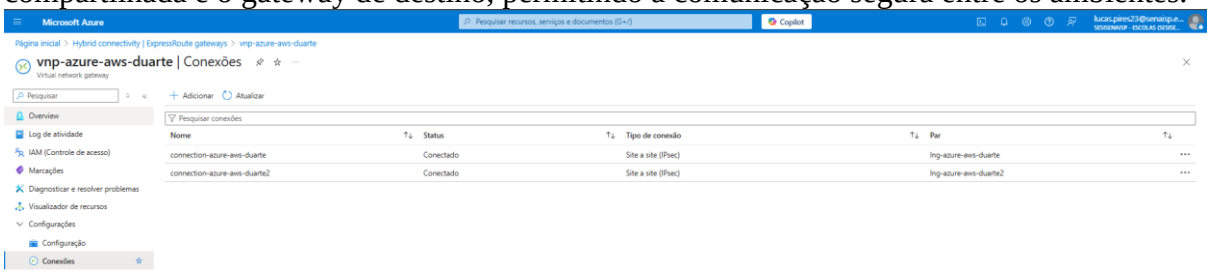



## 4º Passo – Criar o Local Network Gateway

O Local Network Gateway representa a rede local (on-premises) no Azure. Ele armazena informações como o endereço IP público do gateway local e o espaço de endereçamento da rede remota, sendo essencial para estabelecer a conexão VPN site-to-site.

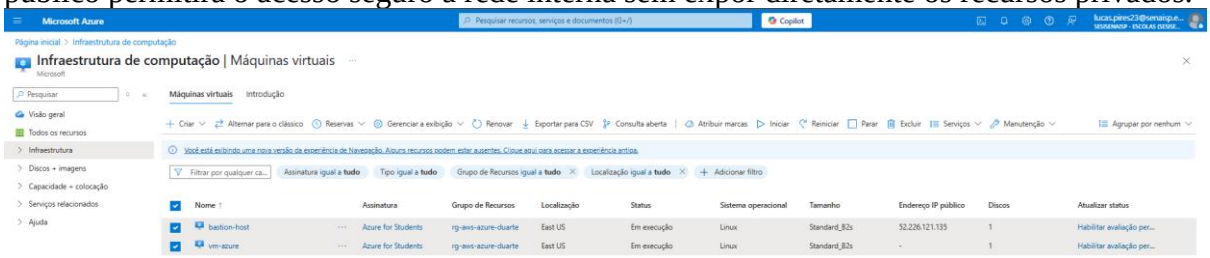
## 5º Passo – Criar a Conexão no Virtual Network Gateway

A conexão no Virtual Network Gateway é o que liga a rede virtual do Azure à rede local. Nessa etapa, são definidas as configurações da VPN, como tipo de conexão, chave compartilhada e o gateway de destino, permitindo a comunicação segura entre os ambientes.



