Professor: Danilo Sibov

**Cloud Computing | Aula 17**

**Introdução ao AWS Command Line**

Este módulo aborda os seguintes tópicos:

**Laboratório 1 –** Instalação do MSI Amazon CLI v2  
**Laboratório 2 –** Configurar Ambiente local com o Amazon CLI v2

**Laboratório 3** – Criar uma VPC Publica 1 - AZ1a e VPC Publica 2 - AZ1a e Criar Grupo de Segurança

**Laboratório 4** – Criar par de chaves, localizar imagens e Criar um Linux da máquina local

**Laboratório 5** – Criar um Windows Cliente da máquina local

**Referência Bibliográfica**

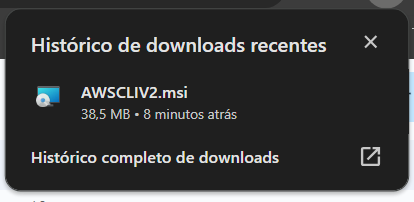
* Acesso ao Conteúdo AWS

<https://docs.aws.amazon.com/pt_br/cli/latest/userguide/getting-started-install.html>

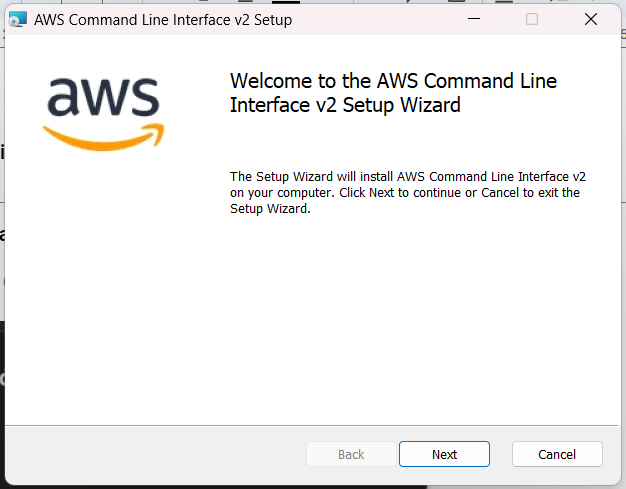
* Baixar e executar o instalador MSI da AWS CLI para Windows  
  <https://awscli.amazonaws.com/AWSCLIV2.msi>

**Laboratório 1 -** Instalação do MSI – Amazon CLI v2

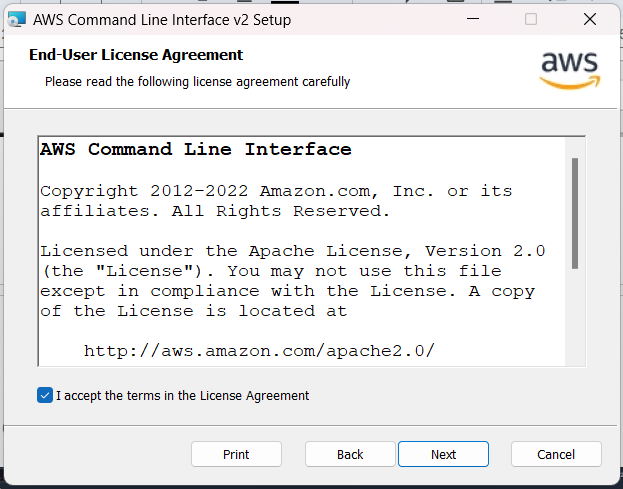
**Etapa 1 –** Clique no Link de Instalação e execute o instalador

****

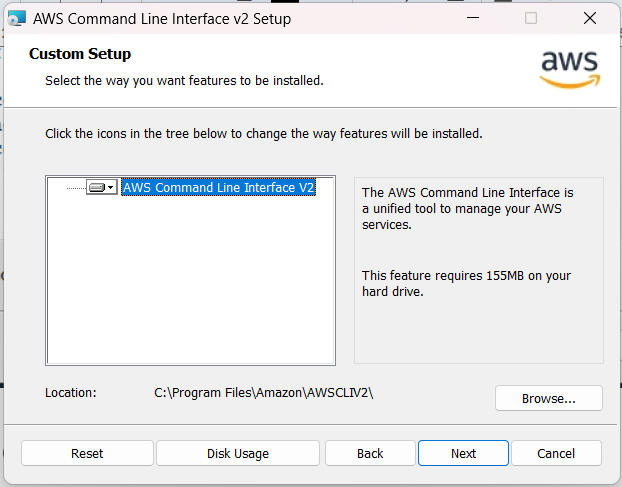
**Etapa 2 –** Clique em Next



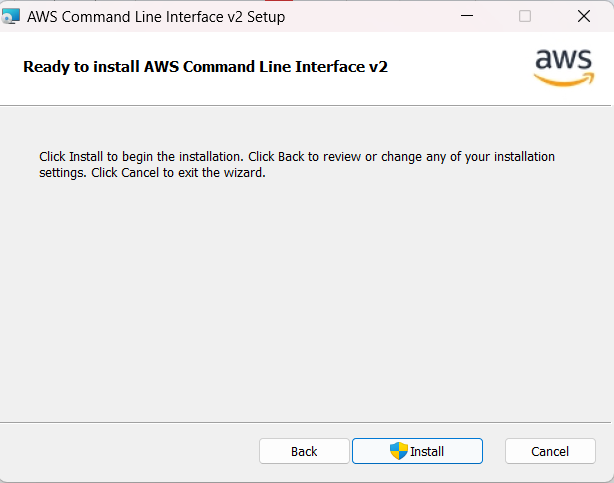
**Etapa 3 –** Aceite os termos e clique em Next



