



Laboratório – Explorando a AWS com o Amazon EC2

Resumo do laboratório

Esse laboratório irá te fornecer uma visão básica e prática do que é uma instância EC2, como inicializá-la pelo console e via CloudShell.

O Amazon Elastic Compute Cloud é um serviço que fornece poder computacional, com máquinas virtuais (ou também chamadas de VMs) que irão funcionar como um computador físico, para as mais diversas funções. Foi feito para que, sempre que desenvolvedores precisarem de poder computacional, podem providenciar facilmente e em poucos minutos.

Objetivos

Ao concluir o lab, você aprenderá o seguinte:

- Iniciar um servidor web de teste via console de gerenciamento da AWS.
- Configurar o servidor web para permitir a conexão via HTTP.
- Iniciar outra instância EC2, através de comandos no CloudShell.
- Finalizar suas instâncias EC2.

Início

1. Acesse o [console de gerenciamento da AWS](#)

Caso apresente a mensagem de erro abaixo, clique no texto em azul onde consta a informação “To logout, click here”.



Amazon Web Services Sign In

The credentials in your login link were invalid. Please contact your administrator.

To logout, click [here](#)

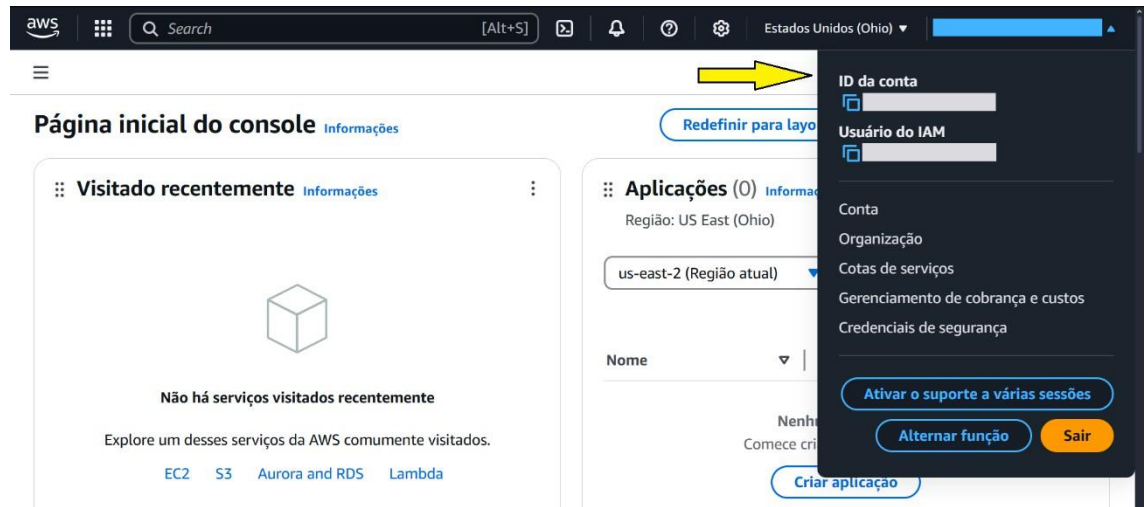


Terms of Use Privacy Policy © 1996-2025, Amazon Web Services, Inc. or its affiliates.

An  amazon.com company

Atenção: Após efetuar login, irá mostrar o console de gerenciamento da AWS.

Sempre confira, no canto superior direito do console, qual a conta está logada, para evitar acessar com a conta incorreta e evitar gastos desnecessários.



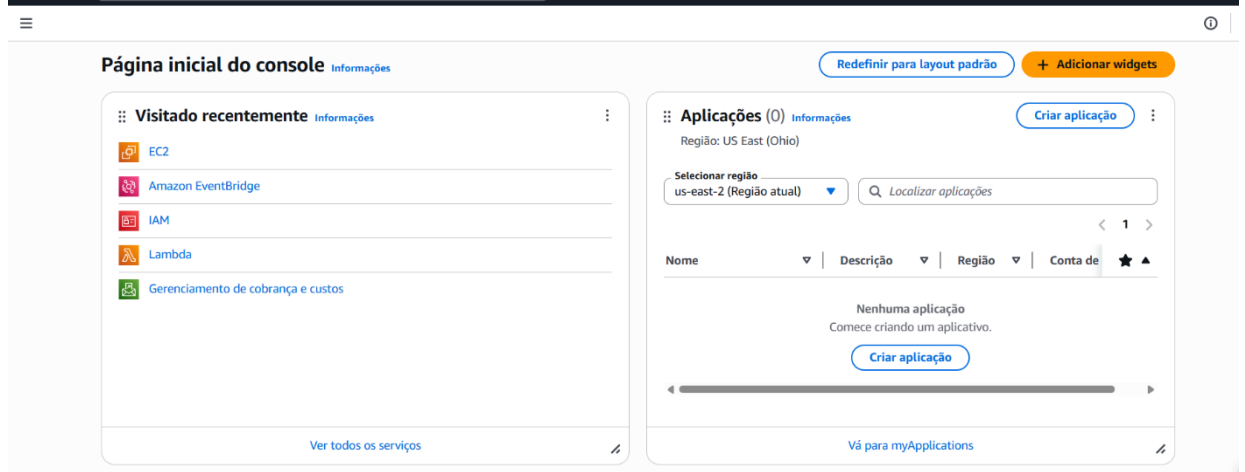
Acesso controlado no console AWS

Os recursos liberados serão limitados para permitir apenas o necessário no laboratório. Mensagens de erro serão comuns de aparecer, caso tente acessar algum recurso não liberado na sua conta ou mesmo ao abrir algum serviço com limitações. Porém sempre siga à risca os passos propostos neste e em outros labs.