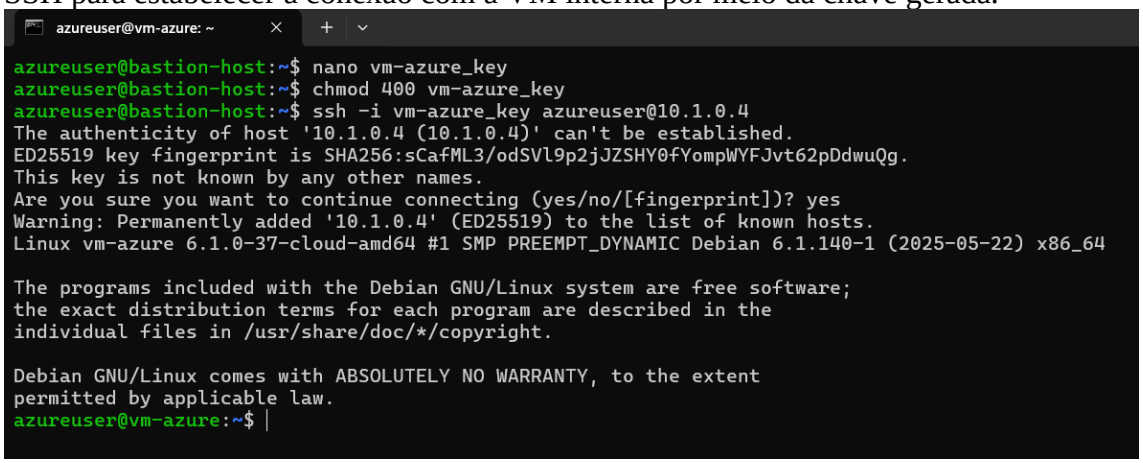

## 6º Passo – Criar Máquinas Virtuais (IP Privado e Bastion Host)

Nesta etapa, serão criadas duas máquinas virtuais: uma com IP privado, que simula um ambiente interno, e outra com IP público, que servirá como Bastion Host. A máquina com IP público permitirá o acesso seguro à rede interna sem expor diretamente os recursos privados.




## 7º Passo – Gerar e Configurar a Chave de Acesso no Bastion Host

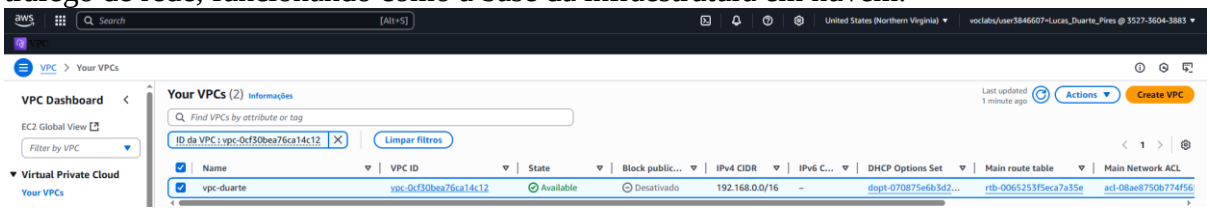
No Bastion Host, será gerada e configurada a chave de acesso necessária para conectar com segurança à máquina virtual privada. Após atualizar os pacotes, criaremos um arquivo para armazenar a chave, aplicaremos as permissões corretas e, por fim, utilizaremos o comando SSH para estabelecer a conexão com a VM interna por meio da chave gerada.



# Aws

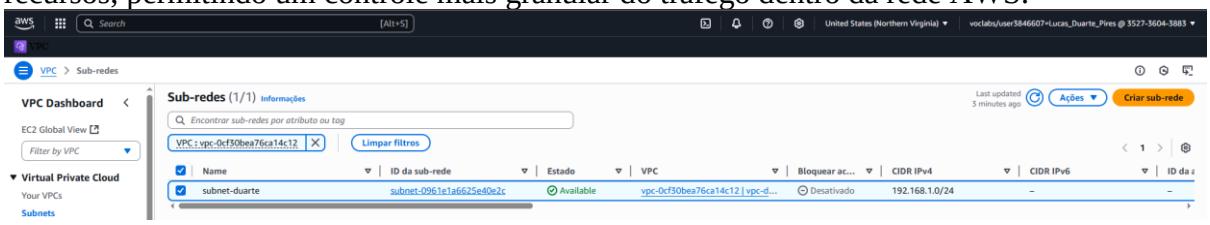
## 1º Passo – Criar a VPC

A VPC (Virtual Private Cloud) é a rede virtual dentro da AWS onde serão implantados os recursos. Ela permite definir um espaço de endereçamento IP personalizado e controlar o tráfego de rede, funcionando como a base da infraestrutura em nuvem.



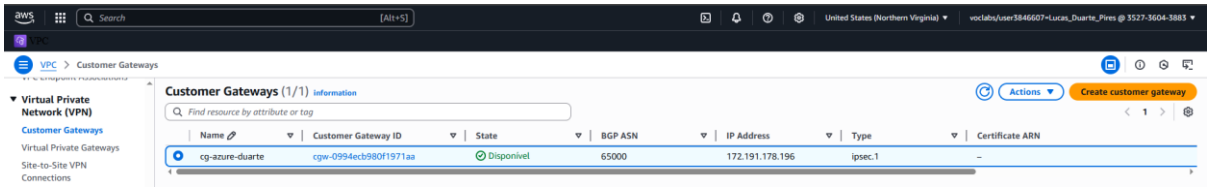

## 2º Passo – Criar uma Subnet

A subnet é uma subdivisão da VPC que segmenta o espaço de IPs para organizar e isolar recursos, permitindo um controle mais granular do tráfego dentro da rede AWS.



