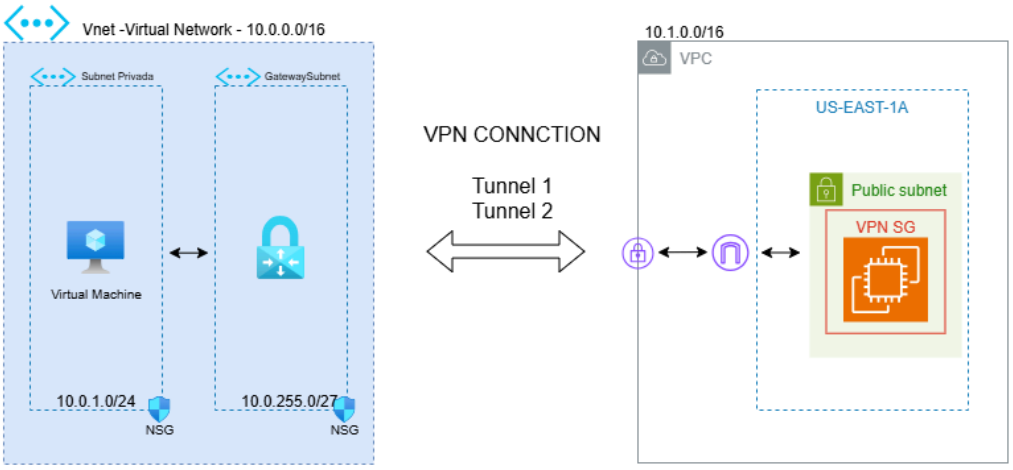
Documentação Técnica — Integração Multi-Cloud Azure + AWS via VPN Site-to-Site

Visão Geral do Projeto

Este projeto tem como objetivo criar uma integração entre as plataformas **Microsoft Azure** e **Amazon Web Services (AWS)**, utilizando uma conexão VPN site-to-site. A comunicação deve ocorrer exclusivamente através de IPs privados, garantindo segurança e isolamento de rede.

Diagrama da Arquitetura



Descrição da arquitetura:

- **Azure:**
  - VNet com subnet privada.
  - Gateway VPN.
  - VM Ubuntu com IP privado.
- **AWS:**
  - VPC com subnet privada.

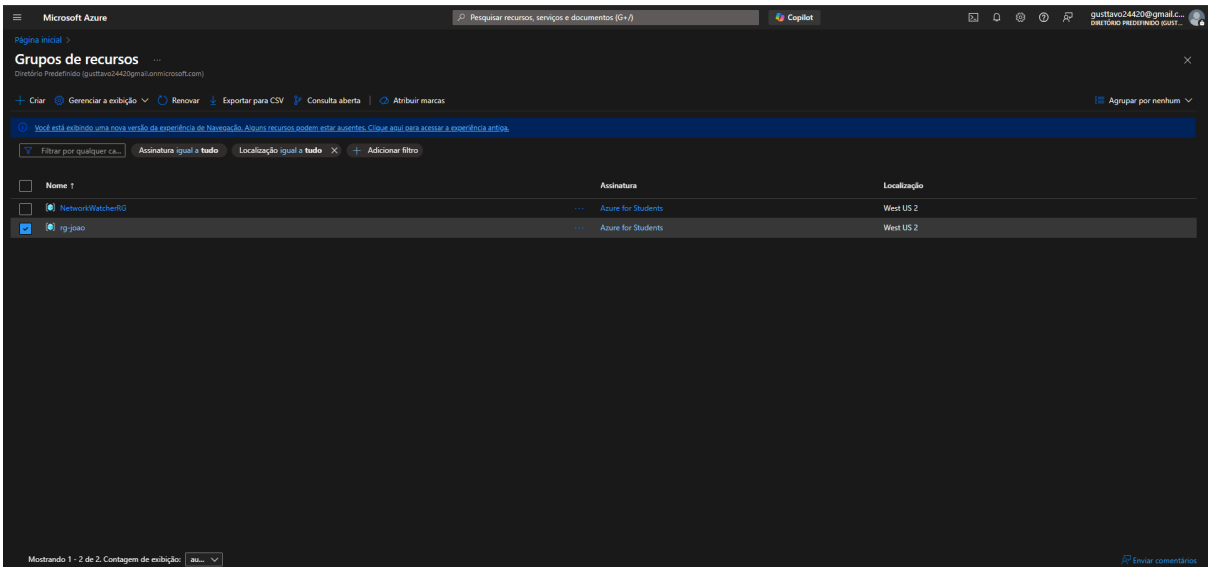
    - Virtual Private Gateway (VGW) e Customer Gateway (CGW).
    - Instância EC2 Ubuntu com IP privado.
- **Conexão VPN Site-to-Site:**
    - Criptografada.
    - Túnel estabelecido entre os dois ambientes.
    - Tráfego roteado exclusivamente por IP privado.

CONFIGURAÇÃO NA AZURE

Criar um grupo de recursos no Azure para implantar os recursos

- Nome do Grupo de Recursos: rg-joao

- Região: West-US 2



Criar uma Rede Virtual (VNet)

- Nome do Grupo de Recursos: rg-joao

- Região: West-US 2

- Nome da VNet: vnet-azure-joao

- IPv4 da VNet: 10.0.0.0/16

- Nome da Sub-rede: sub-net-privada

- IPv4 da Sub-rede : 10.0.1.0/24

- Nome da Sub-rede: GatewaySubnet

- IPv4 da Sub-rede : 10.0.255.0/27

Microsoft Azure | Pesquisar recursos, serviços e documentos (G+/) | Copilot | gusttavo24420@gmail.c... DIRETÓRIO PREDEFINIDO (GUST...

Página inicial >

Redes virtuais

Diretório Predefinido (gusttavo24420gmail.onmicrosoft.com)

+ Criar | Gerenciar a exibição | Renovar | Exportar para CSV | Consulta aberta | Atribuir marcas | Agrupar por nenhum

Você está exibindo uma nova versão da experiência de Navegação. Alguns recursos podem estar ausentes. Clique aqui para acessar a experiência antiga.

Filtrar por qualquer ca... | Assinatura igual a **tudo** | Grupo de Recursos igual a **tudo** | Localização igual a **tudo** | + Adicionar filtro

Não há redes virtuais para exibir

Crie uma rede virtual para conectar os recursos do Azure uns aos outros com segurança. Conecte a rede virtual às suas redes locais usando um Gateway de VPN ou ExpressRoute do Azure.

