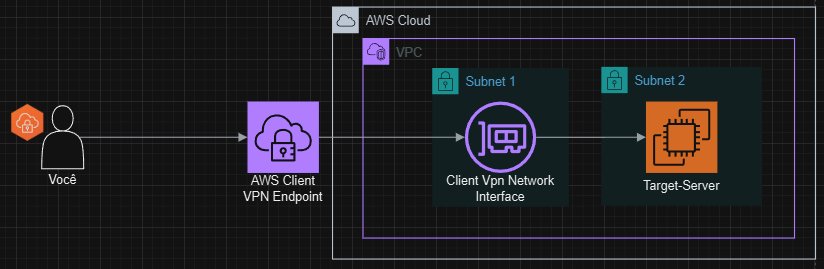
**AWS VPN: Conectividade Segura com a Nuvem**

O **AWS VPN** oferece soluções seguras para conectar redes locais, escritórios remotos e dispositivos à infraestrutura global da AWS. Ele inclui dois serviços principais:

* **AWS Site-to-Site VPN:** ideal para conexões seguras entre redes locais e a AWS.
* **AWS Client VPN:** permite que usuários se conectem a recursos na AWS ou on-premises usando um cliente de software VPN.

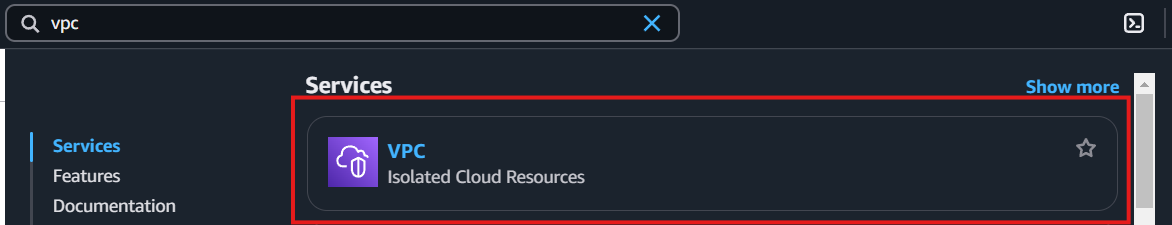
**Referencia:** https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/client-auth-mutual-enable.html

Essas soluções são gerenciadas, altamente disponíveis e escaláveis, garantindo segurança e simplicidade no tráfego de rede.

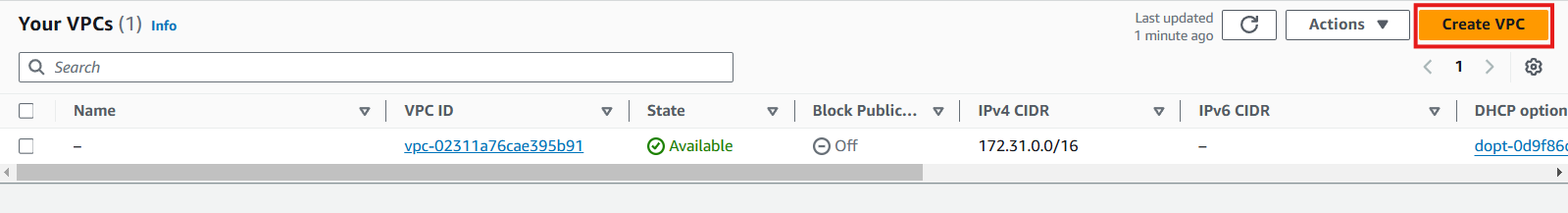


### **Configurando uma VPC para a VPN.**

Para criar uma VPN Client na AWS, você precisa configurar uma **Virtual Private Cloud (VPC)**. Siga as etapas abaixo:

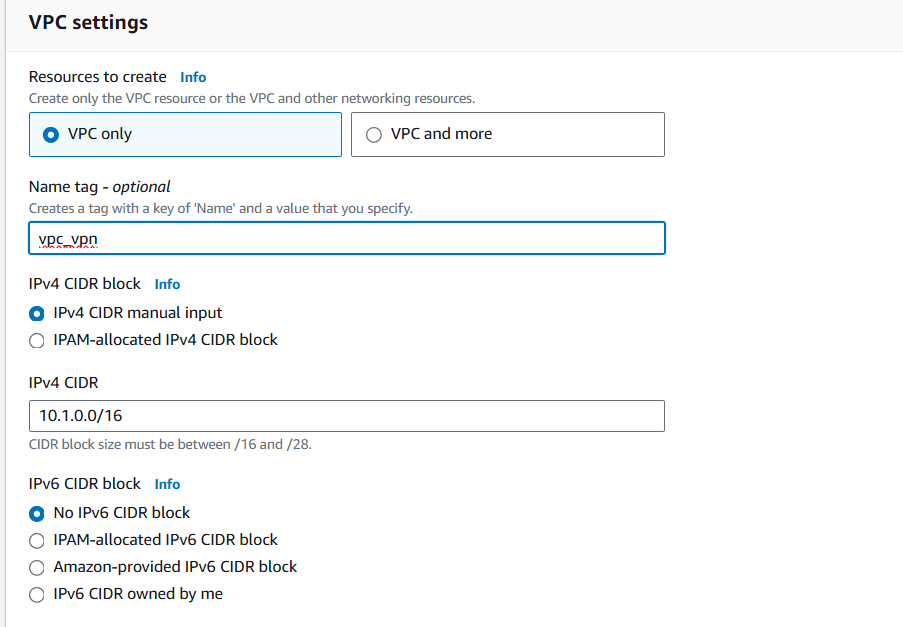


Agora dentro do console da VPC vamos criar uma rede virtual para servir de acesso para nossa VPN.

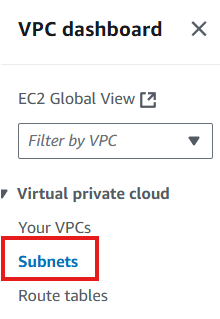


Dentro do console clique **Create VPC** e deixe selecionado como **VPC only**, agora dentro da parte do VPC settings colocar:

* **Nome:** vpc\_vpn
* **IPv4 Cidr:** 10.1.0.0/16

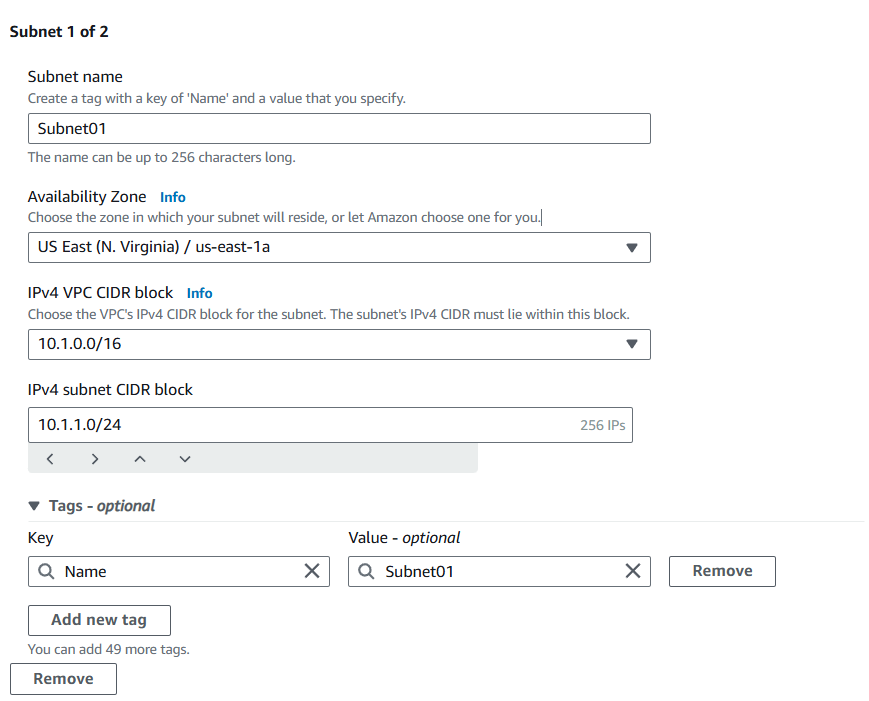


Com isso, temos que criar duas subnets para utilizar no ambiente, ainda dentro do console em baixo de **Suas VPCs** e clicar em **Subnets.**



Dentro do console clique **Create Subnet**, agora dentro do **VPC ID** selecionar a **VPC** criada anteriormente, e em subnet configurar ela assim:

* **Nome:** Subnet01
* **IPv4 Cidr:** 10.1.1.0/24
* **Availability Zone:** us-east-1a



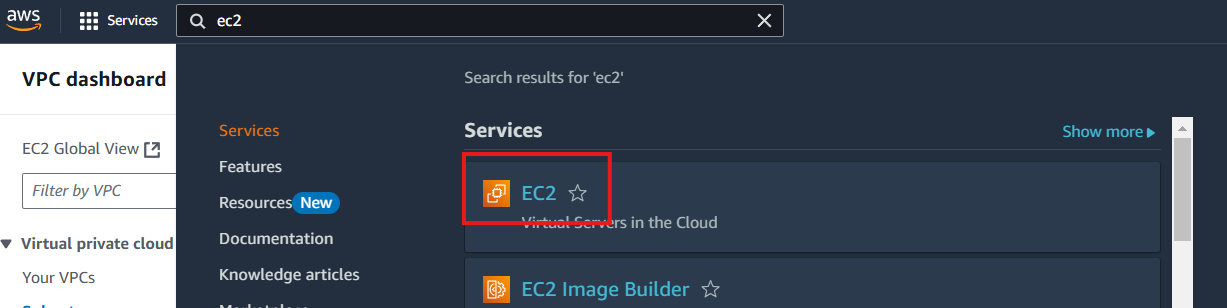
Repita esse processo para uma outra Subnet:

* **Nome:** Subnet02
* **IPv4 Cidr:** 10.1.2.0/24
* **Availability Zone:** us-east-1b

Agora no total temos uma VPC já configurada e duas Subnets em duas zonas diferentes.

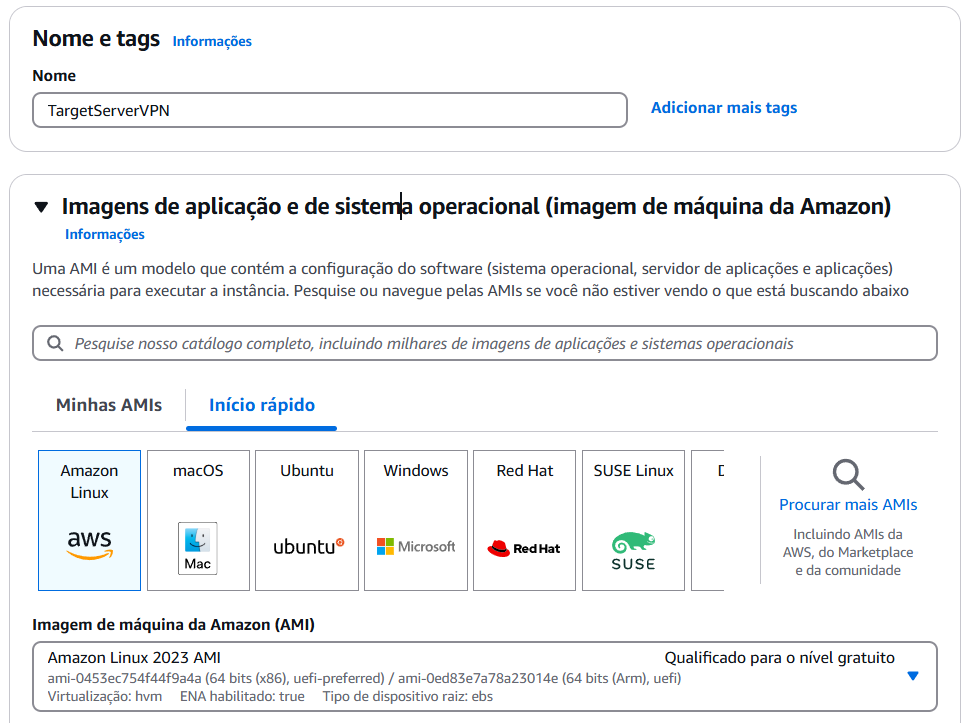
### **Configurando a EC2 Target-Server.**

No console da AWS procure por EC2 e clique nela.

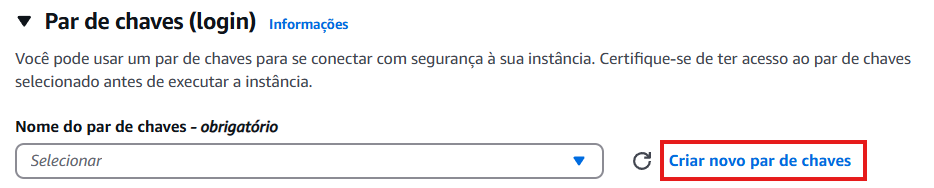


Já dentro do console procure por Instâncias e clique em **Executar instâncias**, já dentro da configuração siga os passos abaixo:

* **Nome:** TargetServerVPN
* **Imagem:** Amazon Linux 2023
* **Tipo de instância:** t2.micro



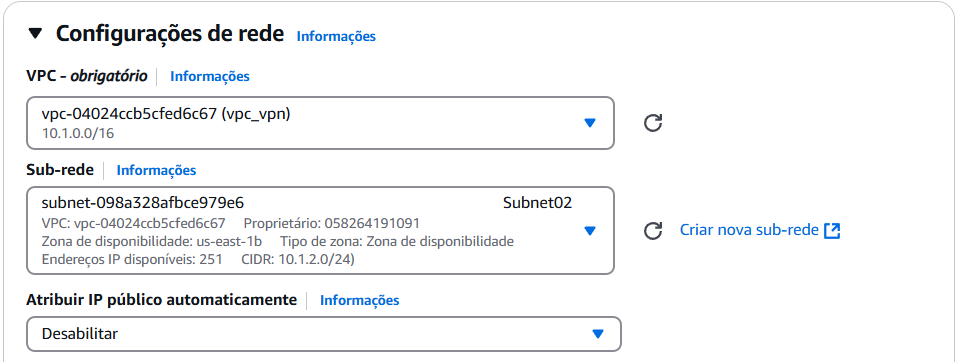
Em Par de chaves crie uma para sua instância.