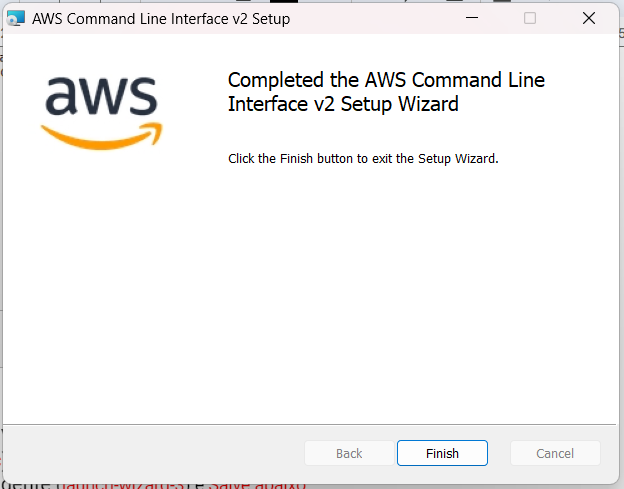
**Etapa 4 –** Clique em Next



**Etapa 5** **–** Clique em Install



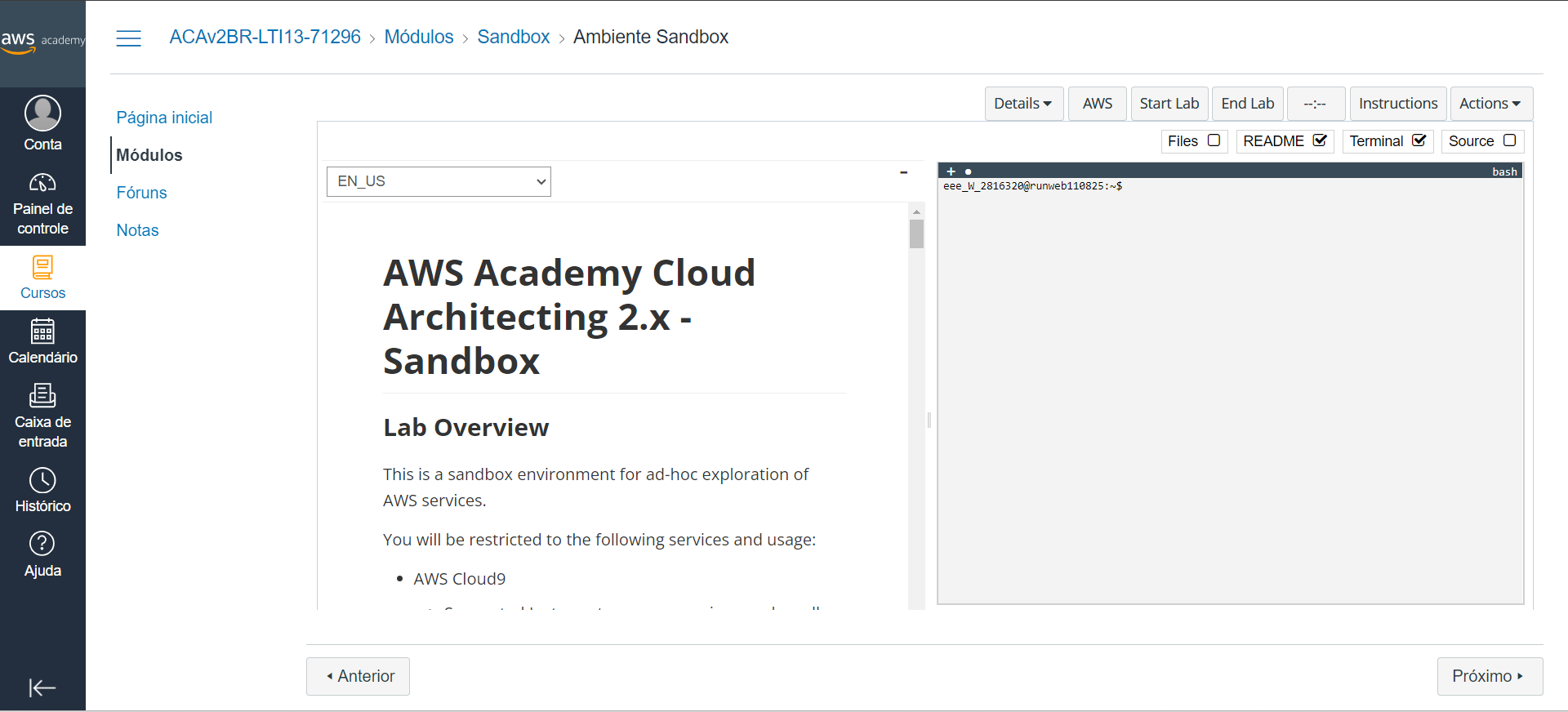
**Etapa 6** **–** Finalize a instalação clicando em Finish