+ Criar

Saiba mais

Mostrando 1 - 0 de 0. Contagem de exibição: au...

Enviar comentários

Microsoft Azure | Pesquisar recursos, serviços e documentos (G+/) | Copilot | gusttavo24420@gmail.c... DIRETÓRIO PREDEFINIDO (GUST...

Página inicial > Redes virtuais >

Criar rede virtual

Básicos | Segurança | Endereços IP | Rótulos | Revisar + criar

A VNet (Rede Virtual) do Azure é o bloco de construção fundamental para a sua rede privada no Azure. A VNet habilita muitos tipos de recursos do Azure, como as VMs (Máquinas Virtuais) do Azure, para se comunicar com segurança entre si, a Internet e redes locais. A VNet é semelhante a uma rede tradicional que você operaria no seu próprio data center, mas traz os benefícios adicionais da infraestrutura do Azure, como escala, disponibilidade e isolamento.
Saiba mais.

Detalhes do projeto

Selecione a assinatura para gerenciar os custos e os recursos implantados. Use grupos de recursos como pastas para organizar e gerenciar todos os seus recursos.

Assinatura * : Azure for Students

Grupo de recursos * : (Novo) rg-joao
Criar novo

Detalhes da instância

Nome da rede virtual * : VNet-Azure-Joao

Região * : (US) West US 2
Implantar em uma Zona Estendida do Azure

Anterior | Avançar | Revisar + criar

Enviar comentários

Microsoft Azure | Pesquisar recursos, serviços e documentos (G+/) | Copilot | gusttavo24420@gmail.c... DIRETÓRIO PREDEFINIDO (GUST...

Página inicial > Redes virtuais >

Criar rede virtual

Básicos | Segurança | **Endereços IP** | Rótulos | Revisar + criar

Configure seu espaço de endereço de rede virtual com os endereços de IPv4 e IPv6 e as sub-redes necessárias. Saiba mais

Defina o espaço de endereço da rede virtual com um ou mais intervalos de endereços IPv4 ou IPv6. Crie sub-redes para segmentar o espaço de endereço da rede virtual em intervalos menores para uso por seus aplicativos. Quando você implanta recursos em uma sub-rede, o Azure atribui ao recurso um endereço IP da sub-rede. Saiba mais

+ Adicionar uma sub-rede

10.0.0.0/16 — Excluir espaço de endereço

10.0.0.0 | /16

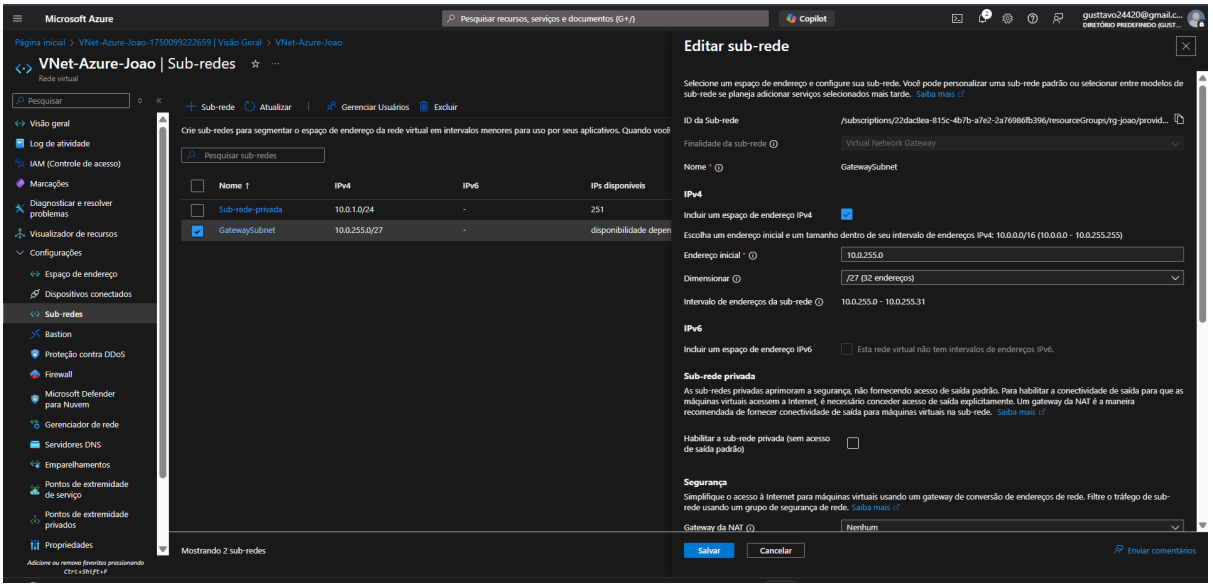
10.0.0.0 - 10.0.255.255 | 65.536 endereços

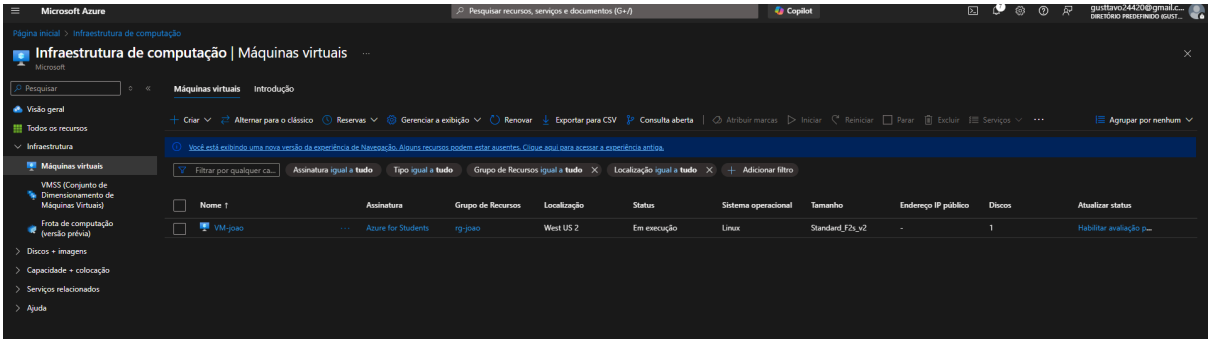
Subredes	Intervalo de endereços IP	Dimensionar	Gateway da NAT
Sub-rede-privada	10.0.1.0 - 10.0.1.255	/24 (256 endereços)	-