Na parte da configuração da chave, coloque:

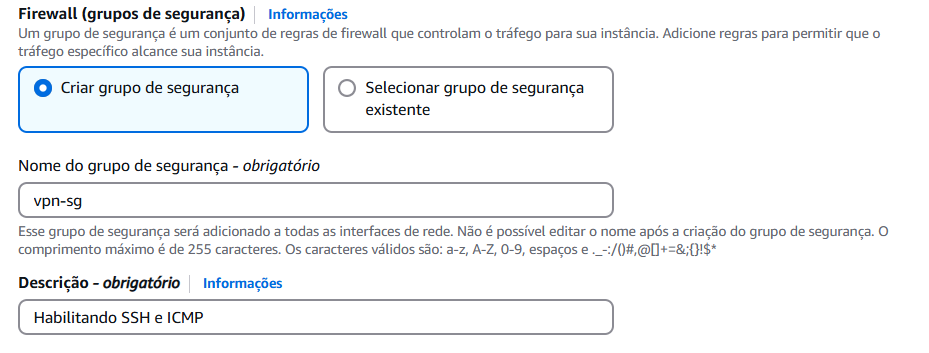
* **Nome:** pairkey
* **Tipo da chave:** .pem

Na parte de Configurações de rede selecionar a vpc criar anteriormente e a Subnet02.



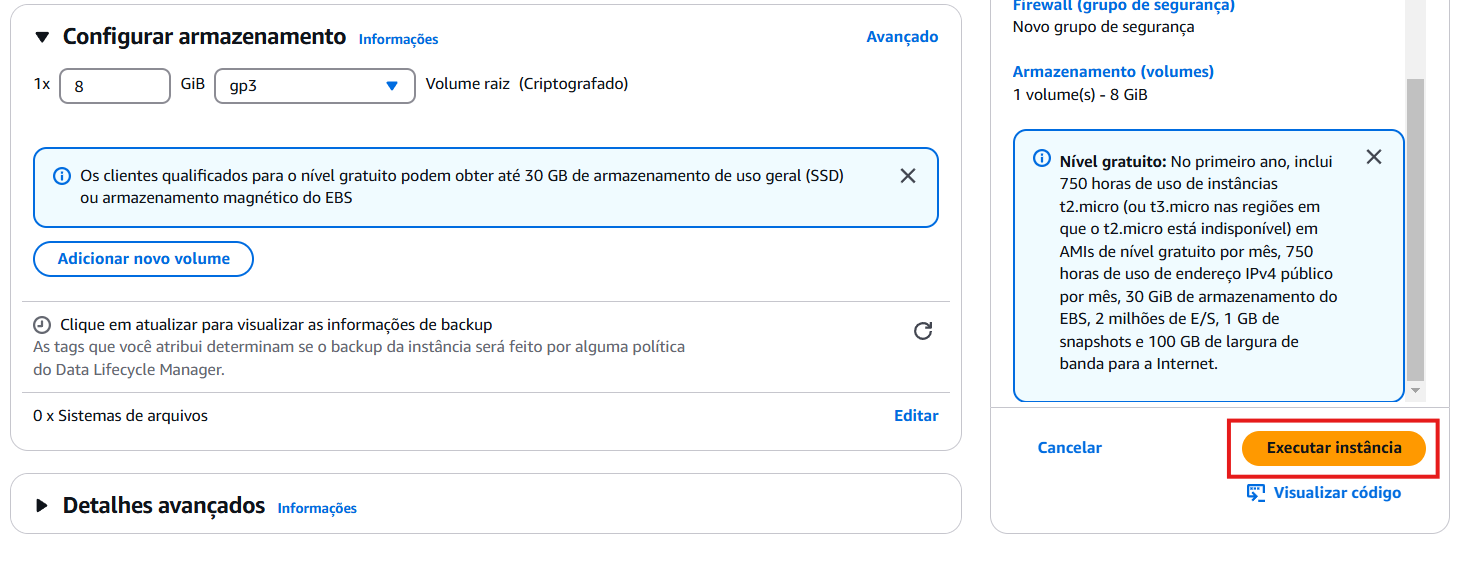
Na configuração do SG coloque **Criar grupo de segurança** e coloque as seguintes configurações:

* **Nome:** vpn-sg
* **Descrição:** Habilitando SSH e ICMP
* **Regras:** SSH e ICMP

****

****

E clique em executar as instâncias.

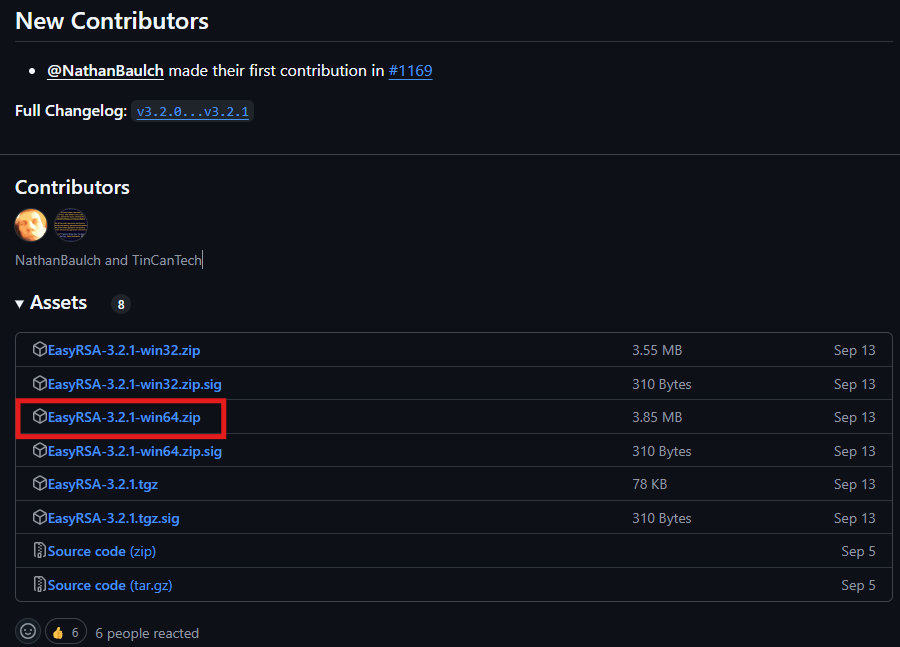


**Certificados**

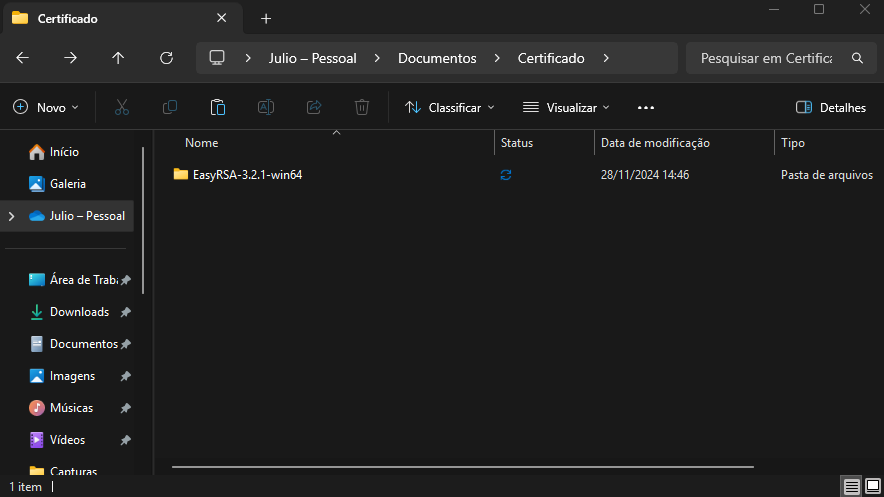
<https://github.com/OpenVPN/easy-rsa/releases>