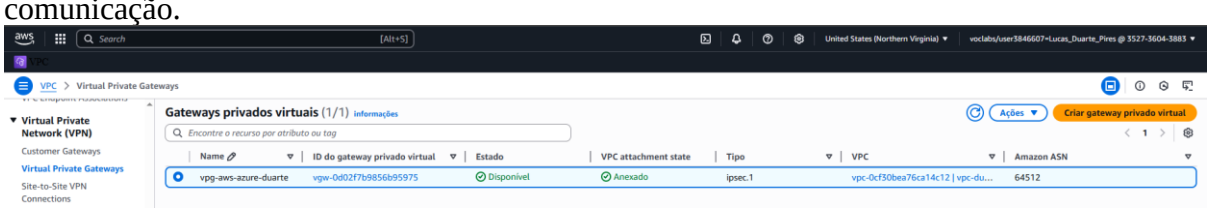

## 3º Passo – Criar o Customer Gateway

O Customer Gateway representa o dispositivo ou a rede local do cliente no ambiente AWS. Ele armazena as informações necessárias para estabelecer a conexão VPN entre a infraestrutura local e a AWS.



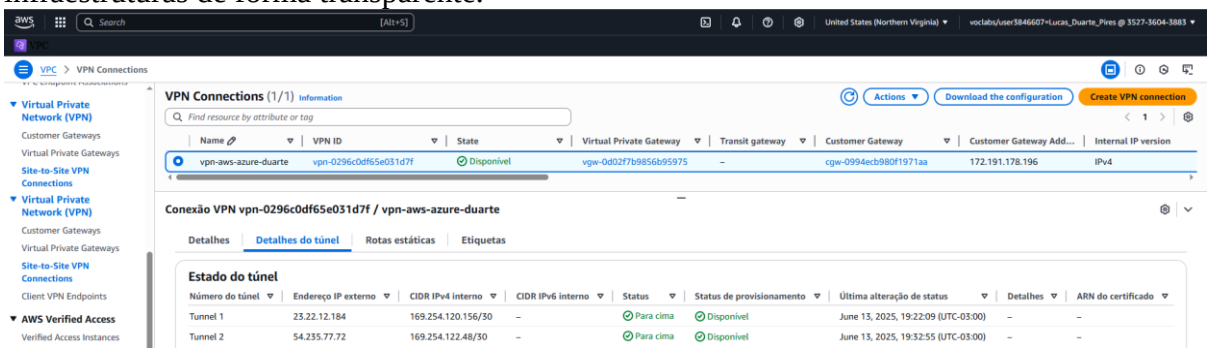

## 4º Passo – Criar a Virtual Private Gateway e Anexar à VPC

A Virtual Private Gateway atua como o ponto de conexão do lado da AWS para a rede privada, permitindo que a VPC se comunique com redes externas, como a infraestrutura local, por meio de VPNs. Após criada, ela deve ser anexada à VPC para estabelecer essa comunicação.



