



Infraestrutura I

Cloud computing na Amazon

Vamos ver como acessar a plataforma Amazon AWS e criar uma máquina virtual.

Acesso ao console de gerenciamento da AWS

Devemos entrar pelo URL: <https://405378853534.signin.aws.amazon.com/console>

ID da conta: 405378853534, é o fornecido pela Digital House

Nome do usuário, coloque o nome de usuário que o seu professor lhe passou.

Senha: coloque a senha que o seu professor lhe passou, podendo ser alterada por você.



Fazer login como usuário do IAM

ID da conta (12 dígitos) ou alias da conta

Nome de usuário:

Senha:

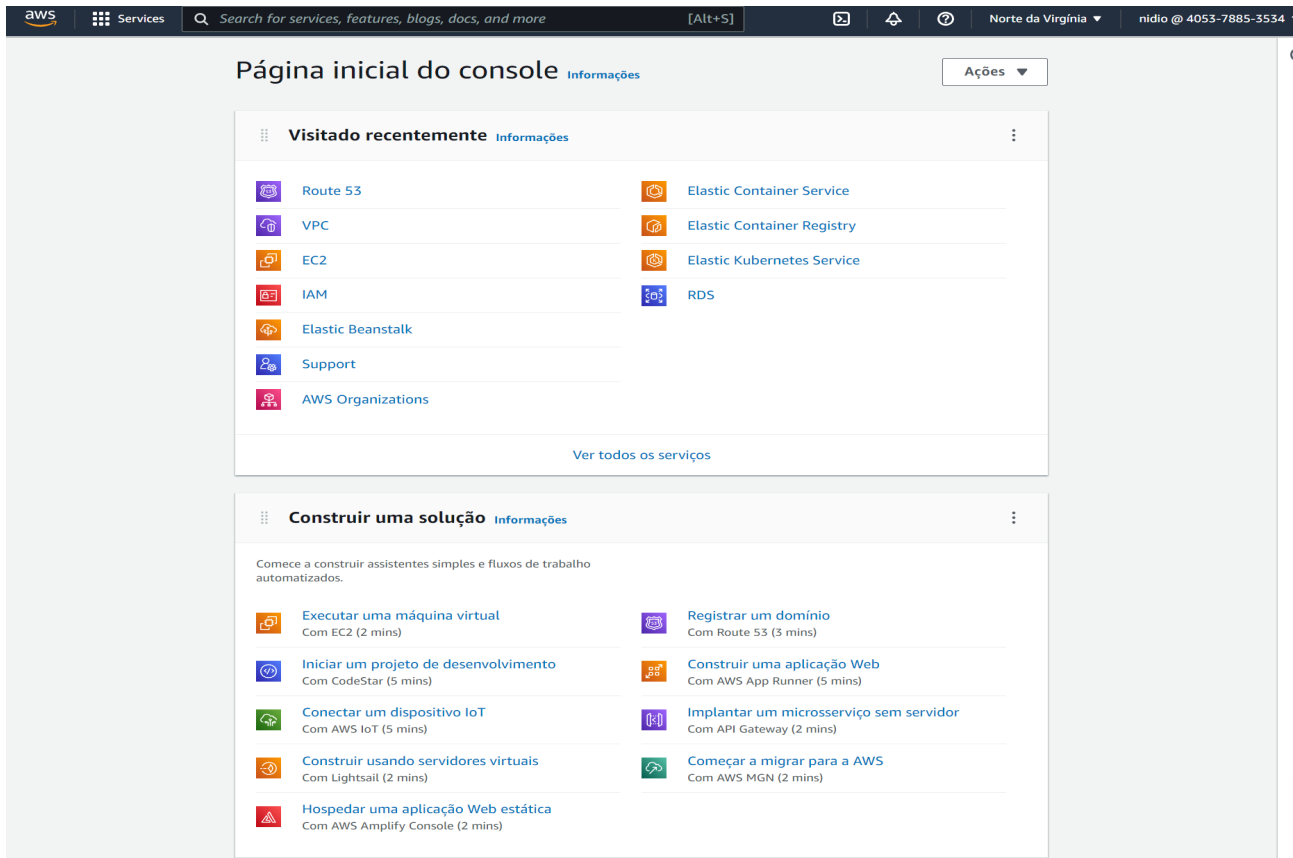
☐ Lembrar desta conta

Entrar

[Fazer login usando o e-mail do usuário root](#)