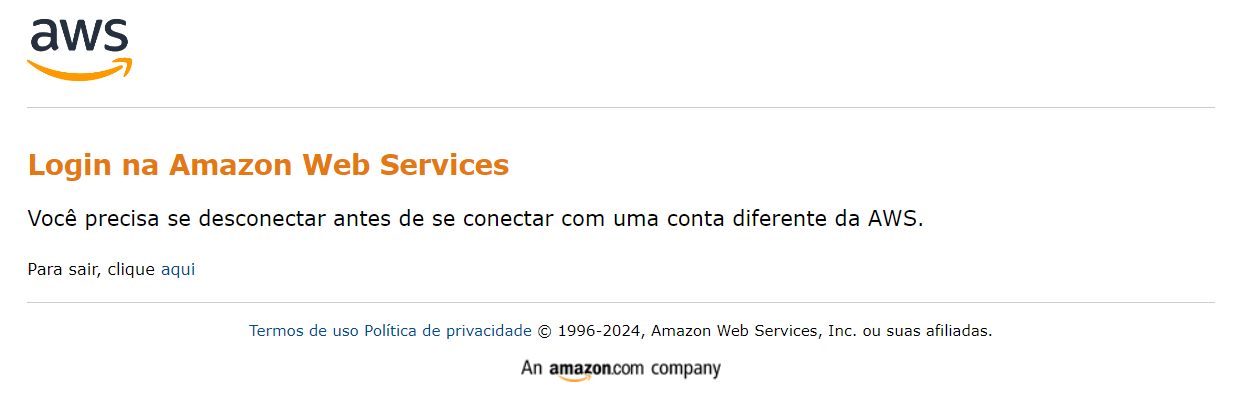


**Laboratório 2 -** Configurar Ambiente local com o Amazon CLI v2

**Etapa 1** **–** Abra O Laboratório ( **Ambiente Sandbox** ) o curso **AWS Academy Cloud Architecting** e clique em **Start Lab**,

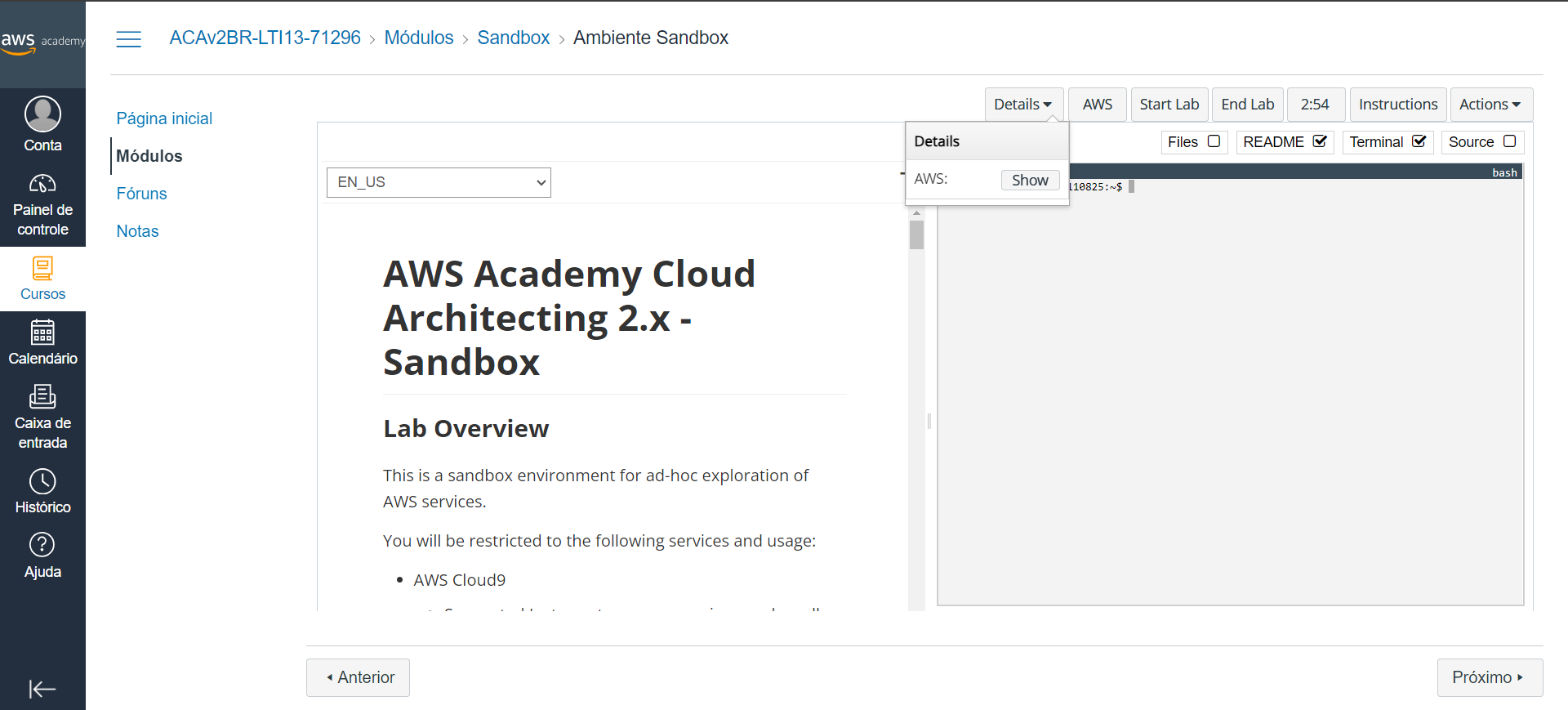
Abrirá uma telinha, **clique no** **X** e quando iniciar na mesma página clique em **AWS**