1. Executar uma Instância EC2 pelo console

Iremos iniciar uma instância através do console de gerenciamento, que será um servidor web de teste. Depois iremos testar a conectividade desse servidor web.

3. No canto superior esquerdo, na barra de pesquisa, pesquise pelo serviço EC2.

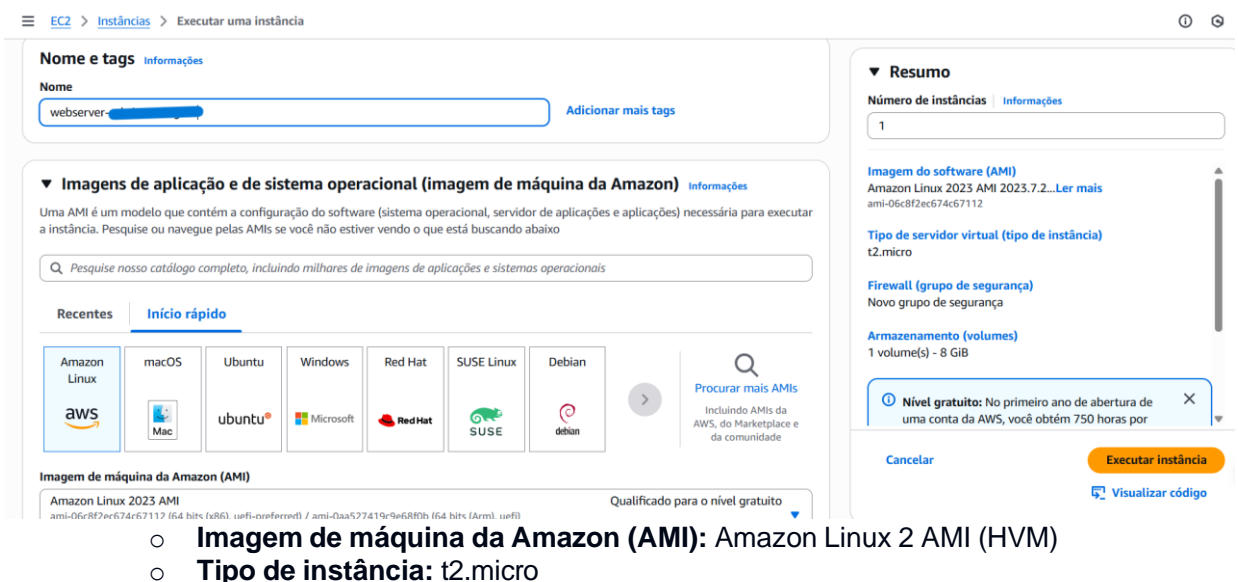


4. Clique em **Executar instância**. Se não aparecer o botão laranja, você ir no menu esquerdo, em Instâncias e depois em **Executar instância**.

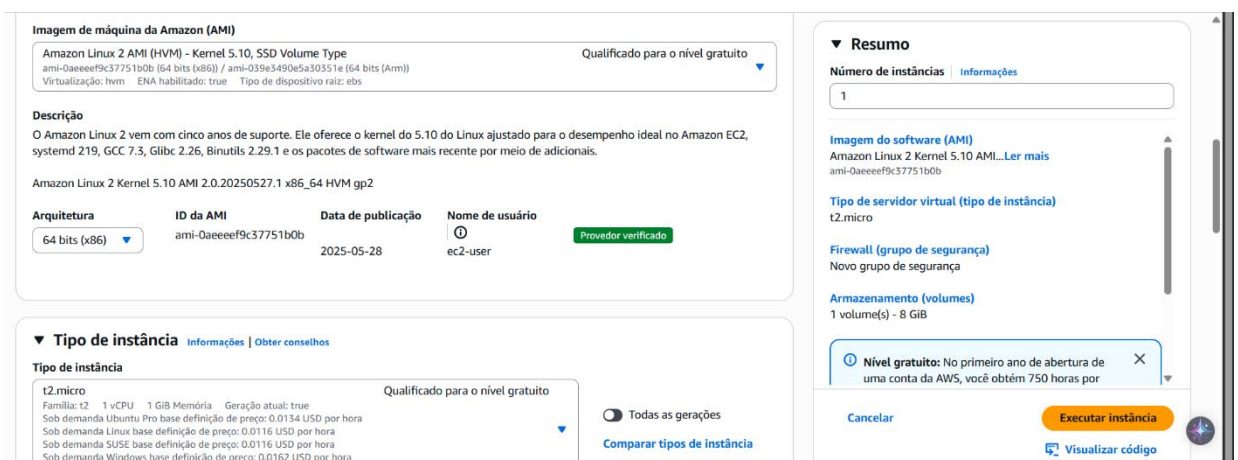


5. Preencha as informações conforme abaixo. Os campos que não forem mencionados, deixe no valor padrão:

- **Nome:** webserver-<seu nome e sobrenome>.
- (Não digite espaço, nem os sinais <>. Por exemplo, se seu nome for Jeff Bezos, digite **webserver-jeffbezoz**)



- **Imagem de máquina da Amazon (AMI):** Amazon Linux 2 AMI (HVM)
- **Tipo de instância:** t2.micro



- **Par de chaves (login):** no canto direito há a opção azul **Criar novo par de chaves**. Clique nela, para criar um par de chaves.
- Para o par de chaves ainda, crie com o nome **parchave-<seu nome e sobrenome>**.
- (Não digite espaço, nem os sinais <>. Por exemplo, se seu nome for Jeff Bezos, digite **parchave-jeffbezos**)
- Tipo de par de chaves: RSA
- Formato de arquivo de chave privada: .pem
- Clique em **Criar par de chaves**. Irá aparecer uma tela para salvar o arquivo .pem. Salve-o em uma pasta de fácil localização, pois o utilizaremos em breve.