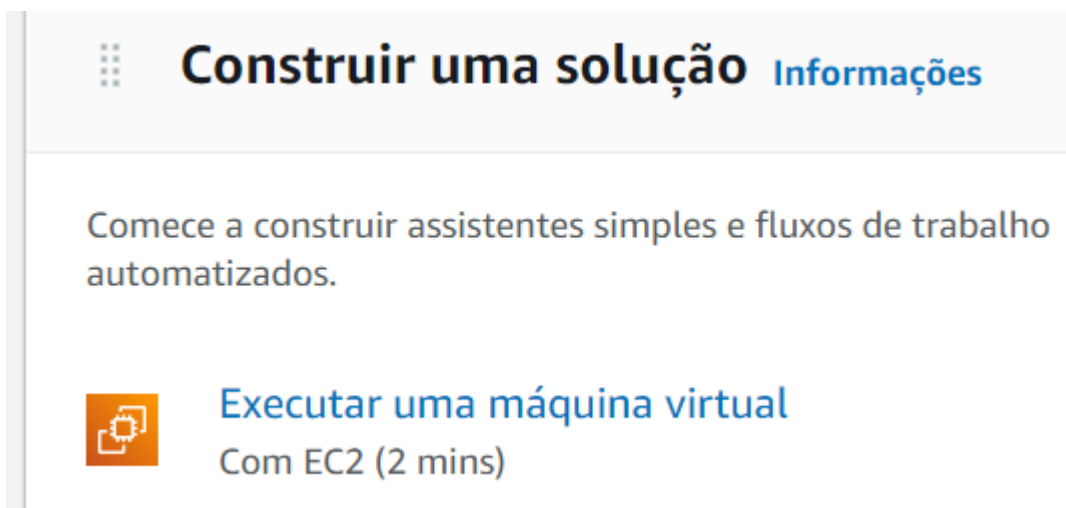
[Esqueceu sua senha?](#)

Este é o console de gerenciamento da plataforma AWS:



Crie uma máquina virtual com o serviço Amazon EC2

Clicamos em “Executar uma máquina virtual com EC2” ou “Launch a virtual machine with EC2”.



Defina um nome para a máquina virtual, coloque inicialmente o código da sua turma, ex: t1 em seguida o número da sua mesa de trabalho 01 e seu nome:

Iniciar uma instância [Informações](#)

O Amazon EC2 permite criar máquinas virtuais, ou instâncias, que são executadas na Nuvem AWS. Comece a usar rapidamente seguindo as etapas simples abaixo.

Nome e tags [Informações](#)

Nome

t101nidio

[Adicionar mais tags](#)

Em seguida, selecionamos a imagem “Ubuntu Server 22.04 LTS”.

▼ Imagens de aplicação e de sistema operacional (imagem de máquina da Amazon)

[Informações](#)

Uma AMI é um modelo que contém a configuração do software (sistema operacional, servidor de aplicações e aplicações) necessária para executar a instância. Pesquise ou navegue pelas AMIs se você não estiver vendo o que está buscando abaixo

Pesquise nosso catálogo completo, incluindo milhares de imagens de aplicações e sistemas operacionais

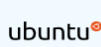
Recentes

Início rápido

Amazon
Linux



Ubuntu



Windows



Red Hat



SUSE Linux



ma



[Procurar mais AMIs](#)

Incluindo AMIs da
AWS, do Marketplace e
da comunidade

Imagem de máquina da Amazon (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type
ami-052efd3df9dad4825 (64 bits (x86)) / ami-070650c005cce4203 (64 bits (Arm))
Virtualização: hvm ENA habilitado: true Tipo de dispositivo raiz: ebs

Qualificado para o nível gratuito ▼

Descrição

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2022-06-09

Arquitetura

64 bits (x86) ▼

ID da AMI

ami-052efd3df9dad4825

Selecione a opção t2.micro como tipo de instância.