Adicionar espaço de endereço IPv4

Anterior | Avançar | Revisar + criar

Enviar comentários





Criar o Gateway VPN

- Nome do Gateway VPN: vpn-azure-aws

- Região: West-US 2

- Tipo de Gateway: VPN

- SKU: VpnGw1

- Geração: Geração 1

- Rede Virtual: vnet-azure-joao

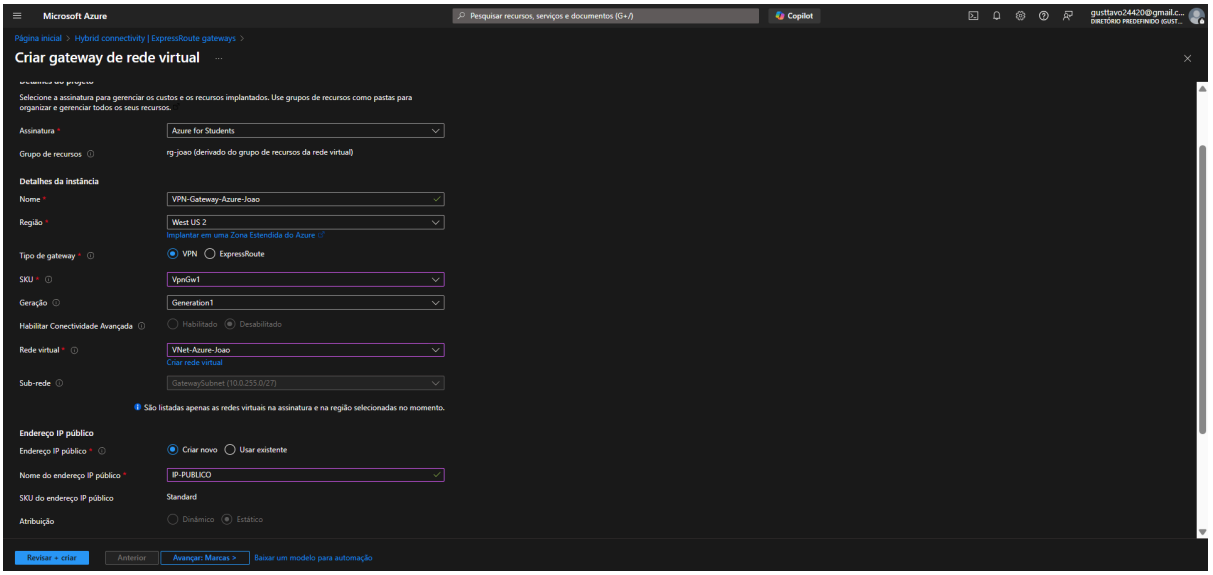
- Endereço IP Público: IP PUBLICO

- Tipo de Endereço IP Público: Básico

- Atribuição: Dinâmica

- Modo ativo-ativo habilitado: Desabilitado

- Configurar BGP: Desabilitado



Criar o Local Network Gateway no Azure

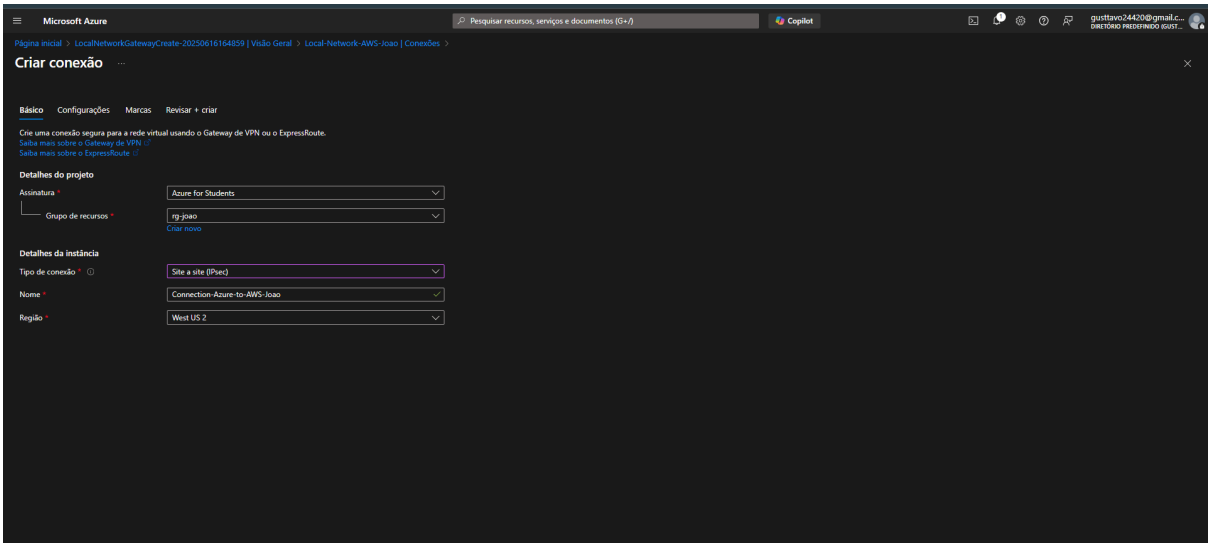
- Nome: lng-azure-aws

- Grupo de Recursos: rg-joao

- Região: West-US 2

- Endereço IP: IP do 1°Primeiro Túnel da conexão Site-to-Site VPN

- Espaço(s) de Endereço: 10.1.0.0/16



Criar a conexão no Virtual Network Gateway do Azure

- Nome: connection-azure-to-aws-Joao

- Tipo de Conexão: Site-to-Site

- Local Network Gateway: Selecionar o criado anteriormente

- Chave Compartilhada: Configurada no 1°Primeiro Túnel da conexão Site-to-Site VPN