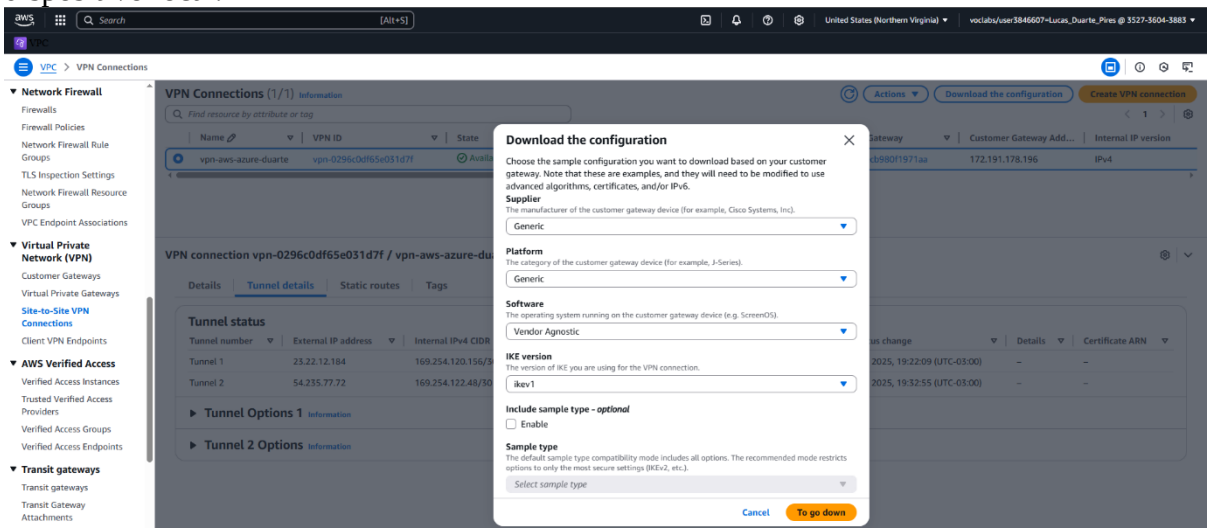
## 5º Passo – Criar a Conexão VPN Site-to-Site

A conexão VPN site-to-site estabelece um túnel seguro entre a rede local do cliente e a AWS, permitindo a comunicação privada e criptografada entre os ambientes, integrando as infraestruturas de forma transparente.