****

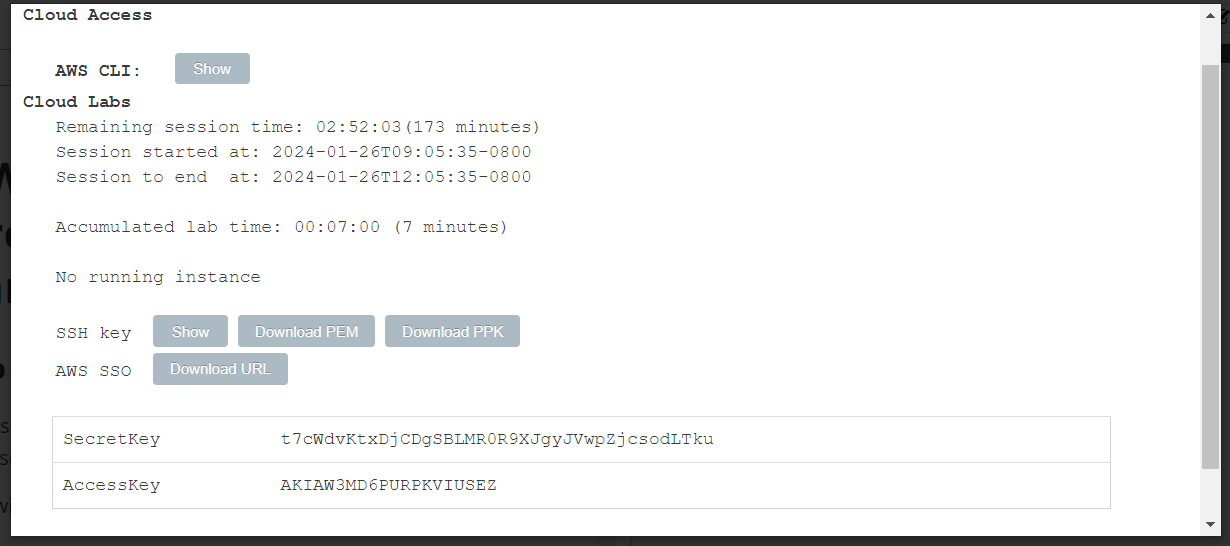
****

Clique em aqui, caso entre na tela para fazer login feche a página e clique novamente em **AWS**