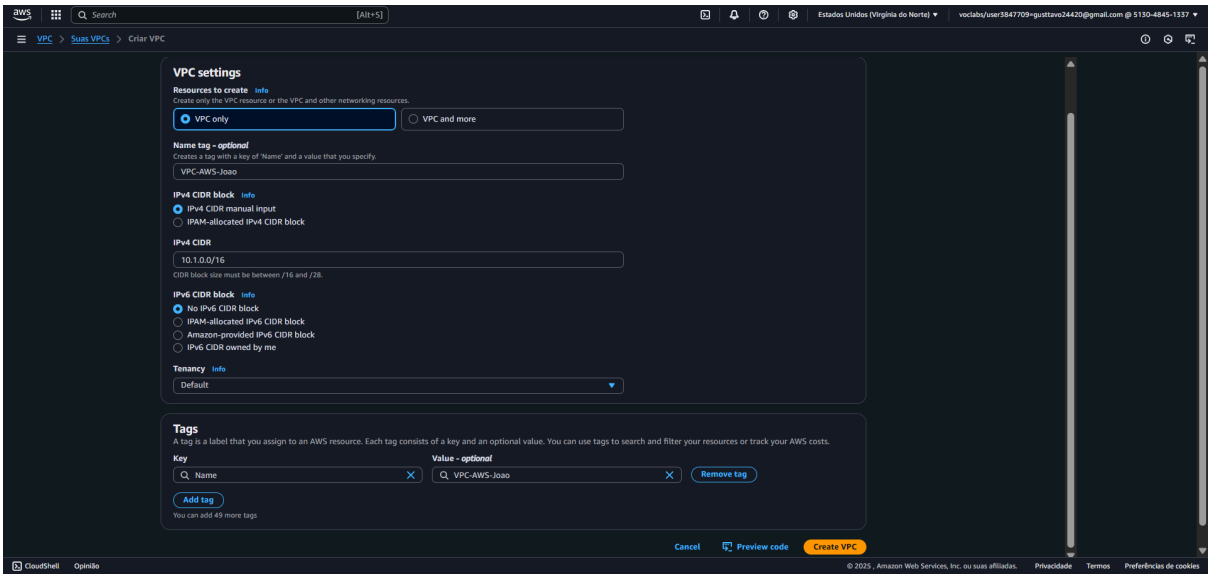
- Esperar até o status mudar para: Conectado

CONFIGURAÇÃO NA AWS

Criando uma VPC.

- Nome: VPC-AWS-Joao

- CIDR IPv4: 10.1.0.0/16



Criação das subnet.