<https://github.com/OpenVPN/easy-rsa/releases/download/v3.2.1/EasyRSA-3.2.1-win64.zip>

Agora vamos precisar de um certificado para o cliente e um para o server que vamos ter que usar para criar nossa vpn.

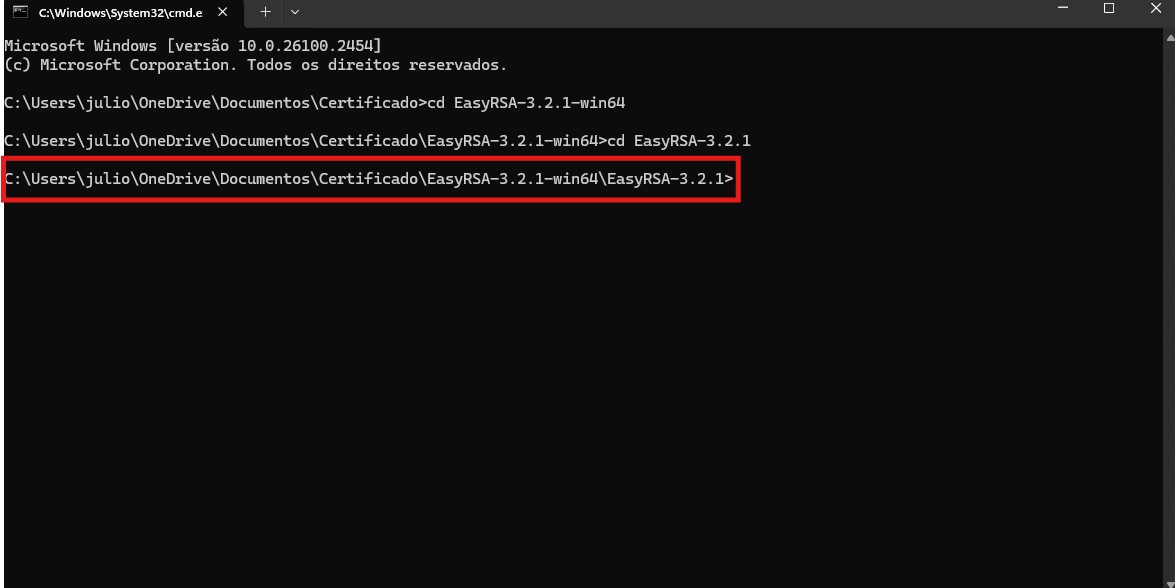


Com isso precisamos criar uma pasta localmente para servir de armazenamento para nosso certificado e precisamos colocar o arquivo já extraído da instalação do nosso certificado.



agora com o arquivo da rsa precisamos executar esse arquivo vamos seguir esse caminho para achar o arquivo. ( no meu caso foi: C:\Users\Julio\OneDrive\Documents\Certificado\EasyRSA-3.2.1-win64\EasyRSA-3.2.1.)

Mas fique livre para criar uma pasta da sua escolha em qualquer lugar, a única coisa importante é ter o arquivo EasyRSA descompactado dentro dessa pasta.

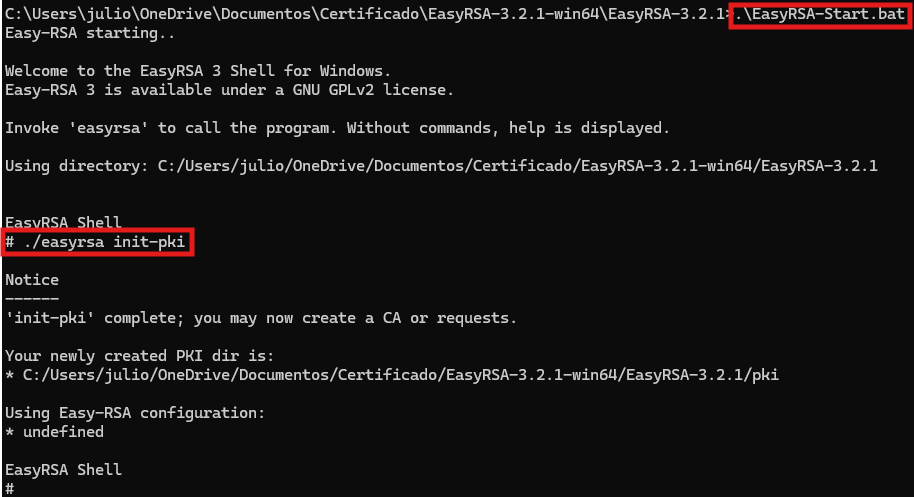


Com isso agora podemos executar o arquivo a seguir segue o comando para executar o arquivo dentro da pasta:

.\EasyRSA-Start.bat

Com isso agora já dentro do software precisamos colocar esse comando para iniciar nosso software:

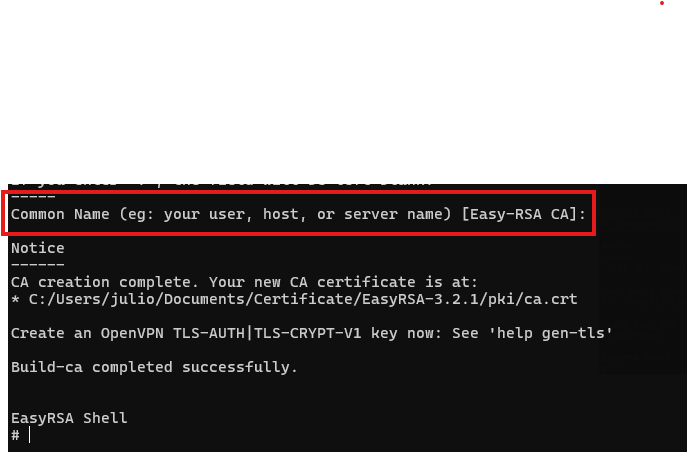
./easyrsa init-pki



Agora gerando a rsa:

./easyrsa build-ca nopass

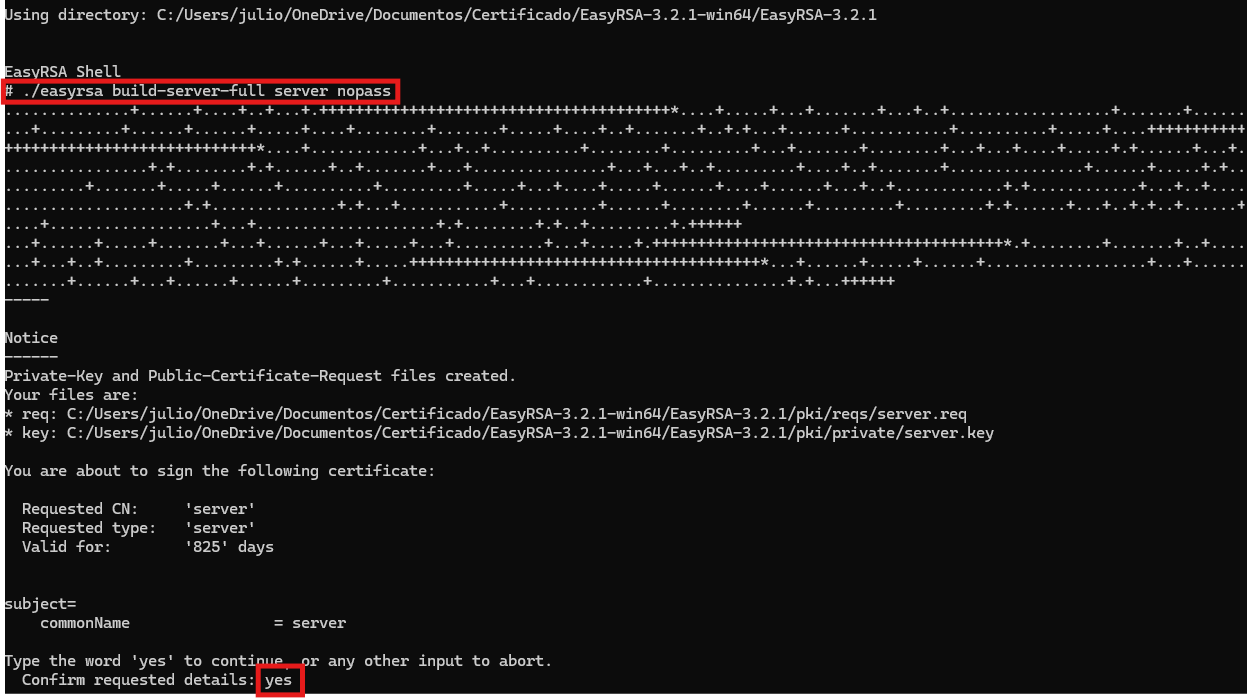
Na parte do Common Name podemos seguir deixando em branco mesmo.



Agora colocamos esse comando:

./easyrsa --san=DNS:server build-server-full server nopass

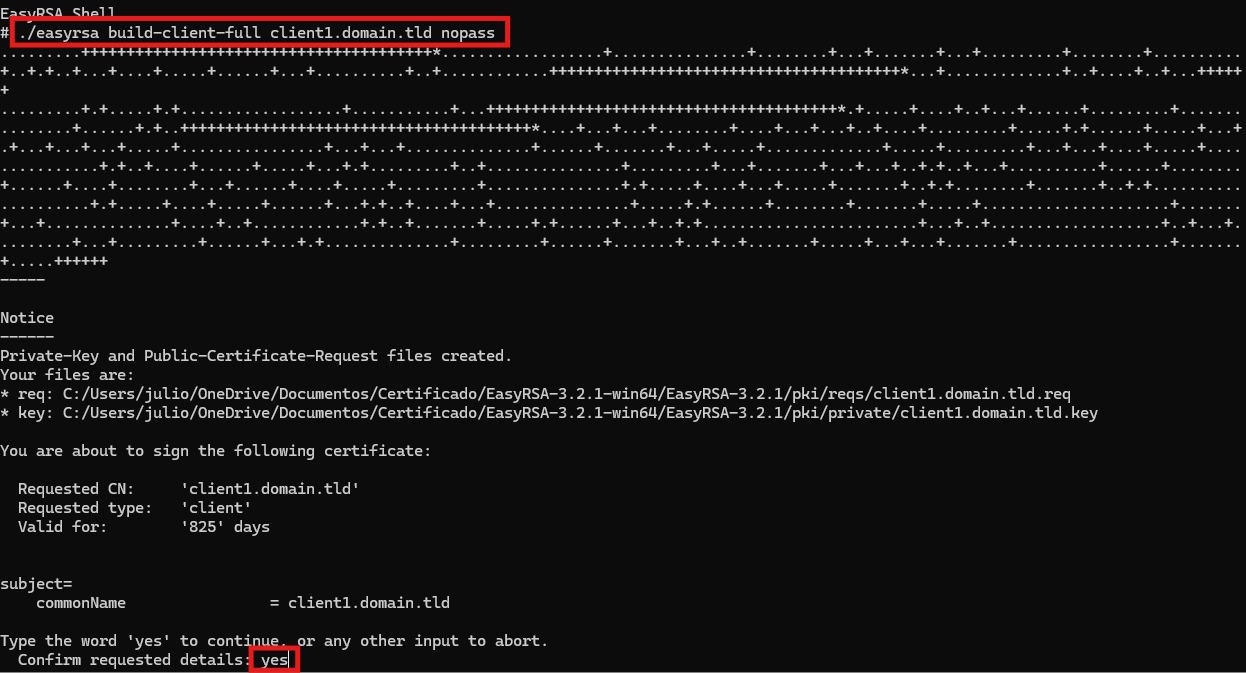
No prompt colocar yes.



Continuando para o último comando:

./easyrsa build-client-full client1.domain.tld nopass

No prompt colocar yes.



Só sair com o exit

**Comandos:**

.\EasyRSA-Start.bat

./easyrsa init-pki

./easyrsa build-ca nopass

./easyrsa --san=DNS:server build-server-full server nopass

./easyrsa build-client-full client1.domain.tld nopass

exit

Agora dentro o diretório podemos colocar esses comandos para organização dos nossos certificados:

**Comandos:**

mkdir vpncert

copy pki\ca.crt vpncert

copy pki\issued\server.crt vpncert

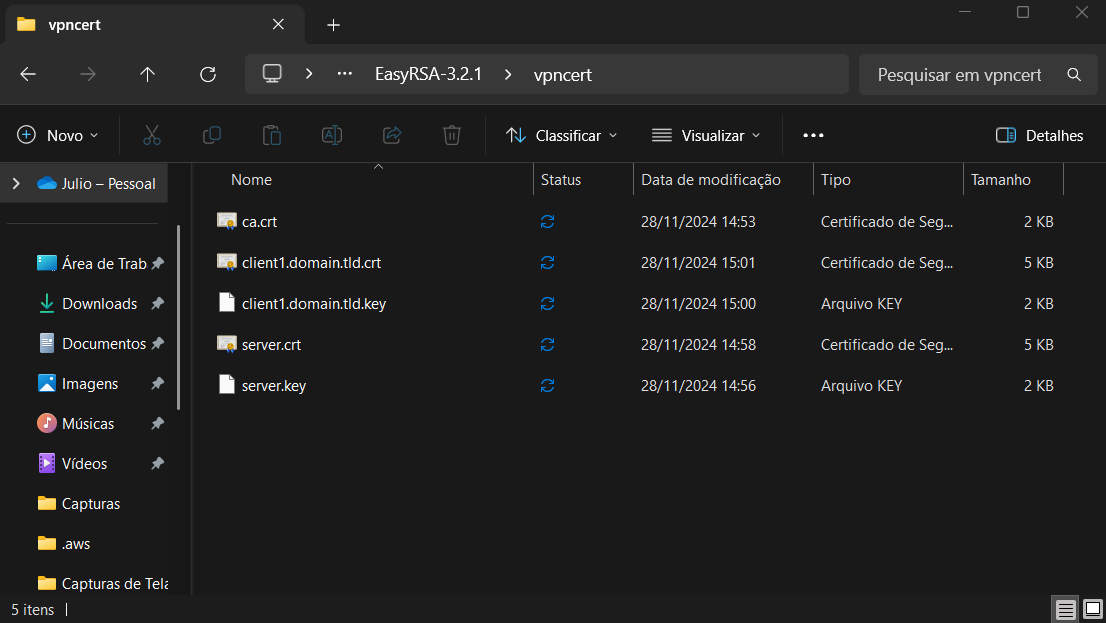
copy pki\issued\client1.domain.tld.crt vpncert

copy pki\private\server.key vpncert

copy pki\private\client1.domain.tld.key vpncert

cd vpncert

Agora dentro da pasta podemos ver nossos certificados que usaremos dentro da nossa vpn.



Voltando para dentro da AWS precisamos utilizar o certificate manager para importar esse certificado, na aba da AWS precisamos procurar pelo certificate manager.

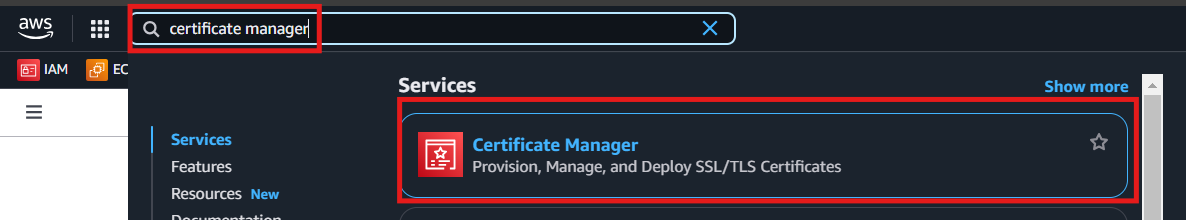
obs: podemos também importar os certificados pela AWS CLI ficando bem mais fácil, só iremos precisar que a AWS CLI esteja configurada e conectada a sua AWS.

**Comandos – AWS CLI:**

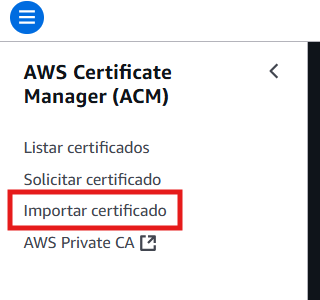
aws acm import-certificate --certificate fileb://server.crt --private-key fileb://server.key --certificate-chain fileb://ca.crt

aws acm import-certificate --certificate fileb://client1.domain.tld.crt --private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt

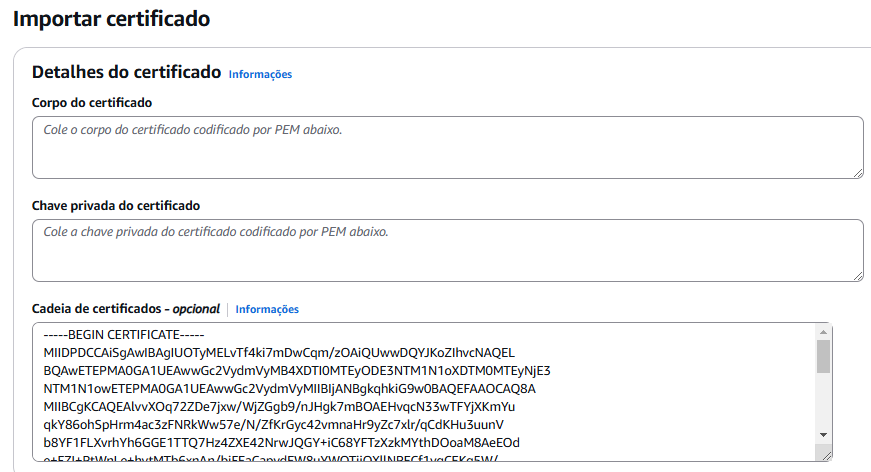
**Passo a passo – AWS:**



agora já dentro do acm vamos importar nosso certificado



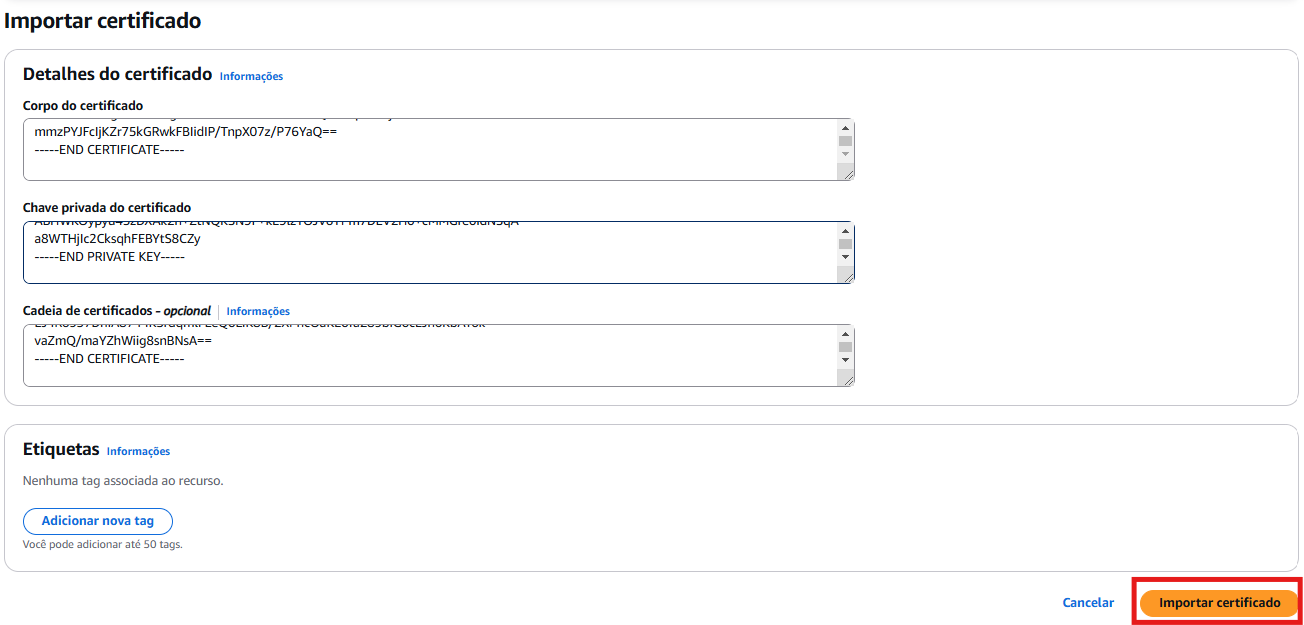
Agora dentro da pasta vpncert pegar o conteúdo dos arquivos **ca.cert** e colocar na cadeia de certificados.