**Etapa 2 –** Volte na página do curso e **clique em Details,** em seguida **clique em Show**



**Etapa 3 –** Vai Abrir uma tela com suas informações de KEY

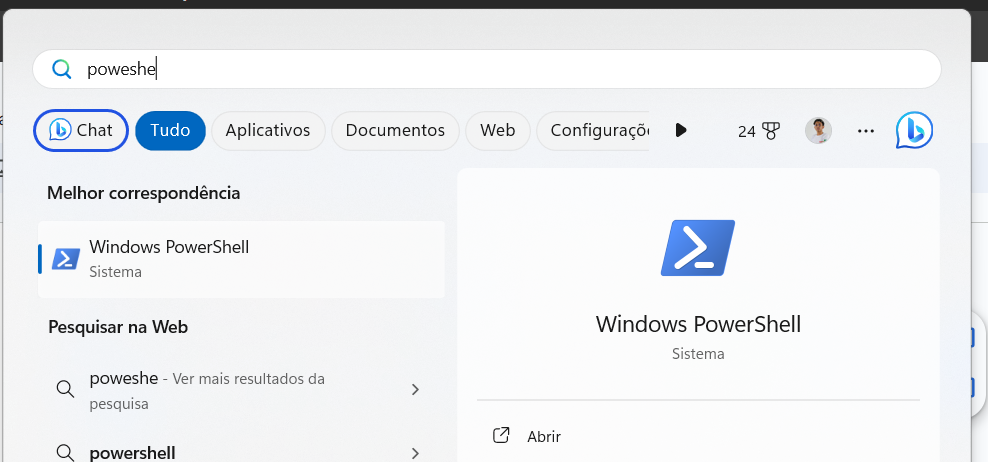
****

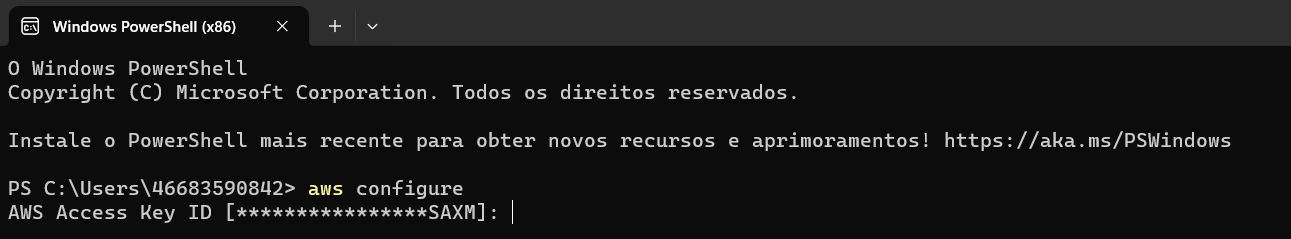
**Etapa 4 –** Copie o AccessKey e o SecretKey e cole no bloco de notas

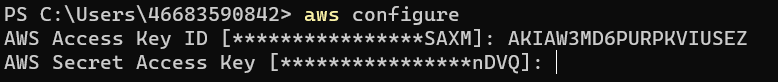
**SecretKey:** cNnE42/qbQb5W3Ak21pcVtHmLZr2FFLdVTRJKg7s

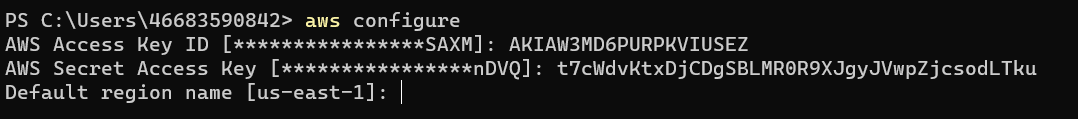
**AccessKey:** AKIA6GBMG75MEYUTFC4C

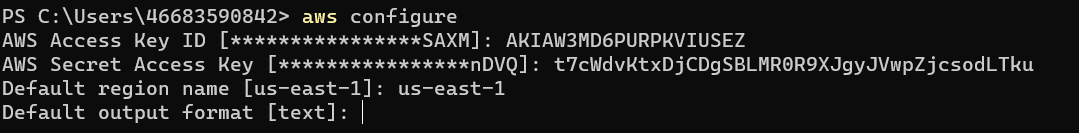
**Etapa 5 –** Abra o PoweShell na sua máquina local



**Etapa 6** **–** Vamos configurar nosso acesso a AWS – Digite (aws configure) e pressione **ENTER**  
  


**Etapa 7** **–** Cole o ( AccessKey ) copiado anteriormente e pressione **ENTER**   
  


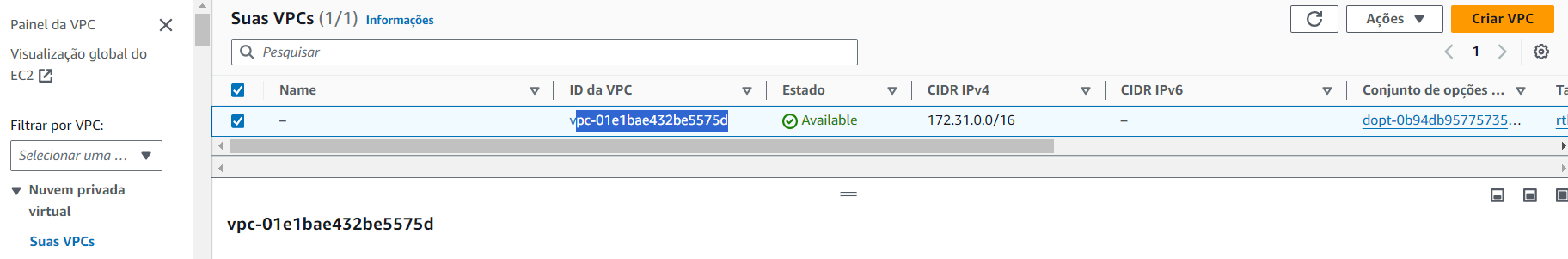
**Etapa 8** **–** Cole o ( SecretKey ) copiado anteriormente e pressione **ENTER**  
  


**Etapa 9** **–** Defina a região: us-east-1   
  


Defina o formato: **text** e pressione **ENTER** para finalizar.

**Laboratório 3 -** Criar uma VPC Publica 1 - AZ1a e VPC Publica 2 - AZ1a

**Etapa 1 – Configura**

Listar VPC existente  
  


# aws ec2 describe-vpcs

Filtrar por ID e por nome

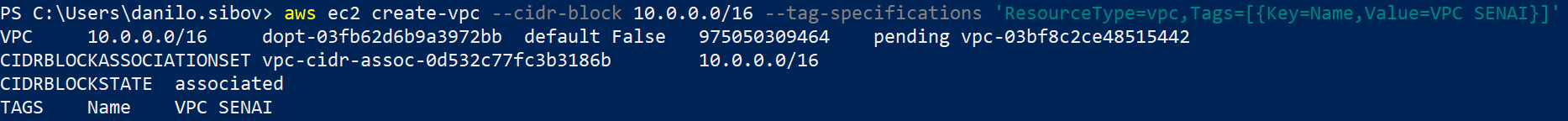
# aws ec2 describe-vpcs --query 'Vpcs[\*].VpcId'