▼ **Tipo de instância** [Informações](#)

Tipo de instância

t2.micro Qualificado para o nível gratuito

Família: t2 1 vCPU 1 GiB Memória

Sob demanda Linux definição de preço: 0.0116 USD por hora

Sob demanda Windows definição de preço: 0.0162 USD por hora

[Comparar tipos de instância](#)

Utilize a mesma chave criada na aula anterior:

▼ **Par de chaves (login)** [Informações](#)

Você pode usar um par de chaves para se conectar com segurança à sua instância. Certifique-se de ter acesso ao par de chaves selecionado antes de executar a instância.

Nome do par de chaves - *obrigatório*

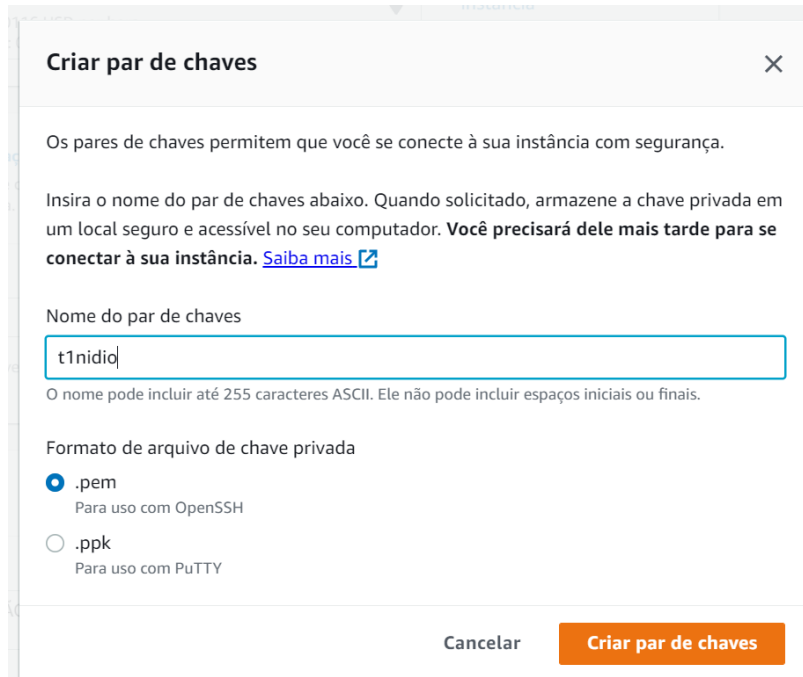
t1nidio

[Criar novo par de chaves](#)

Ou crie uma chave nova (processo abaixo é só pra quem não criou a chave):

Agora, precisamos criar um arquivo de chave privada, para o qual vamos nomear (padrão de nome: turma + seu nome) e baixar o arquivo de chave privada. Em seguida, executamos a instância:

Dica: A chave será nosso meio de autenticação entre nosso equipamento e as instâncias (máquinas virtuais) dentro da AWS, podendo a mesma chave ser utilizada para mais de uma instância, guarde bem a chave para não ter problema de acesso, pois a mesma não pode ser recuperada, terá que ser criada uma nova chave.



Criar par de chaves ✕

Os pares de chaves permitem que você se conecte à sua instância com segurança.

Insira o nome do par de chaves abaixo. Quando solicitado, armazene a chave privada em um local seguro e acessível no seu computador. **Você precisará dele mais tarde para se conectar à sua instância.** [Saiba mais](#)

Nome do par de chaves

t1nidio

O nome pode incluir até 255 caracteres ASCII. Ele não pode incluir espaços iniciais ou finais.