- Depois volte à tela do console da AWS e selecione o par de chaves com o seu nome.
- **Configurações de rede > Firewall (grupos de segurança):** Criar grupo de segurança. Marque a opção “Permitir tráfego HTTP”.

- **Detalhes avançados:** clique nessa opção, depois vá até o final, em Dados de usuário (opcional) e insira o texto abaixo:

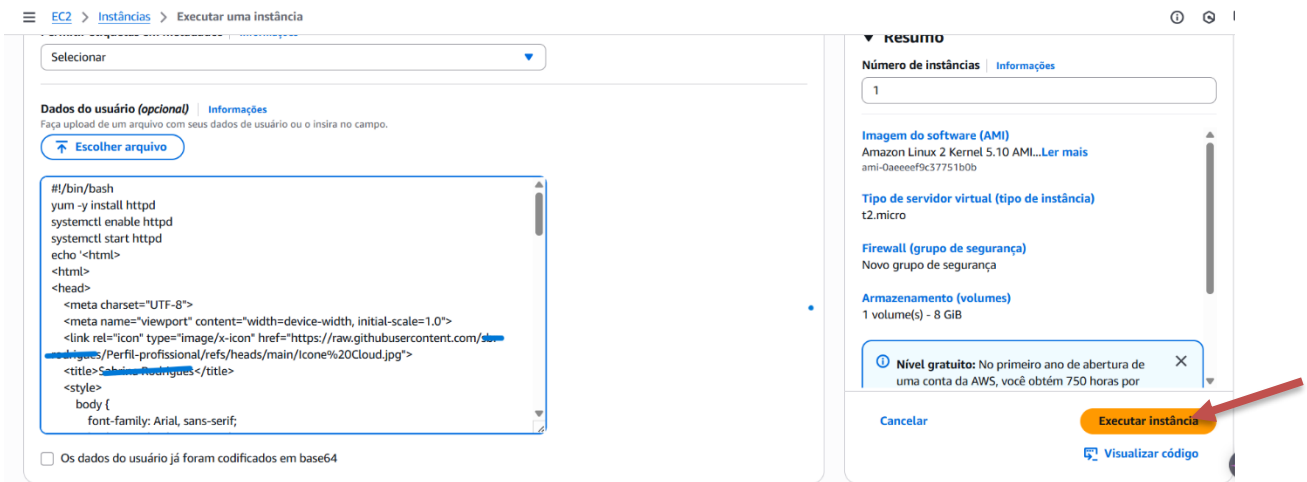
```
#!/bin/bash
```

```
yum -y install httpd
```

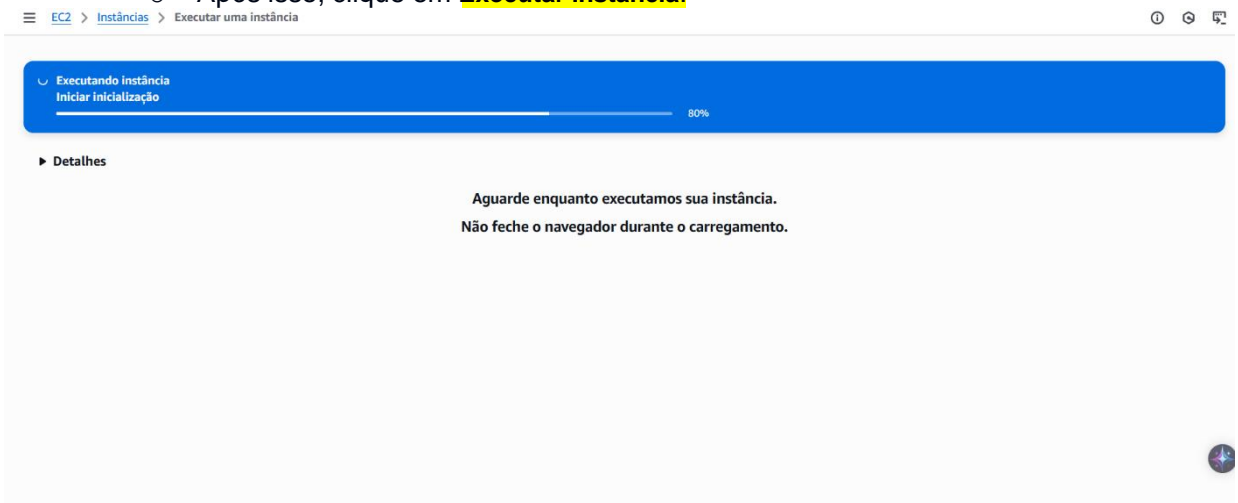
```
systemctl enable httpd
```

```
systemctl start httpd
```

```
echo '<html><h1>Bem-vindo, ao meu perfil!</h1></html>' > /var/www/html/index.html
```