# aws ec2 describe-vpcs --query 'Vpcs[\*].[VpcId,Tags[?Key==Name].Value]'

**Laboratório 2 -** Criar uma VPC Publica 1 - AZ1a e VPC Publica 2 - AZ1a e Criar Grupo de Segurança

**Etapa 1.1 - Criar uma VPC (VPC SENAI):**

# aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications 'ResourceType=vpc,Tags=[{Key=Name,Value=VPC SENAI}]'

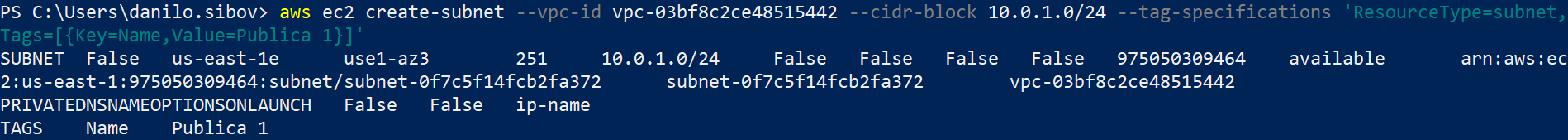


Este comando cria uma VPC com o bloco CIDR especificado (10.0.0.0/16). Anote o VpcId retornado ex.: vpc-03bf8c2ce48515442, pois será usado em comandos subsequentes.

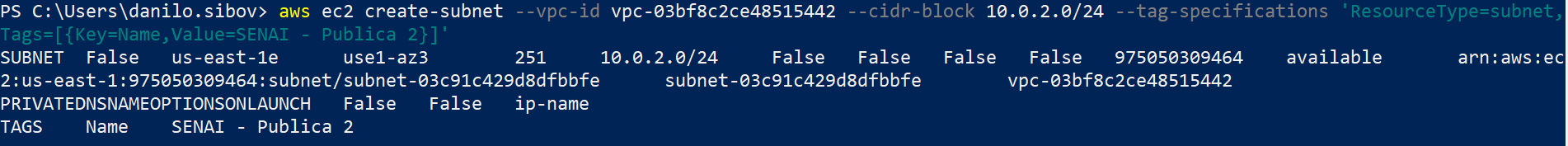
**Etapa 1.2 - Criar duas Sub-redes (Publica 1 e Publica 2):,** Substitua <VpcId> pelo ID da VPC criada anteriormente. Este comando cria uma sub-rede dentro da VPC com o bloco CIDR especificado (10.0.1.0/24).

aws ec2 create-subnet --vpc-id <VpcId> --cidr-block 10.0.1.0/24 --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Publica 1}]'

aws ec2 create-subnet --vpc-id vpc-03bf8c2ce48515442 --cidr-block 10.0.1.0/24 --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=SENAI - Publica 1}]'



aws ec2 create-subnet --vpc-id vpc-03bf8c2ce48515442 --cidr-block 10.0.2.0/24 --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value= SENAI - Publica 2}]'



Anotar os IDS das Sub Redes:

subnet-0f7c5f14fcb2fa372 - SENAI Publica 1

[subnet-03c91c429d8dfbbfe](https://us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#SubnetDetails:subnetId=subnet-03c91c429d8dfbbfe) - SENAI Publica 2

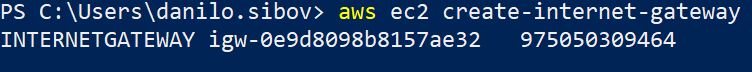
**Etapa 1.3 –** Listar Sub Redes

aws ec2 describe-subnets

**Etapa 2** **–** Adicionar um Internet Gateway (IGW) a uma VPC na AWS

**Etapa 2.1** **–** Criar o Internet Gateway (IGW)

aws ec2 create-internet-gateway

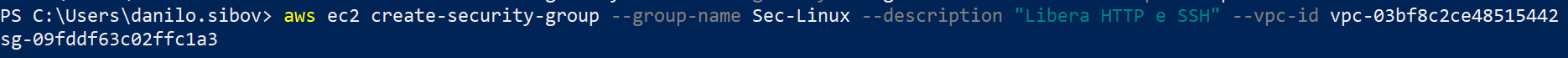


Anotar o ID do Internet Gateway igw-0e9d8098b8157ae32

**Etapa 2.2** **–** associar o Internet Gateway à sua VPC

aws ec2 attach-internet-gateway --internet-gateway-id <igw-id> --vpc-id <vpc-id>

aws ec2 attach-internet-gateway --internet-gateway-id igw-0e9d8098b8157ae32 --vpc-id vpc-03bf8c2ce48515442

**Etapa 4.1** **–** Criar um Grupo de Segurança   
  
aws ec2 create-security-group --group-name Sec-Linux --description "Libera HTTP e SSH" --vpc-id vpc-03bf8c2ce48515442  
  