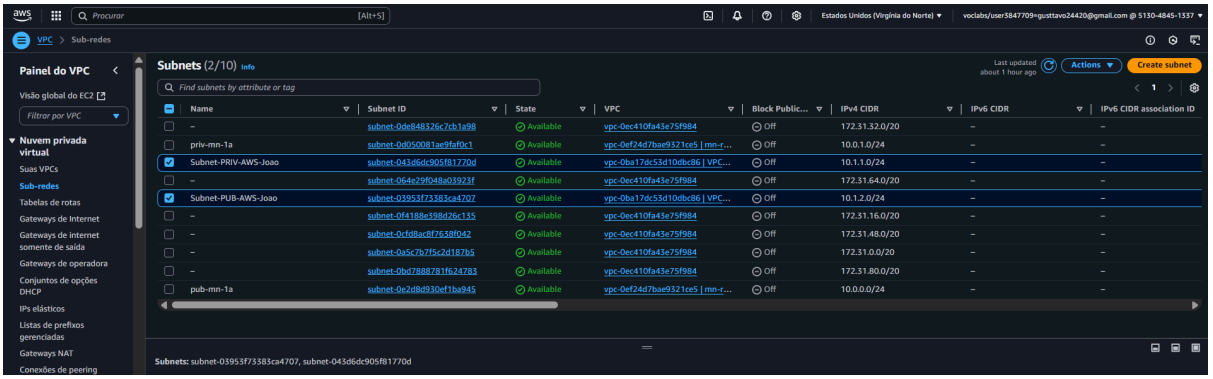
- CIDR IPv4 da VPC: 10.1.0.0/16

- Nome:Subnet-PRIV-AWS-Joao

- CIDR IPv4 da Sub-rede-privada : 10.1.1.0/24

- Nome: Subnet-PUB-AWS-Joao

- CIDR IPv4 da Sub-rede-publica : 10.1.2.0/24



Criação das EC2

- Nome:VM-AWS-Joao-priv

- ISO:Ubuntu Server 24.0

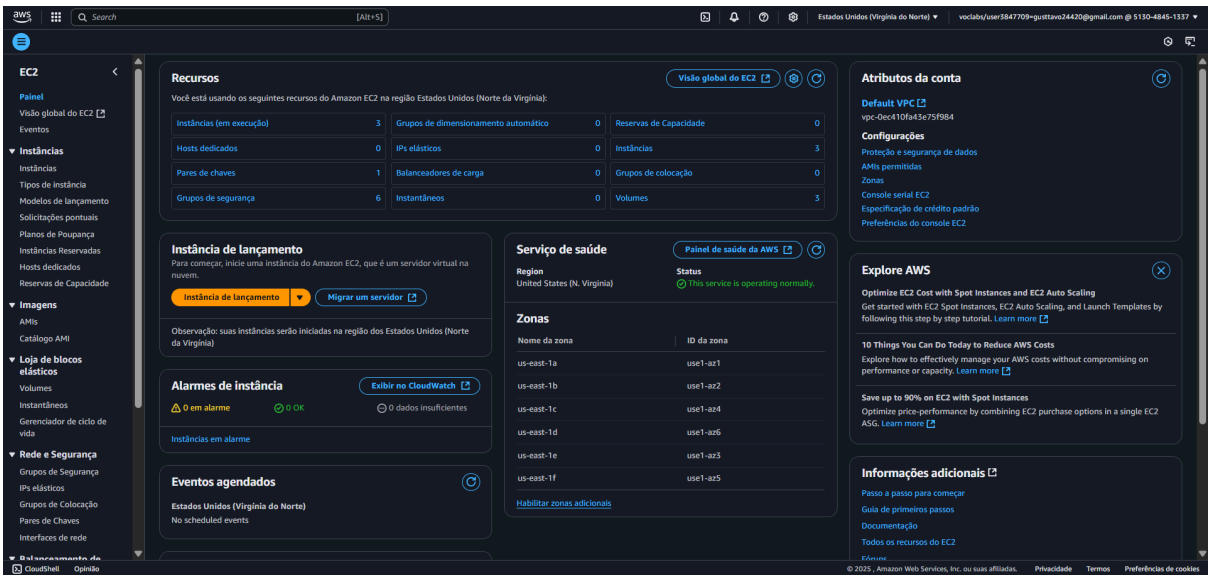
- Chave:Vockey

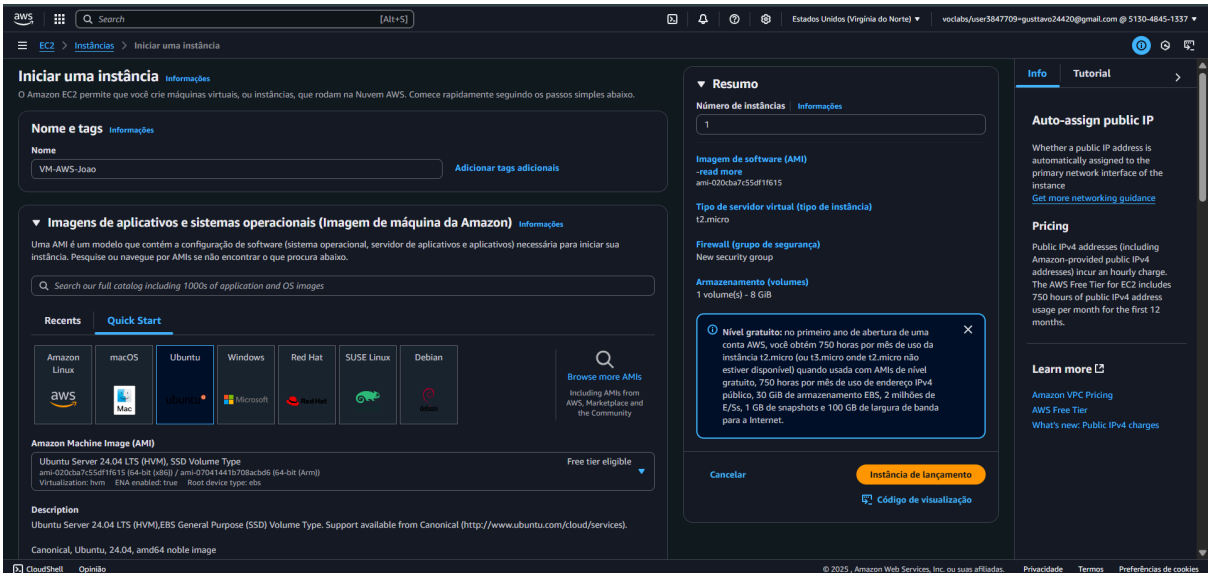
- Rede:VPC-AWS-Joao

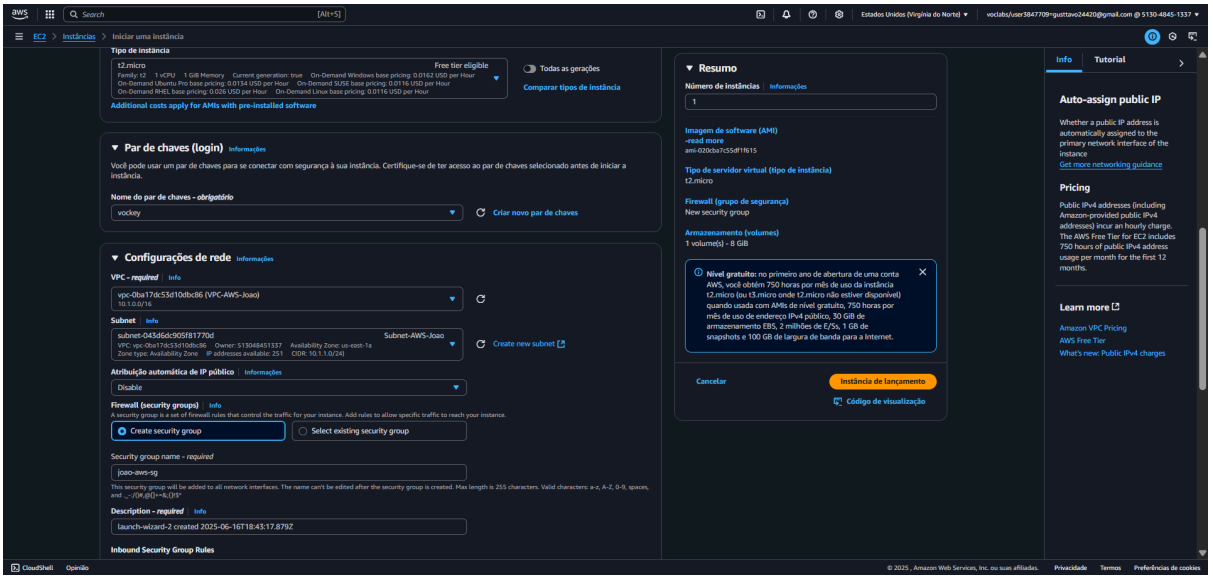
- Rede:Subnet-PRIV-AWS-Joao