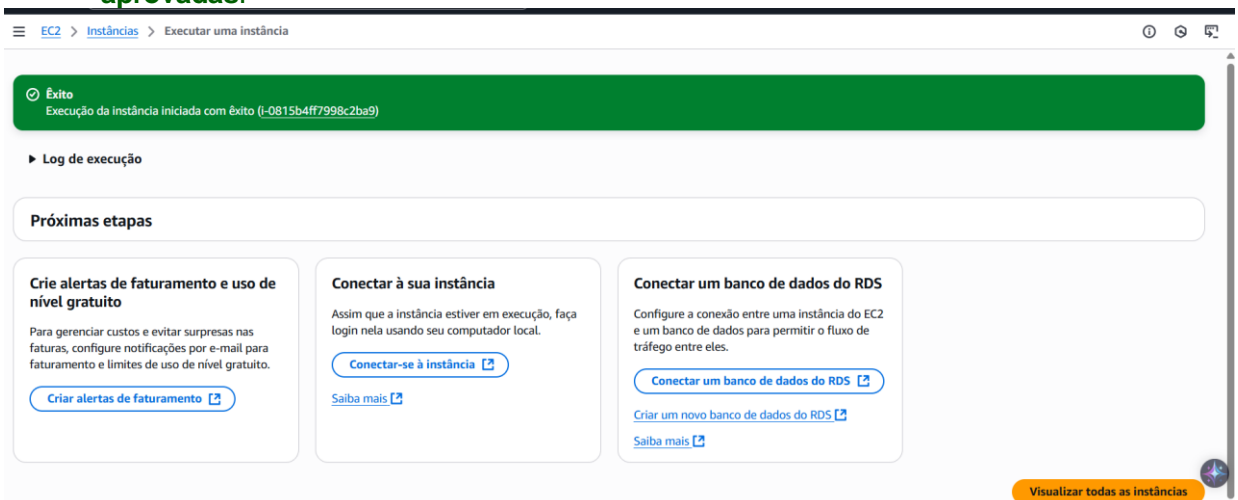


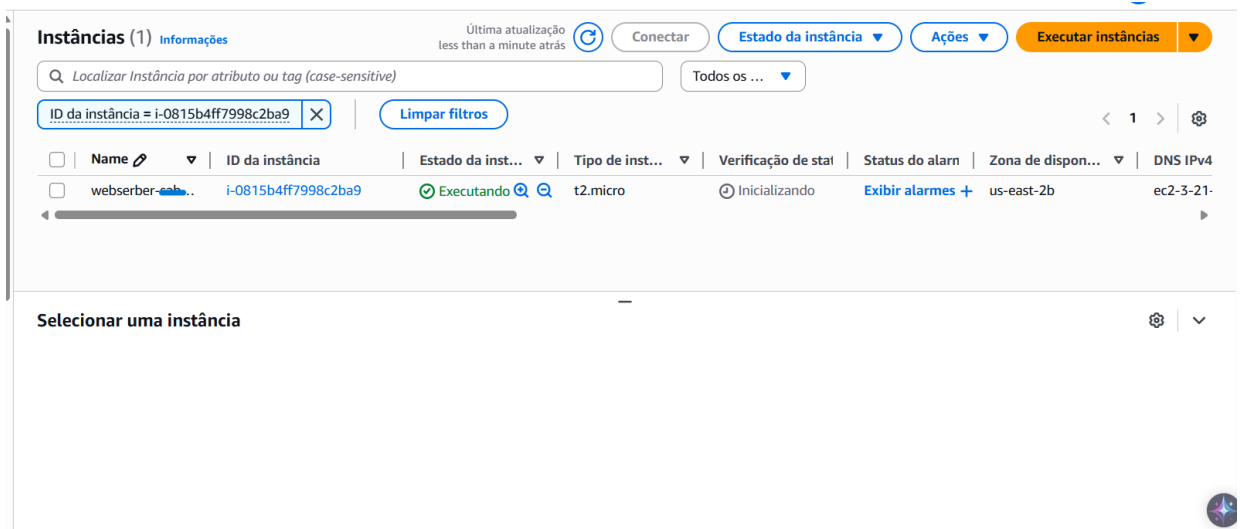
- Com estes dados de usuário, iremos instalar e iniciar um componente, para subirmos um servidor web. E então é criada uma página web simples.
- Após isso, clique em **Executar instância**.



Caso precisar, anote o nome da instância que você utilizou, pois iremos precisar em breve. Após clicar para executar a instância, irá mostrar uma mensagem de Êxito. Você pode clicar em cima do ID da instância (geralmente começa com i- e terão várias letras e números) ou volte para o serviço EC2 e no menu esquerdo, clique em Instâncias.

6. Após abrir a tela de Instâncias, localize a instância pelo seu nome e clique em cima do ID da instância e aguarde a Verificação de status mostrar **2/2 verificações aprovadas**.





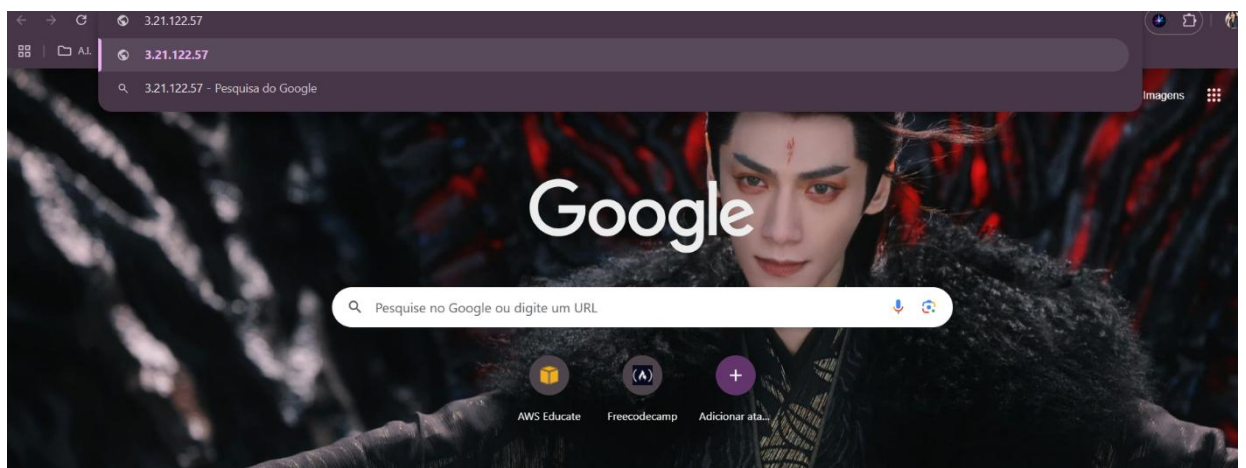
- Após isso, clique em cima do ID da sua instância, para mostrar todos os detalhes. Logo no início, irá mostrar o Endereço IPv4 público. Copie-o e deixe-o salvo em algum editor de texto. Usaremos este IP em breve.