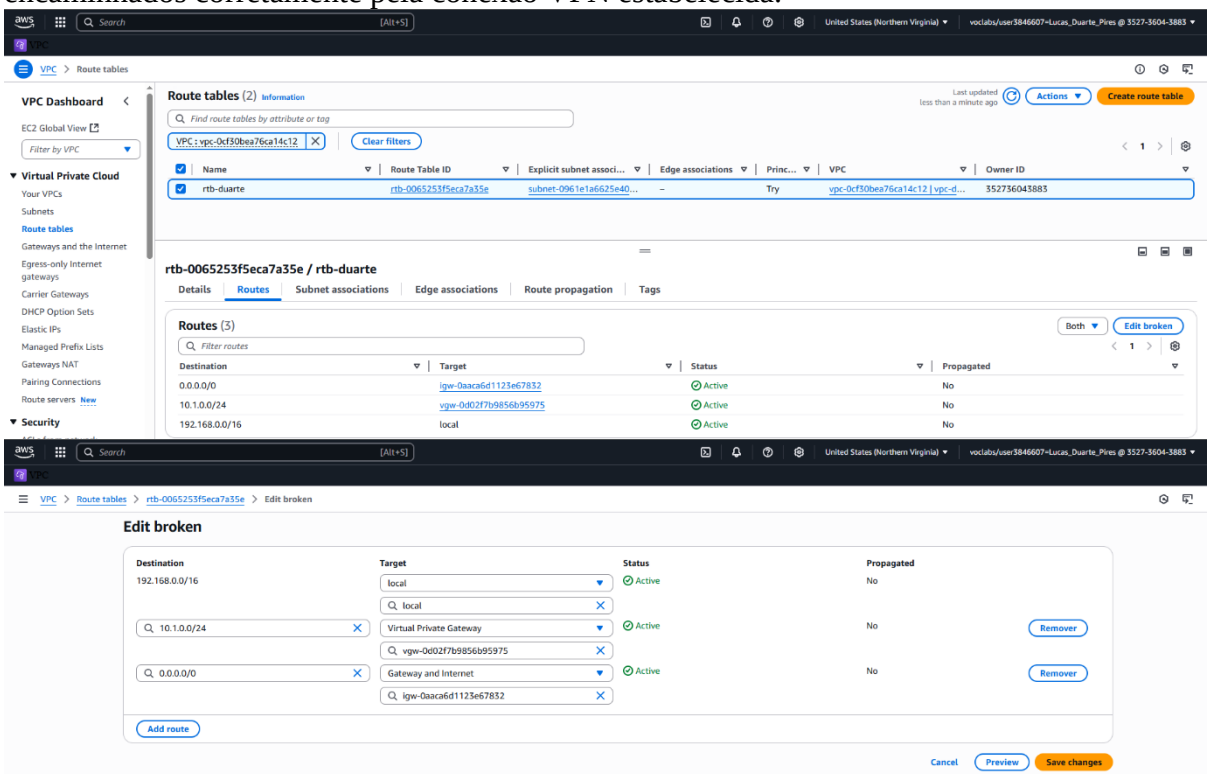

## 6º Passo – Download do Arquivo de Configuração e Dados da Conexão VPN

Após criar a conexão VPN, faça o download do arquivo de configuração gerado pela AWS. Nele, constam informações essenciais para o estabelecimento do túnel seguro, como as chaves pré-compartilhadas (Pre-Shared Keys) e os endereços dos Virtual Private Gateways para cada túnel da conexão. Esses dados são necessários para configurar corretamente o dispositivo local.



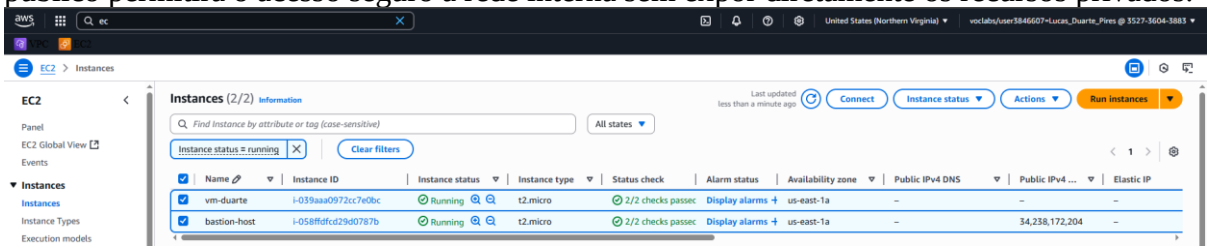
## 7º Passo – Criar e Associar a Route Table ao Virtual Private Gateway

Nesta etapa, será criada e configurada a tabela de rotas da VPC para direcionar o tráfego destinado à rede local através do Virtual Private Gateway, garantindo que os pacotes sejam encaminhados corretamente pela conexão VPN estabelecida.