- IP Publico:Desabilitado

-Grupo de Segurança:joao-aws-sg







- Nome:VM-AWS-Joao-pub

- ISO:Ubuntu Server 24.0

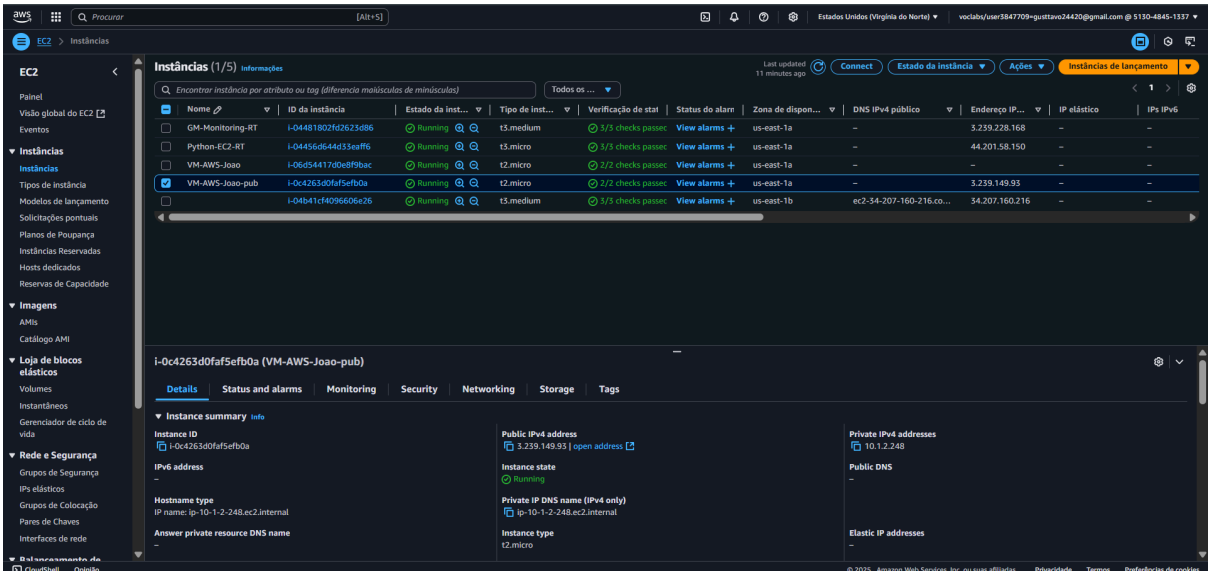
- Chave:Vockey

- Rede:VPC-AWS-Joao-pub

- Rede:Subnet-PUB-AWS-Joao

- IP Publico:Habilitado

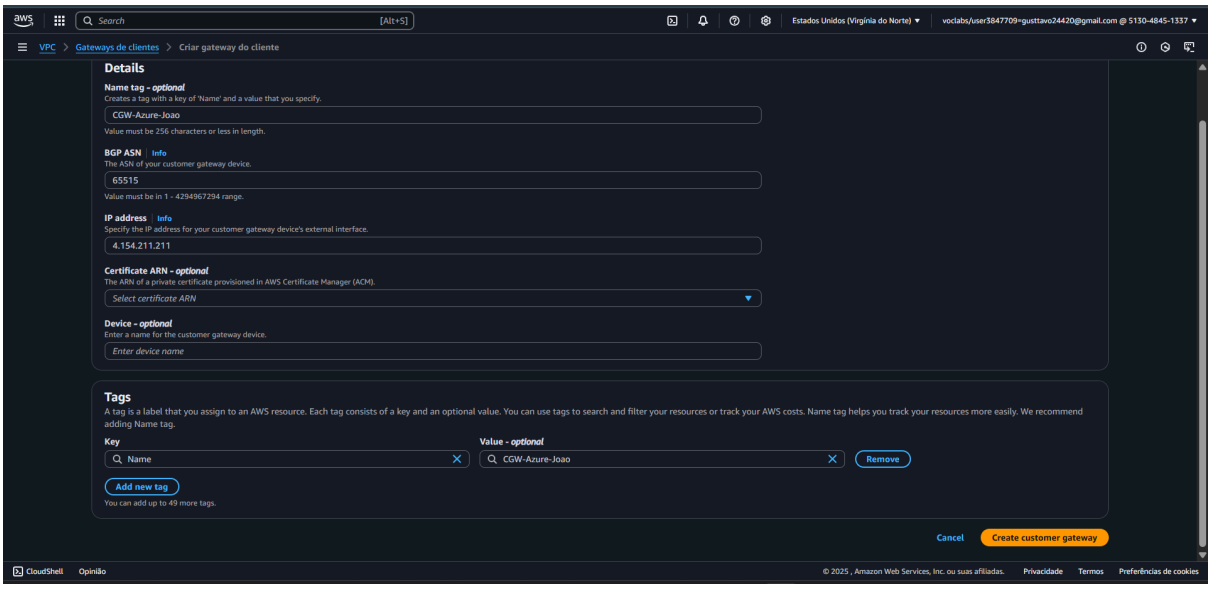
-Grupo de Segurança:joao-aws-sg



Criar um Customer Gateway apontando para o IP público do Azure VPN Gateway

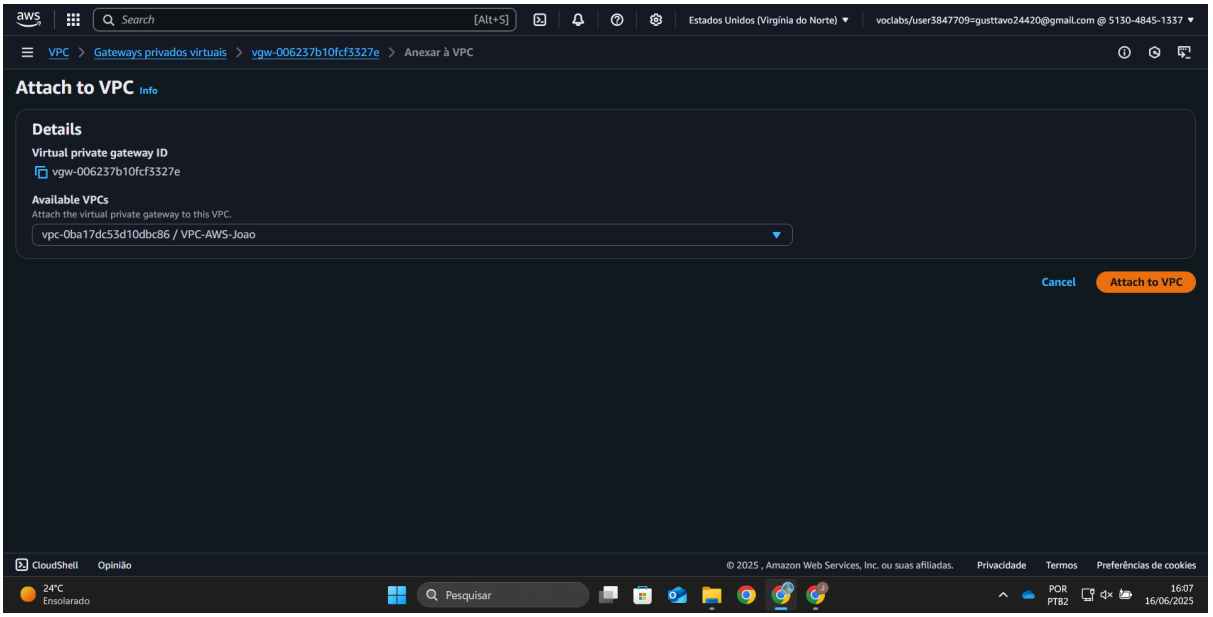
- Endereço IP: IP Público do Gateway VPN do Azure