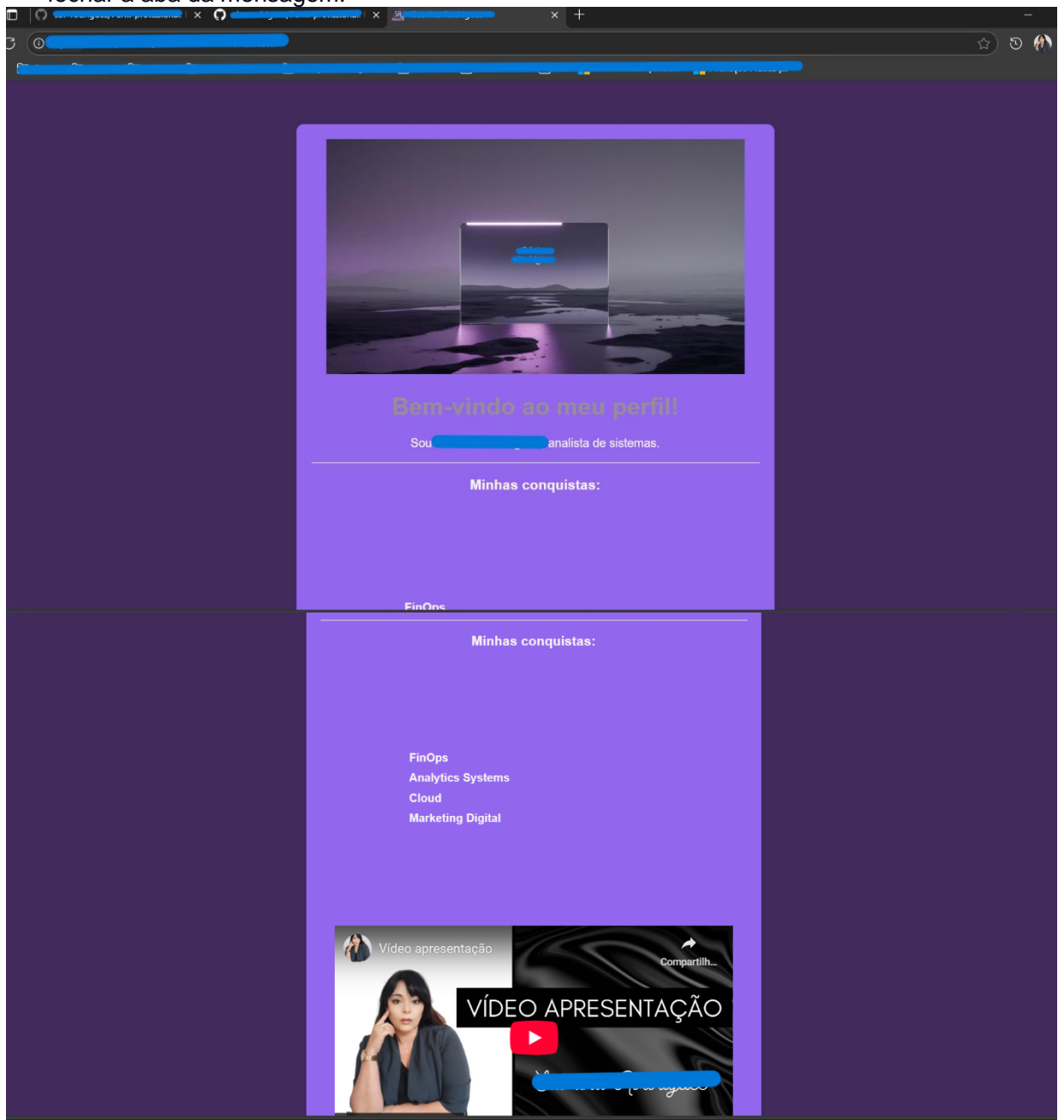
- Abra outra aba no seu navegador e digite `http://` e então o Endereço IPv4 público da sua instância.

(Por exemplo, se o IP da sua instância for 8.8.8.8, digite `http://8.8.8.8`)

Ao acessar pelo navegador, alguém vai te dar um oi!



9. O servidor de teste está iniciado! Se apareceu a mensagem corretamente, pode fechar a aba da mensagem.



Agora iremos iniciar outra instância pelo CloudShell.

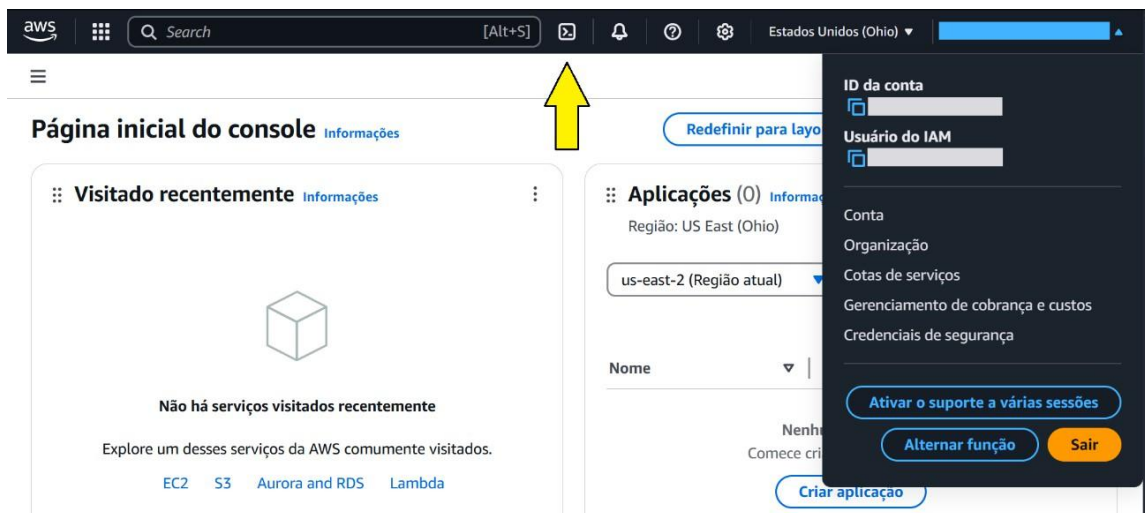
2. Inicializar outra instância através do CloudShell