  
Anotar o ID do Grupo de Segurança sg-09fddf63c02ffc1a3 **Etapa 3.2** **–** Adicionar regras ao Grupo de Segurança

aws ec2 authorize-security-group-ingress --group-id sg-09fddf63c02ffc1a3 --protocol tcp --port 22 --cidr 0.0.0.0/0

aws ec2 authorize-security-group-ingress --group-id sg-09fddf63c02ffc1a3 --protocol tcp --port 80 --cidr 0.0.0.0/0

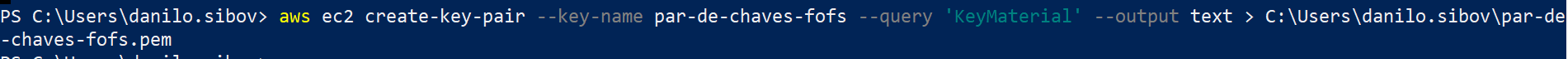
**Etapa 3.3 –** Verificar Grupo de Segurança

aws ec2 describe-security-groups

**Laboratório 4 –** Criar par de chaves, localizar imagens e Criar um Linux da máquina local

**Etapa 4.1 –** Criar Chave de Segurança (.PPK) usando o PowerShell

aws ec2 create-key-pair --key-name meu-par-de-chaves --query 'KeyMaterial' --output text > C:\Users\usuario\meu-par-de-chaves.pem



Copiar a chave e salvar em um local importante.

**Etapa 4.2 –** Listar Par de Chave de Segurança

aws ec2 describe-key-pairs

Copiar o ID da Chave

key-0904066bb74f1fa7c

**Etapa 4.3 –** Converter a chave SSH para o formato .PPK usando o PuTTYgen

**Etapa 5.1** **– Mostrar as informações da Imagem**

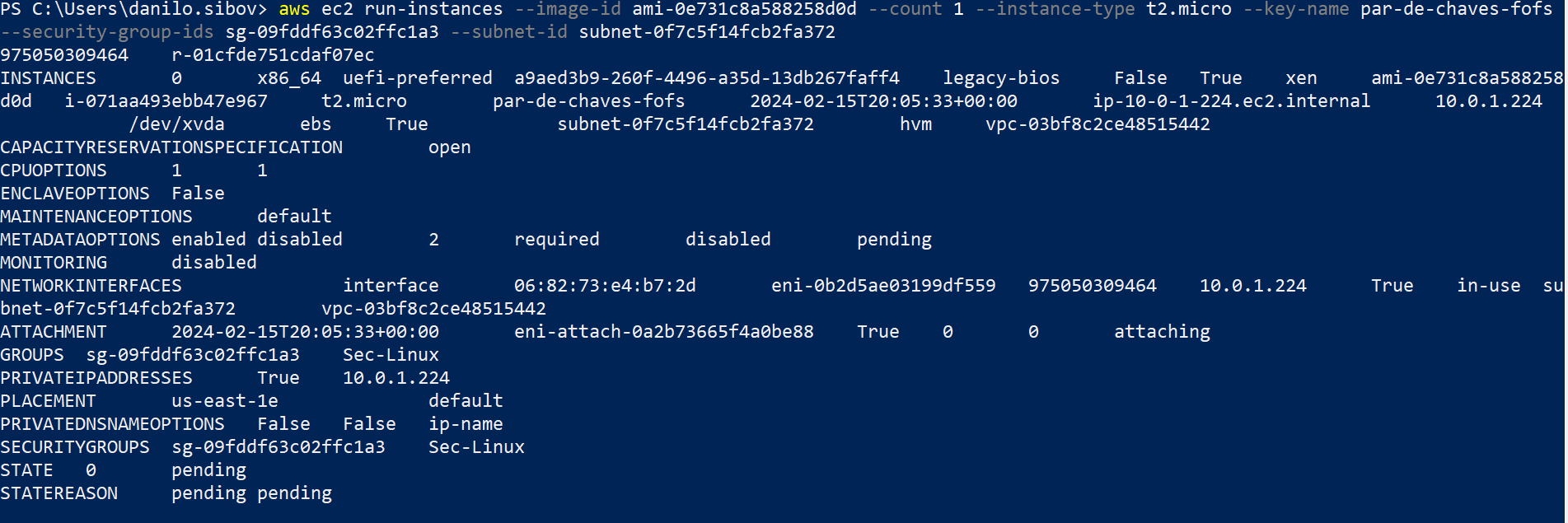
aws ec2 describe-images --image-ids ami-0e731c8a588258d0d

**Etapa 5.2** **– Criar uma instancia com a imagem e VPC criadas**

aws ec2 run-instances --image-id ami-0e731c8a588258d0d --count 1 --instance-type t2.micro --key-name use seu par de chave) --security-group-ids sg-(cole o id do grupo criado) --subnet-id subnet-(cole o id da subnet)

Exemplo:

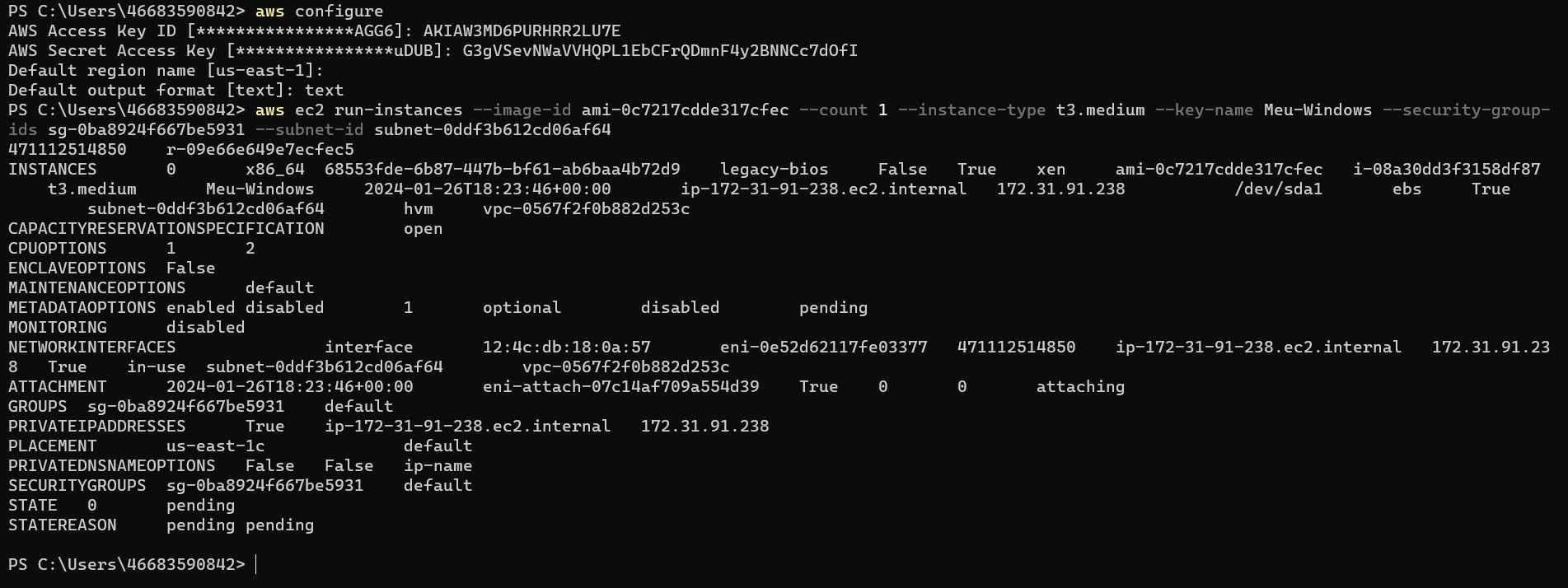
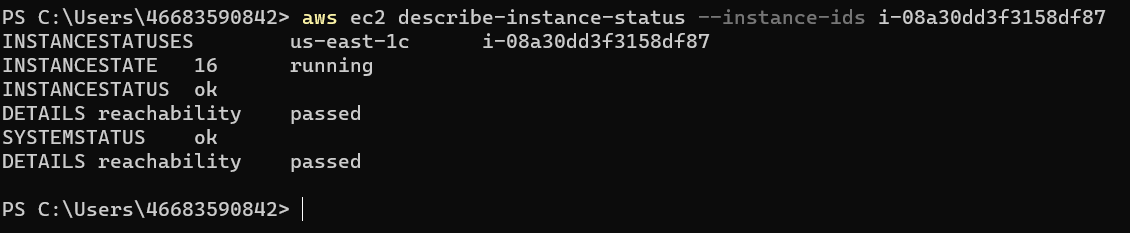
aws ec2 run-instances --image-id ami-0e731c8a588258d0d --count 1 --instance-type t2.micro --key-name par-de-chaves-fofs --security-group-ids sg-09fddf63c02ffc1a3 --subnet-id subnet-0f7c5f14fcb2fa372



Para ver o status da Instância execute o comando:

aws ec2 describe-instance-status --instance-ids (id-da-instância)   
  
Exemplo: aws ec2 describe-instance-status --instance-ids i-0dc4da9077bc6df35   
  
  


**Laboratório 5 -** Cria um Windows Cliente da máquina local

**Repita as etapas acima de configuração (** toda vez que você parar o laboratório no Ambiente SandBox o **id Key vai mudar** **)   
  
Nesta etapa vamos alterar o AMI da máquina (** ami-0c7217cdde317cfec **, AMI DO WINDOWS )   
**aws ec2 run-instances --image-id ami-0c7217cdde317cfec --count 1 --instance-type t3.medium --key-name ( seu par de chave ) --security-group-ids sg-( ID da segurança de grupos ) --subnet-id subnet-( ID da sub-rede )  
aws ec2 run-instances --image-id ami-0c7217cdde317cfec --count 1 --instance-type t3.medium --key-name Meu-Windows --security-group-ids sg-0ba8924f667be5931 --subnet-id subnet-0ddf3b612cd06af64 **Repita o comando de verificação do status da instância**comando: aws ec2 describe-instance-status --instance-ids (id-da-instância)   
  
Exemplo: aws ec2 describe-instance-status --instance-ids i-08a30dd3f3158df87 ****