- Demais configurações: Padrão



Criar o Virtual Private Gateway e anexar à VPC

- Nome: VGW-AWS-Joao



Criar a conexão Site-to-Site VPN

- Nome: vpn-aws-to-azure-Joao

- Tipo de gateway de destino: Virtual Private Gateway

- Customer Gateway: Existente

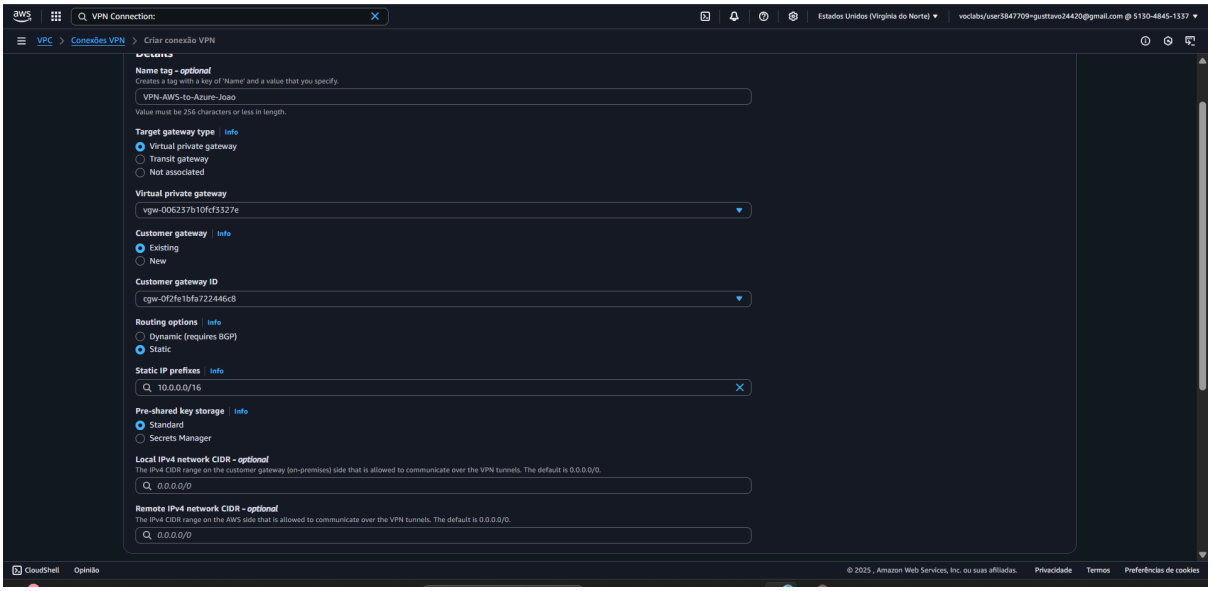
- Opções de roteamento: Estático

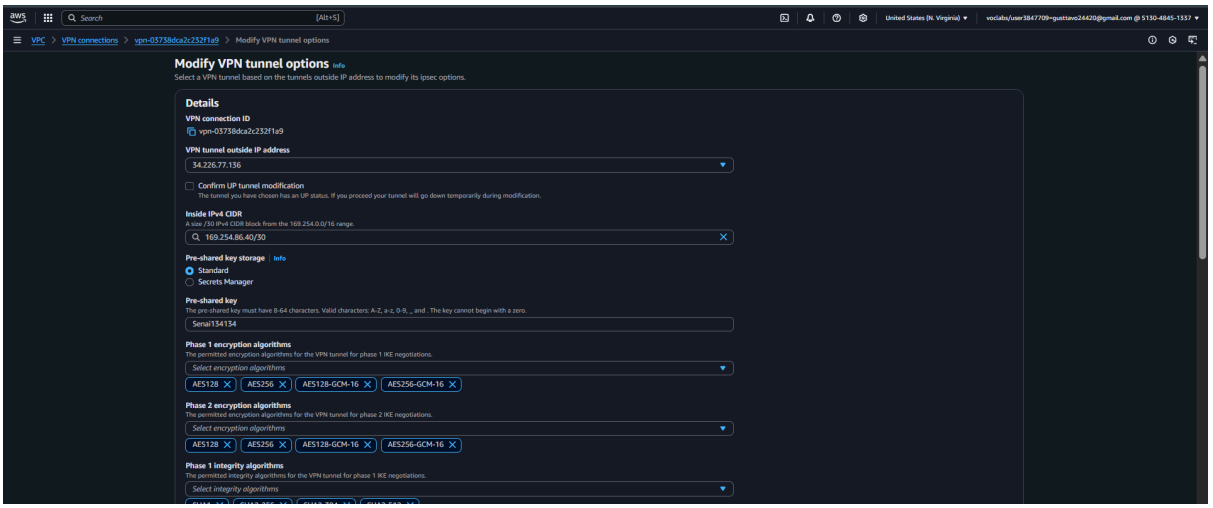
- Prefixos IP estáticos: 10.0.0.0/16

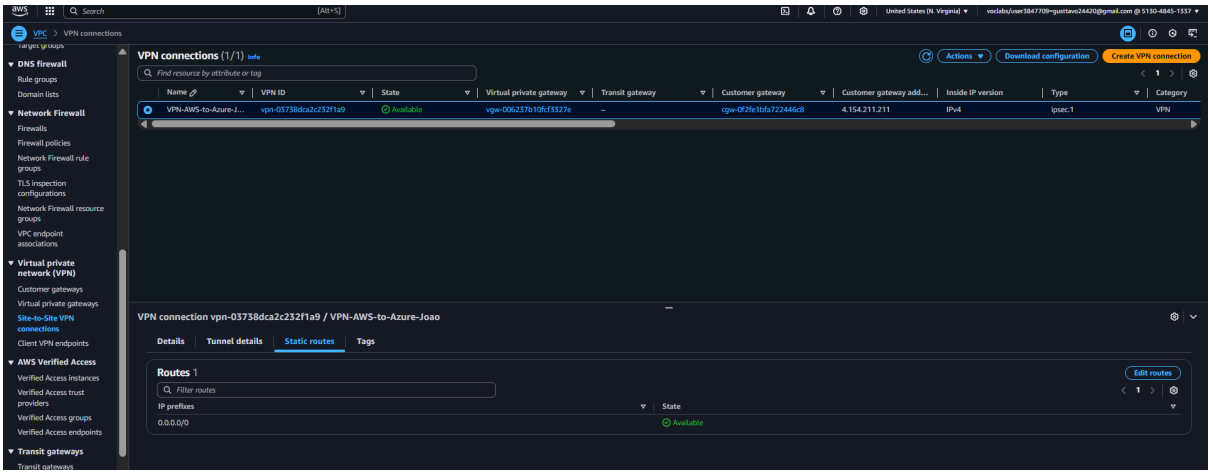
- Demais configurações: Padrão

- Pre-shared key: Mudar a senha

- Tabela de Rotas: Liberar rota

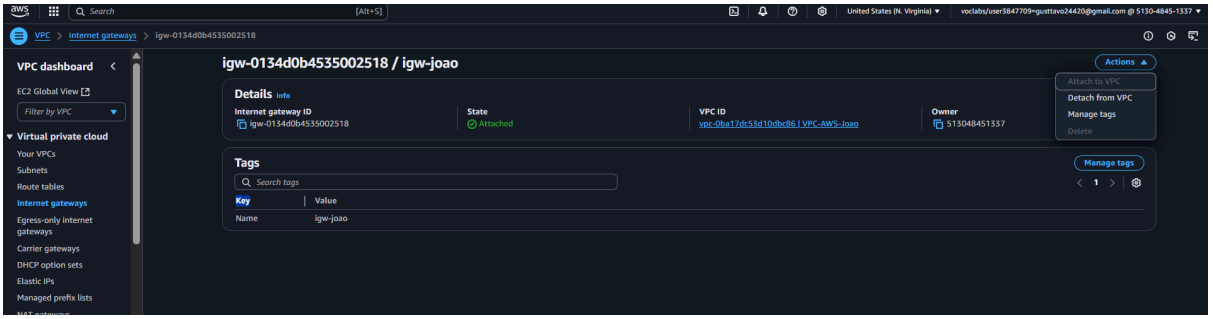






Criar Internet Gateway e anexar à VPC

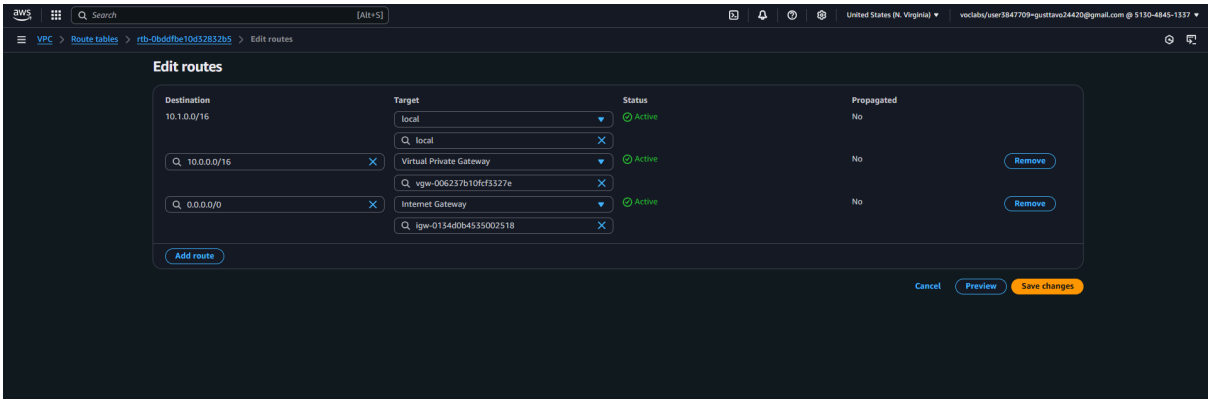
- Nome:igw-joao



Editar a tabela de rotas associada à VPC

- Destino: 10.0.0.0/24 - Target: Virtual Private Gateway

- Destino: 0.0.0.0/0 - Target: Internet Gateway



TESTAR A CONEXÃO

ubuntu@ip-10-1-1-224: ~

```
ubuntu@ip-10-1-1-224:~$ ping 10.0.1.4
PING 10.0.1.4 (10.0.1.4) 56(84) bytes of data.
64 bytes from 10.0.1.4: icmp_seq=1 ttl=64 time=70.5 ms
64 bytes from 10.0.1.4: icmp_seq=2 ttl=64 time=70.3 ms
64 bytes from 10.0.1.4: icmp_seq=3 ttl=64 time=70.1 ms
64 bytes from 10.0.1.4: icmp_seq=4 ttl=64 time=70.3 ms
64 bytes from 10.0.1.4: icmp_seq=5 ttl=64 time=71.6 ms
```

senai@VM-joao: ~

```
senai@VM-joao:~$ ping 10.1.1.224
PING 10.1.1.224 (10.1.1.224) 56(84) bytes of data.
64 bytes from 10.1.1.224: icmp_seq=1 ttl=64 time=70.1 ms
64 bytes from 10.1.1.224: icmp_seq=2 ttl=64 time=70.2 ms
64 bytes from 10.1.1.224: icmp_seq=3 ttl=64 time=70.7 ms
64 bytes from 10.1.1.224: icmp_seq=4 ttl=64 time=71.2 ms
```

ubuntu@ip-10-1-1-224: ~

```
ubuntu@ip-10-1-2-248:~$ ssh -i 'labsuser (1).pem' ubuntu@10.1.1.224
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-1029-aws x86_64)