Agora que aprendemos como inicializar uma instância através console de gerenciamento da AWS, vamos inicializar outra instância através de uma ferramenta útil, que é o CloudShell.

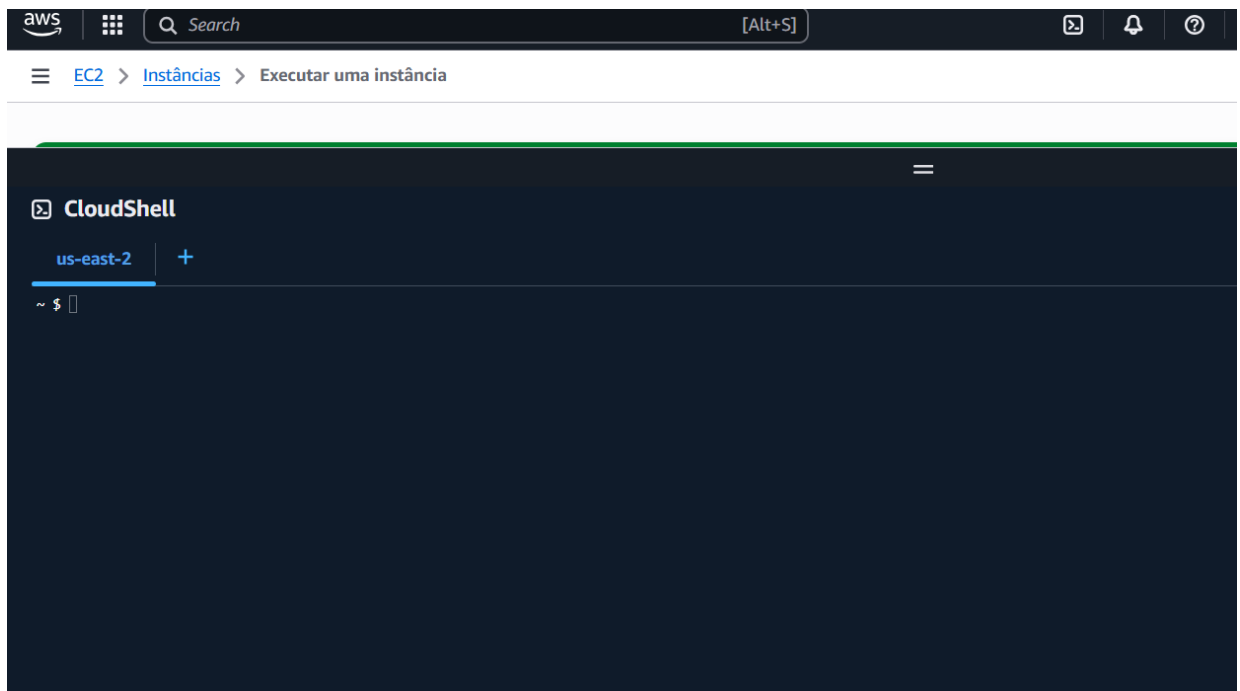
O CloudShell e também o AWS CLI nos permitem gerenciar toda a nossa infraestrutura, através de comandos ou scripts. Apesar de demandar uma curva maior de aprendizado, nos permite ter um controle muito mais apurado e escalável da nossa infraestrutura. Com essas ferramentas é possível inicializarmos dezenas ou até centenas de serviços com poucos ou nenhum clique de mouse, além de terem mecanismos acessíveis apenas destas formas.

10. Volte ao console de gerenciamento da AWS.

11. No canto superior direito do console de gerenciamento da AWS, próximo de onde mostra o nosso login, irá mostrar o ícone conforme abaixo. Clique nele e irá mostrar o CloudShell.



Após isso, o CloudShell irá aparecer na parte de baixo da tela.



12. Agora iremos executar diversos comandos dentro do CloudShell. Copie o comando abaixo para um editor de texto. Mude-o para colocar o seu nome e sobrenome antes do **-grupo**, sem espaços e sem apagar os caracteres antes ou após esse nome. Depois, copie o comando que você editou, clique com o botão direito do mouse no meio do CloudShell que apareceu em baixo e irá aparecer o comando copiado. Depois disso, aperte Enter e irá executá-lo.

```
GRUPO_SEGURANCA="xxxxxxxx-grupo"
```

13. Da mesma forma, copie os dois comandos seguintes para um editor de texto e coloque seu nome, tanto no nome_instancia quanto no par_chave. No par_chave, use o mesmo nome do par de chaves que você criou. Depois disso, aperte Enter e irá executá-lo.

```
NOME_INSTANCIA="instancia-xxxxxxxxxx"
```

```
PAR_CHAVE="parchave-xxxxxxxxxxxxx"
```

14. Execute o comando abaixo.

```
SECURITY_GROUP_ID=$(aws ec2 create-security-group --group-name $GRUPO_SEGURANCA --description "Permitir HTTP" --query "GroupId" --output text)
```

Irá aparecer um aviso no meio da tela. Clique no botão azul **Colar** e aperte Enter.