Agora precisamos pegar o **server.cert** e precisamos colocar ele dentro do corpo do certificado.



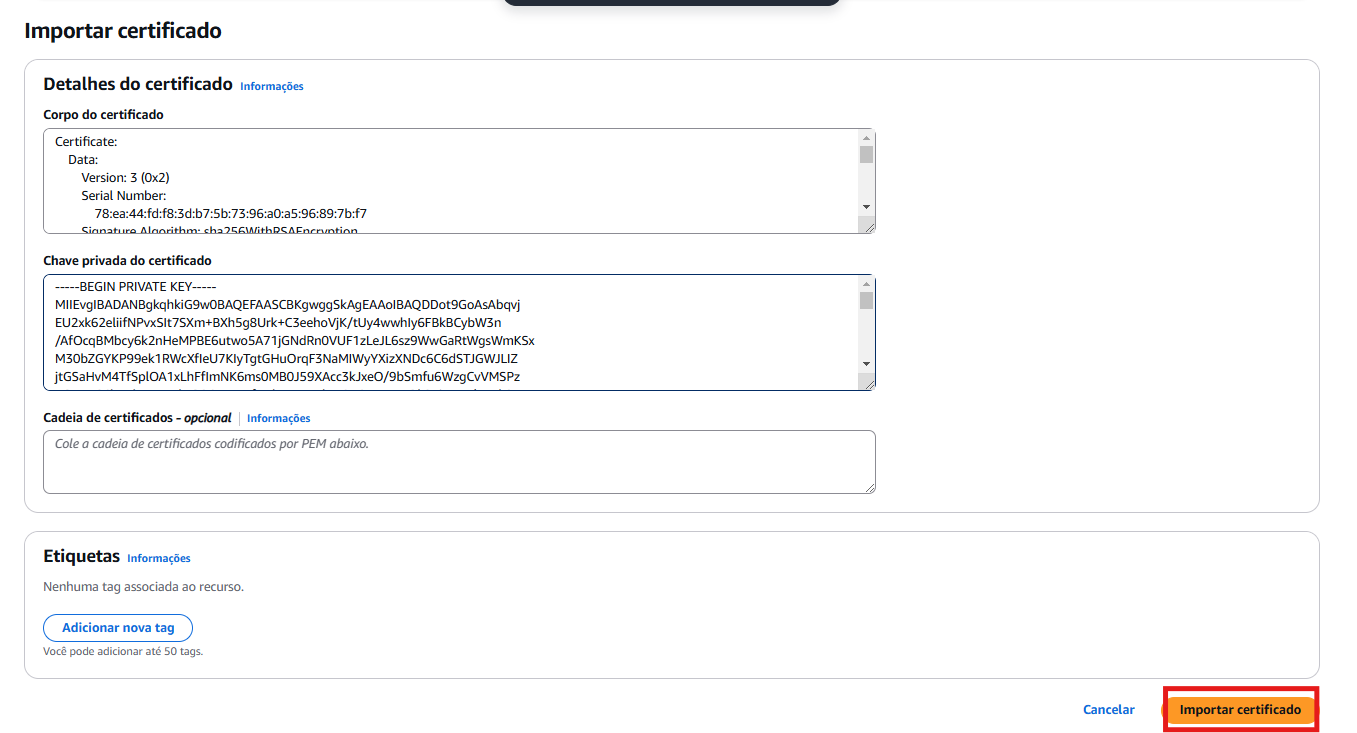
E no final precisamos colocar a **server.key** dentro desse certificado, depois disso daí podemos clicar em importar certificado.



Depois disso vamos ter que importar outro certificado para dentro do certificate manager de novo em importar certificado, e vamos adicionar esses dois arquivos respectivamente o **client1.domain.tld.cert** como corpo do certificado e **client1.domain.tld.key** como chave privada do certificado dentro do certificado.



Ficando assim e já podemos importar esse certificado:



**Listar certificados:**

Em AWS Certificate Manager (ACM) clique em “Listar certificados”.

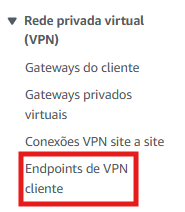
Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

**VPN**

Com isso já podemos criar nossa cliente VPN

Voltando para o console da VPC podemos acessar a aba de VPN para se criar uma VPN cliente para se utilizar como uma conexão ssh de nossa máquina local para a AWS.



Nele vamos clicar em criar um endpoint para a vpn



Agora na configuração vamos utilizar esses passos:

**Nome:** client-vpn

Client IPv4 CIDR: 192.168.0.0/16

Na parte dos Certificates habilitar o usar **autenticação mútua** depois

- colocar o server como primeiro certificado

- o client como segundo.

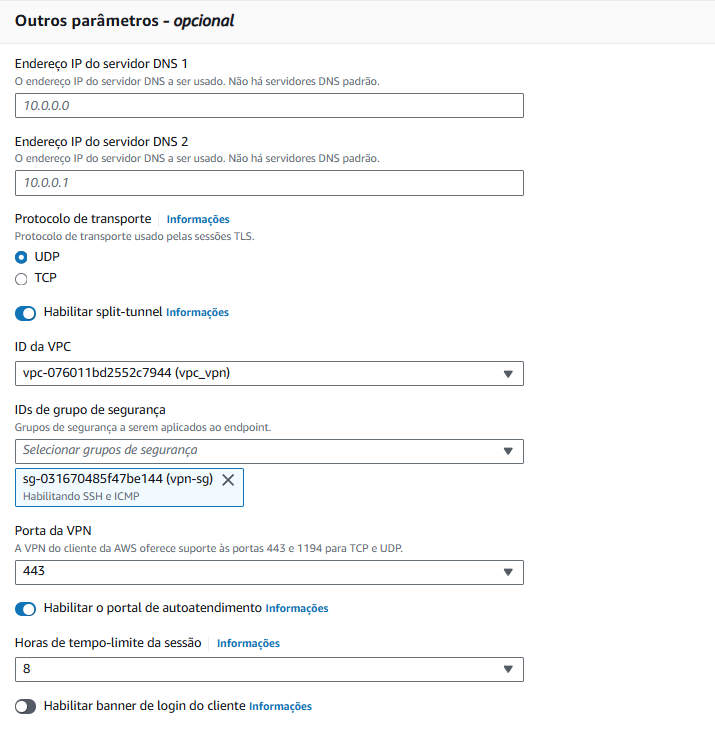


Na aba de outros parâmetros vamos definir que nossa VPN

- use um **split-tunnel** e selecione a VPC-vpn (criada anteriormente)