Formato de arquivo de chave privada

☒ .pem
Para uso com OpenSSH

☐ .ppk
Para uso com PuTTY

Cancelar Criar par de chaves

em **Configurações de rede** clique em **Editar**:

Selecione a **VPC-PADRÃO**, verifique está selecionado **Habilitar** a opção **Atribuir IP Público**

Em **Firewall** selecione para criar um novo **grupo de segurança** e coloque o nome seguindo o padrão: sg _ código da turma _ número da mesa _ seu nome: ex: sg_t1_01_nidio

▼ Configurações de rede

VPC - obrigatório [Informações](#)

vpc-0feaf42bebf22baf2 (VPC-PADRÃO)
172.31.0.0/16

(padrão) ▼



Sub-rede [Informações](#)

Sem preferência ▼



[Criar nova sub-rede](#)

Atribuir IP público automaticamente [Informações](#)

Habilitar ▼

Firewall (grupos de segurança) [Informações](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Criar grupo de segurança

☐ Selecionar grupo de segurança existente

Nome do grupo de segurança - obrigatório

sg_t1_01_nidio

Esse grupo de segurança será adicionado a todas as interfaces de rede. Não é possível editar o nome após a criação do grupo de segurança. O comprimento máximo é de 255 caracteres. Os caracteres válidos são: a-z, A-Z, 0-9, espaços e . _ : / () # , @ [] + = & ; [] ! \$ *

Descrição - obrigatório [Informações](#)

launch-wizard-13 created 2022-06-22T18:52:37.244Z

Regras do grupo de segurança de entrada

▼ Regra de grupo de segurança 1 (TCP, 22, 0.0.0.0/0)

Remover

Tipo [Informações](#)

ssh ▼

Protocolo [Informações](#)

TCP

Intervalo de portas [Informações](#)

22

Tipo de origem [Informações](#)

Qualquer lugar ▼

Origem [Informações](#)

Adicionar CIDR, lista de prefixos

0.0.0.0/0 ✕

Descrição - optional [Informações](#)

p. ex. SSH para a área de trabalho d



Regras com origem 0.0.0.0/0 permitem que todos os endereços IP acessem sua instância. Recomendamos configurar regras de grupo de segurança para permitir o acesso apenas de endereços IP conhecidos.



Add security group rule

As configurações de armazenamento e as demais configurações vamos deixar padrão:

▼ Configurar armazenamento [Informações](#)

Avançado

1x GiB ▼ Volume raiz

Os clientes qualificados para o nível gratuito podem obter até 30 GB de armazenamento de uso geral (SSD) ou armazenamento magnético do EBS

✕

Adicionar novo volume

A AMI selecionada contém mais volumes de armazenamento de instâncias do que a instância permite. Somente os primeiros volumes de armazenamento de 0 instâncias da AMI poderão ser acessados pela instância

0 x Sistemas de arquivos [Editar](#)

Vamos executar a instância agora.

▼ Resumo

Número de instâncias [Informações](#)

Imagem do software (AMI)

Canonical, Ubuntu, 22.04 LTS, ...[Ler mais](#)

ami-052efd3df9dad4825

Tipo de servidor virtual (tipo de instância)

t2.micro

Firewall (grupo de segurança)

Novo grupo de segurança

Armazenamento (volumes)

1 volume(s) - 8 GiB

Nível gratuito: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.


✕

Cancelar

Executar instância

Clique no ID da sua instancia:

EC2 > Instâncias > Iniciar uma instância

 **Êxito**
Execução da instância iniciada com êxito **i-0136cd7da48ac02d9**

► Log de execução

Próximas etapas

Obter notificação de cobranças estimadas

[Crie alertas de faturamento](#) para obter uma notificação por e-mail quando as cobranças estimadas na sua fatura da AWS ultrapassarem a quantia definida por você (por exemplo, se tiver excedido o nível de uso gratuito)

Como conectar-se à sua instância

Sua instância está sendo executada e pode demorar alguns minutos até que ela esteja no estado em execução, quando estará pronta para uso

Clique em Exibir instâncias para monitorar o status da sua instância. Assim que sua instância estiver no status "em execução", você poderá se conectar a ela na tela Instâncias. Descubra [como se conectar à sua instância](#)