Se aparecer uma tela com vários caracteres no CloudShell, para sair clique com o botão esquerdo do mouse no meio dele, aperte a letra **Q** e depois aperte Enter. Caso tiver dificuldades para sair, abra uma nova guia no próprio CloudShell ou feche-o e reabra o mesmo.

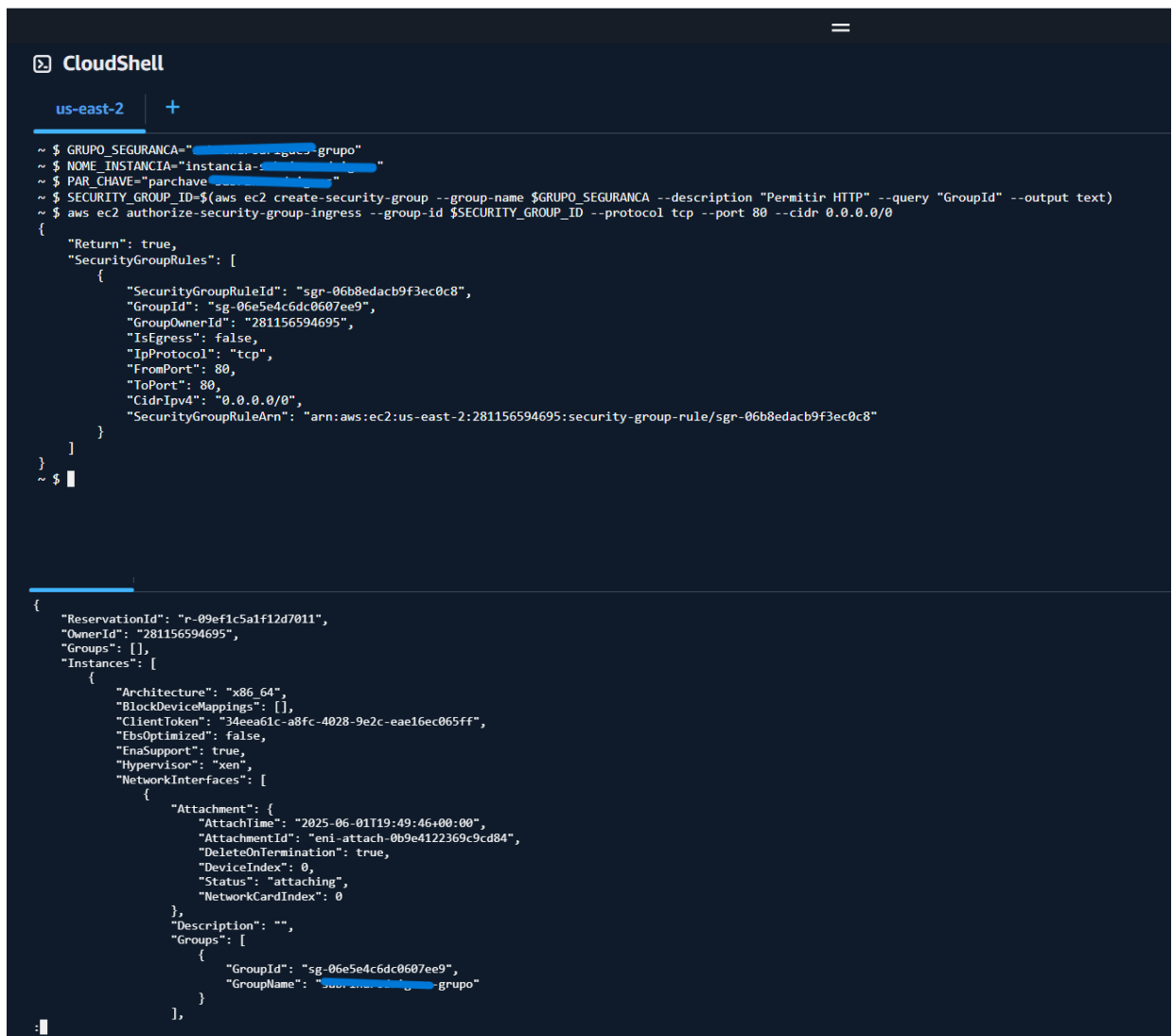
15. Copie e execute o comando abaixo. Não precisa editá-lo.

```
aws ec2 authorize-security-group-ingress --group-id $SECURITY_GROUP_ID --protocol tcp --port 80 --cidr 0.0.0.0/0
```

16. Execute o comando abaixo.

```
aws ec2 run-instances \
  --instance-type t2.micro \
  --image-id $(aws ssm get-parameters-by-path --path "/aws/service/ami-amazon-linux-latest" --
  query "Parameters[?ends_with(Name, 'al2023-ami-kernel-default-x86_64')].Value" --output text) \
  --security-group-ids $SECURITY_GROUP_ID \
  --tag-specifications "ResourceType=instance,Tags=[{Key=Name,Value=$NOME_INSTANCIA}]" \
  --key-name $PAR_CHAVE \
  --user-data
"lyEvYmluL2Jhc2gKeXVtIC15IGluc3RhbGwgaHR0cGQKc3lzdGVtY3RsIGVuYWJsZSBodHRwZAp
zeXN0ZW1jdGwgc3RhcncQgaHR0cGQKZWNoYAnPGh0bWw+PGgxPk9sw6EgZG8gc2V1IHNIcn
ZpZG9yIHdlYiE8L2gxPjwvaHRtbD4nID4gL3Zhci93d3cvaHRtbC9pbmRleC5odG1sCg=="
```