- escolher o grupo de segurança **vpn-sg**

- habilitar a **Habilitar o portal de autoatendimento.**

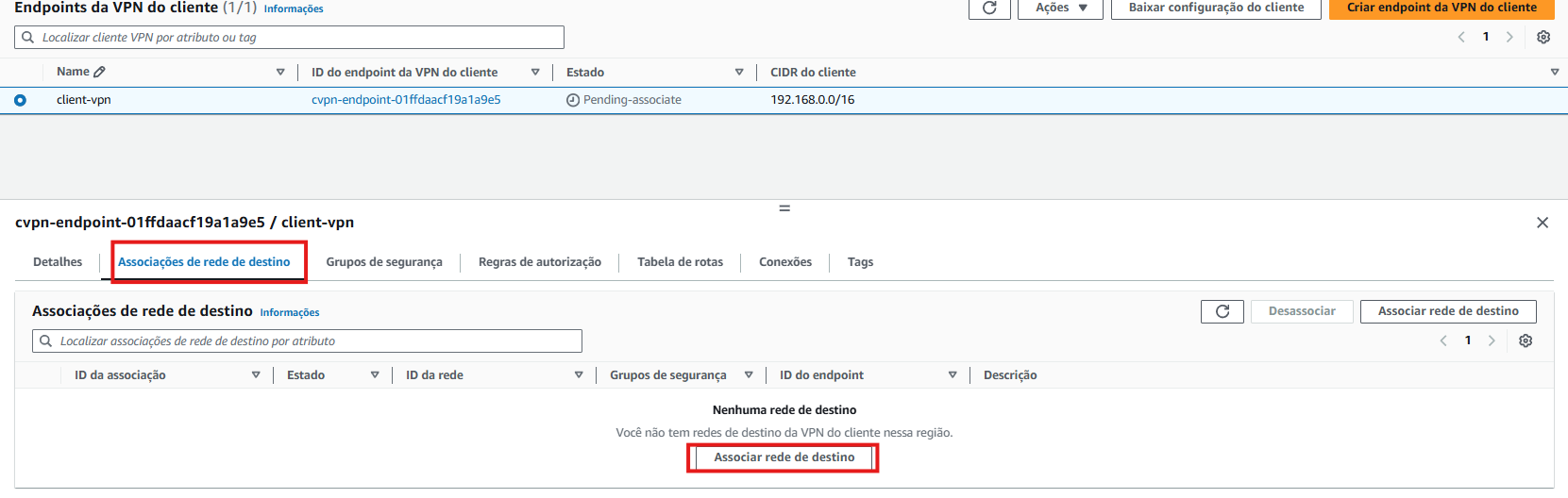


Clique em

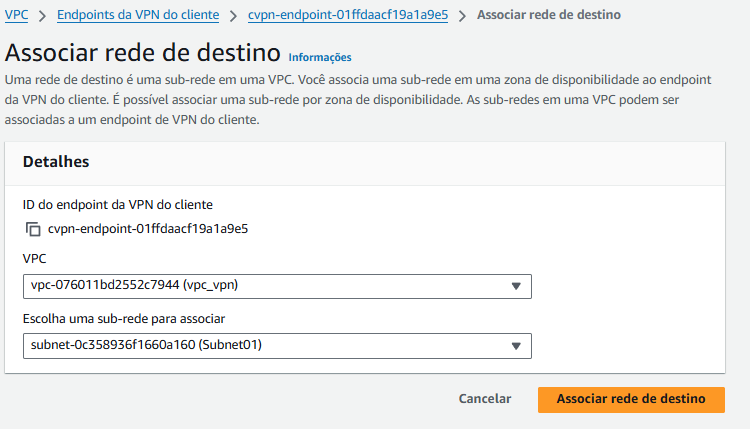


Clicando sobre a “cliente-vpc”

Podemos acessar as associações de rede de destino e podemos clicar em associar rede de destino.



Nela vamos indicar nossa vpc e colocar a **Subnet01.**

****

Agora vamos criar uma regra de autorização para nossa VPN.



Na configuração vamos colocar o CIDR da nossa vpc e deixar permitir acesso a todos os usuários.

Tela de celular com publicação numa rede social

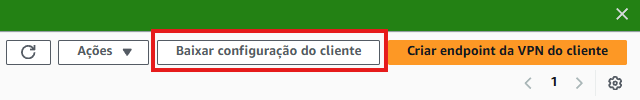
Descrição gerada automaticamente

Vamos precisar esperar as regras e associações serem criadas.

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

Podemos Baixar as configurações do client.



Com esse arquivo baixado vamos ter que editar ele como bloco de notas e ajustá-lo.



No final do arquivo, depois do (verify-x509-name server name) vamos adicionar essas linhas com o espaço:

<cert>

</cert>

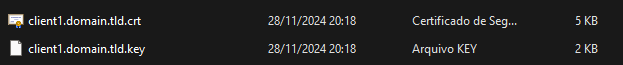
<key>

</key>

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Dentro das chaves vamos colocar o conteúdo do certificado e a key do cliente dentro das chaves <key> XXXXX </key>



Esses dois arquivos respectivamente.

Texto

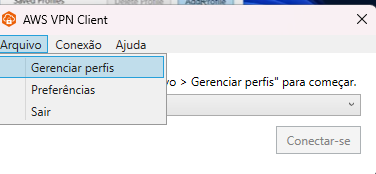
Descrição gerada automaticamente

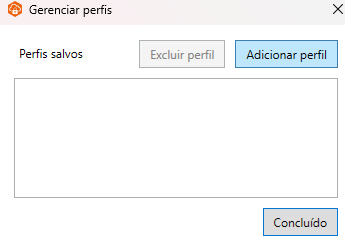
**ACESSANDO:**

Precisamos de software para se conectar a essa vpn o aws client vpn pode baixar ele acessando o link em baixo.

<https://aws.amazon.com/pt/vpn/client-vpn-download/>

com ele aberto vamos ir em arquivo e em gerenciar perfis.



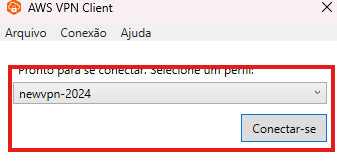


Nele vamos clicar em Adicionar perfil.

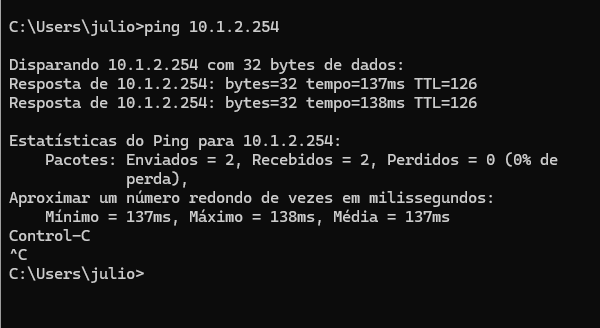


adicionando vamos colocar o nome de exibição e em arquivo vamos colocar o arquivo recém configurado.

Depois só Conectar-se.



Com isso podemos pegar nosso private ipv4 address da nossa máquina e testar o ping nele.



**Teste também conexão SSH.**