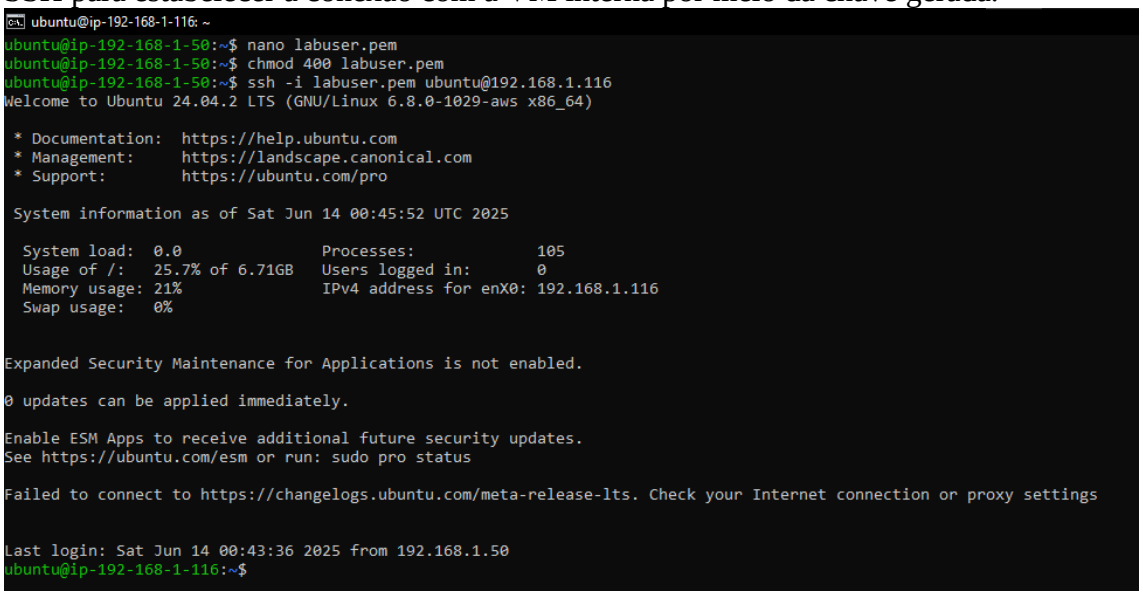



## 8º Passo – Criar Máquinas Virtuais (IP Privado e Bastion Host)

Nesta etapa, serão criadas duas máquinas virtuais: uma com IP privado, que simula um ambiente interno, e outra com IP público, que servirá como Bastion Host. A máquina com IP público permitirá o acesso seguro à rede interna sem expor diretamente os recursos privados.

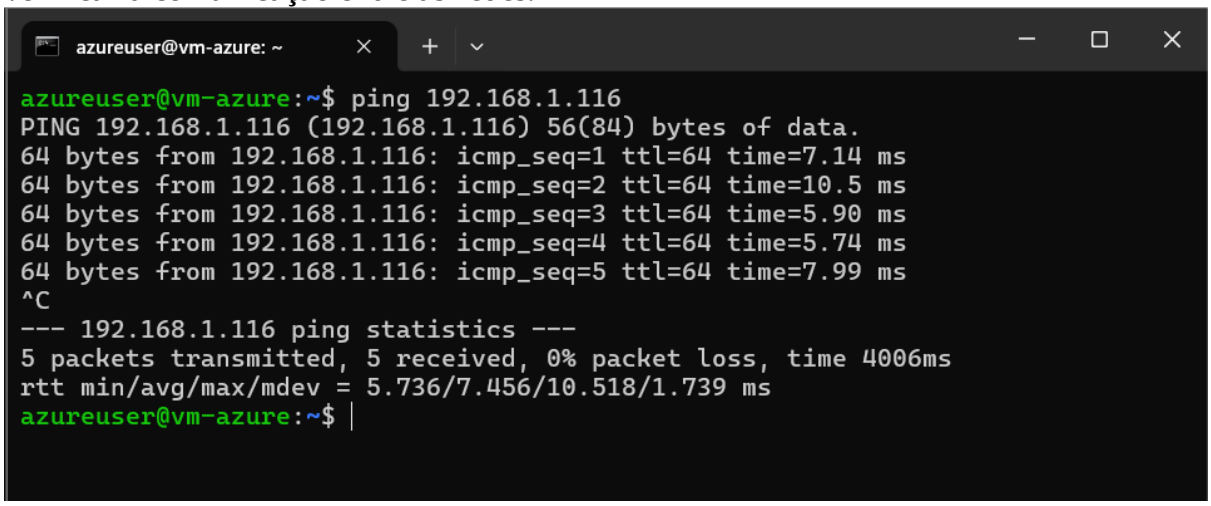


**9º Passo – Gerar e Configurar a Chave de Acesso no Bastion Host**
No Bastion Host, será gerada e configurada a chave de acesso necessária para conectar com segurança à máquina virtual privada. Após atualizar os pacotes, criaremos um arquivo para armazenar a chave, aplicaremos as permissões corretas e, por fim, utilizaremos o comando SSH para estabelecer a conexão com a VM interna por meio da chave gerada.




## Testes

**Azure: Realizando teste de Ping para o IP da máquina AWS (192.168.1.116) para verificar a comunicação entre as redes.**



**Aws: Realizando teste de Ping para o IP da máquina Azure (10.1.0.4) para confirmar a conectividade entre os ambientes.**