(Em base64 Decode)



```
CloudShell
us-east-2 +
~ $ GRUPO_SEGURANCA="sg-06b8edacb9f3ec0c8"
~ $ NOME_INSTANCIA="instancia-06b8edacb9f3ec0c8"
~ $ PAR_CHAVE="parchave-06b8edacb9f3ec0c8"
~ $ SECURITY_GROUP_ID=$(aws ec2 create-security-group --group-name $GRUPO_SEGURANCA --description "Permitir HTTP" --query "GroupId" --output text)
~ $ aws ec2 authorize-security-group-ingress --group-id $SECURITY_GROUP_ID --protocol tcp --port 80 --cidr 0.0.0.0/0
{
  "Return": true,
  "SecurityGroupRules": [
    {
      "SecurityGroupRuleId": "sgr-06b8edacb9f3ec0c8",
      "GroupId": "sg-06e5e4c6dc0607ee9",
      "GroupOwnerId": "281156594695",
      "IsEgress": false,
      "IpProtocol": "tcp",
      "FromPort": 80,
      "ToPort": 80,
      "CidrIpv4": "0.0.0.0/0",
      "SecurityGroupRuleArn": "arn:aws:ec2:us-east-2:281156594695:security-group-rule/sgr-06b8edacb9f3ec0c8"
    }
  ]
}
~ $

{
  "ReservationId": "r-09ef1c5a1f12d7011",
  "OwnerId": "281156594695",
  "Groups": [],
  "Instances": [
    {
      "Architecture": "x86_64",
      "BlockDeviceMappings": [],
      "ClientToken": "34eea61c-a8fc-4028-9e2c-eae16ec065ff",
      "EbsOptimized": false,
      "EnaSupport": true,
      "Hypervisor": "xen",
      "NetworkInterfaces": [
        {
          "Attachment": {
            "AttachTime": "2025-06-01T19:49:46+00:00",
            "AttachmentId": "eni-attach-0b9e4122369c9cd84",
            "DeleteOnTermination": true,
            "DeviceIndex": 0,
            "Status": "attaching",
            "NetworkCardIndex": 0
          },
          "Description": "",
          "Groups": [
            {
              "GroupId": "sg-06e5e4c6dc0607ee9",
              "GroupName": "sg-06b8edacb9f3ec0c8-grupo"
            }
          ]
        }
      ]
    }
  ],
}
```

Troque as USER DATA pelo BASE64 DECODE

EC2

Painel

Visualização Global do EC2

Eventos

▼ Instâncias

Instâncias

Tipos de instância

Modelos de execução

Solicitações spot

Savings Plans

Instâncias reservadas

Hosts dedicados

Reservas de capacidade

▼ Imagens

AMIs

Catálogo de AMIs

Elastic Block Store

Resumo da instância para i-0b43d381081d4320d (instancia-cabineiro-daiguera) Informações

Conectar

Estado da instância

Ações

Atualizado há less than a minute

ID da instância

i-0b43d381081d4320d

Endereço IPv6

-

Tipo de nome do host

Nome do IP: ip-172-31-18-92.us-east-2.compute.internal

Nome do DNS do recurso privado de resposta

-

Endereço IP atribuído automaticamente

3.135.20.167 [IP público]

Função do IAM

-

Endereço IPv4 público

3.135.20.167 | endereço aberto

Estado da instância

Executando

Nome do DNS de IP privado (somente IPv4)

ip-172-31-18-92.us-east-2.compute.internal

Tipo de instância

t2.micro

ID da VPC

vpc-0399852f74ef7a39b

ID da sub-rede

subnet-01af509b2d6e1390f

Endereços IPv4 privados

172.31.18.92

DNS pública

ec2-3-135-20-167.us-east-2.compute.amazonaws.com | endereço aberto

Endereços IP elásticos

-

Descoberta do AWS Compute Optimizer

Opte por participar do AWS Compute Optimizer para obter recomendações. Saiba mais

Nome do Grupo do Auto Scaling

-

Bem-vindo ao meu perfil!

Sou analista de sistemas.

Minhas conquistas:

FinOne

Minhas conquistas:

FinOps

Analytics Systems

Cloud

Marketing Digital

Vídeo apresentação

COMPARTILHAR

VÍDEO APRESENTAÇÃO

Carla

Agora, precisamos encerrar as duas instâncias que criamos. Localize as duas instâncias que você inicializou, selecione-as clicando em cima dos quadrados no

canto esquerdo. Depois, no lado direito, clique em [Estado da instância](#) e em Encerrar (excluir) instância.

Na mensagem que irá aparecer no meio da tela, clique em **Encerrar (excluir)**.

19. Vá no menu esquerdo e mais para baixo, em Rede e segurança > Security groups. Localize e selecione o grupo de segurança com o seu nome, depois clique em [Ações](#) e em Excluir grupos de segurança. Confirme a exclusão, digitando a informação solicitada na mensagem e clique em **Excluir**.

Finalizar Laboratório

Após encerrar as duas instâncias e excluir o grupo de segurança, finalize o seu acesso ao console da seguinte forma.

20. No canto superior direito do console de gerenciamento da AWS, clique em cima do seu nome de usuário que está em azul, depois clique em **Sair** que aparece mais abaixo.
21. Pronto! Laboratório concluído com sucesso!

Recursos adicionais

- [Iniciar uma instância do Amazon EC2](#)
- [Tipos de Instâncias](#)
- [Amazon Machine Images \(AMI\)](#)
- [Amazon EC2 – Dados de usuário e Shell Scripts](#)
- [Amazon EC2 – Volumes raiz](#)
- [Marcar com tag os recursos do Amazon EC2](#)
- [Grupos de segurança](#)
- [Pares de chaves do Amazon EC2](#)
- [Verificações do status das instâncias](#)