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

 System information as of Tue Jun 17 18:04:18 UTC 2025

  System load:  0.08              Processes:             104
  Usage of /:   25.7% of 6.71GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for enX0: 10.1.1.224
  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: Tue Jun 17 18:04:19 2025 from 10.1.2.248
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-1-1-224:~$
```

senai@VM-joao: ~

```
ubuntu@ip-10-1-2-248:~$ ssh senai@10.0.1.4
senai@10.0.1.4'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 Tue Jun 17 18:05:01 UTC 2025

  System load:  0.02              Processes:             134
  Usage of /:   5.6% of 28.02GB   Users logged in:       0
  Memory usage: 7%                IPv4 address for eth0: 10.0.1.4
  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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check y
our Internet connection or proxy settings


Last login: Tue Jun 17 17:47:45 2025 from 10.1.2.248
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

senai@VM-joao:~$
```

ubuntu@ip-10-1-1-224: ~

```
ubuntu@ip-10-1-1-224:~$ ping 10.0.1.4
PING 10.0.1.4 (10.0.1.4) 56(84) bytes of data.
64 bytes from 10.0.1.4: icmp_seq=1 ttl=64 time=70.5 ms
64 bytes from 10.0.1.4: icmp_seq=2 ttl=64 time=70.3 ms
64 bytes from 10.0.1.4: icmp_seq=3 ttl=64 time=70.1 ms
64 bytes from 10.0.1.4: icmp_seq=4 ttl=64 time=70.3 ms
64 bytes from 10.0.1.4: icmp_seq=5 ttl=64 time=71.6 ms
```

senai@VM-joao: ~

```
senai@VM-joao:~$ ping 10.1.1.224
PING 10.1.1.224 (10.1.1.224) 56(84) bytes of data.
64 bytes from 10.1.1.224: icmp_seq=1 ttl=64 time=70.1 ms
64 bytes from 10.1.1.224: icmp_seq=2 ttl=64 time=70.2 ms
64 bytes from 10.1.1.224: icmp_seq=3 ttl=64 time=70.7 ms
64 bytes from 10.1.1.224: icmp_seq=4 ttl=64 time=71.2 ms
```