[Veja mais recursos para começar a usar](#)














[Visualizar todas as instâncias](#)

Agora vamos conectar na nossa instância clicando em conectar:

Resumo da instância para i-0136cd7da48ac02d9 (t101nidio) [Informações](#)

Atualizado há less than a minute

 [Conectar](#) Estado da instância ▼ Ações ▼

ID de instância  i-0136cd7da48ac02d9 (t101nidio)	Endereço IPv4 público  3.237.99.176 endereço aberto 	Endereços IPv4 privados  172.31.1.171
Endereço IPv6 –	Estado da instância  Executando	DNS IPv4 público –
Tipo de nome do host Nome do IP:	Nome do DNS de IP privado (somente IPv4)  ip-172-31-1-171.ec2.internal	Endereços IP elásticos –
Nome do DNS do recurso privado de resposta IPv4 (A)	Tipo de instância t2.micro	Descoberta do AWS Compute Optimizer  Opte por participar do AWS Compute Optimizer para obter recomendações. Saiba mais 
Endereço IP atribuído automaticamente  3.237.99.176 [IP público]	ID da VPC  vpc-0feaf42bebf22baf2 (VPC-PADRÃO) 	Nome do Grupo do Auto Scaling –
Função do IAM –	ID da sub-rede  subnet-089f2373e8ae93e13 	

Selecione Cliente SSH.

EC2 > Instâncias > i-0136cd7da48ac02d9 > Conectar-se à instância

Conectar-se à instância [Informações](#)

Conecte-se à sua instância i-0136cd7da48ac02d9 (t101nidio) usando qualquer uma destas opções

Conexão de instância do EC2

Gerenciador de sessões

Cliente SSH

Console de série do EC2

 Talvez não seja possível conectar-se a essa instância, pois as portas 22 podem precisar estar abertas para serem acessadas. Os grupos de segurança associados atuais não têm as portas 22 abertas. 

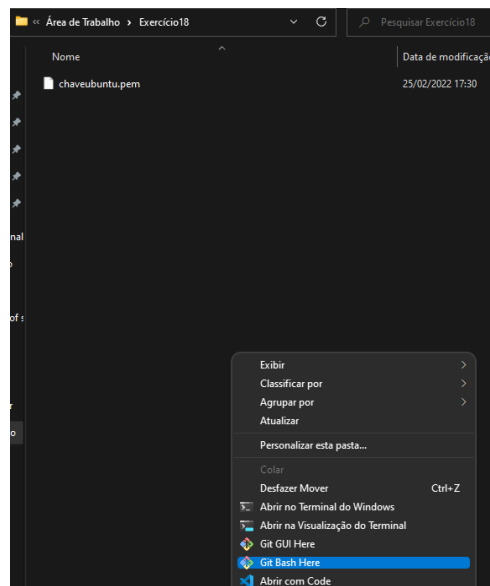
ID de instância
 i-0136cd7da48ac02d9 (t101nidio)

1. Abra um cliente SSH.
2. Localize o arquivo de chave privada. A chave usada para executar esta instância é t1nidio.pem
3. Execute este comando, se necessário, para garantir que sua chave não fique visível publicamente.
 `chmod 400 t1nidio.pem`
4. Conecte-se à sua instância usando sua IP público:
 3.237.99.176

Exemplo:
 `ssh -i "t1nidio.pem" ubuntu@3.237.99.176`

 **Observação:** na maioria dos casos, o nome de usuário suposto está correto. No entanto, leia as instruções de uso da AMI para verificar se o proprietário da AMI alterou o nome de usuário da AMI padrão.

Para acessar a instância executada, devemos encontrar a localização do arquivo .pem em nosso computador e abrir o menu de contexto com o botão direito do mouse em Git Bash Here, ou abra o Git Bash e navegue até onde está localizado o arquivo da sua chave. Para quem usa Linux e MacOS pode usar qualquer terminal.



No Git Bash devemos fazer um **chmod 400 suachave.pem** para alterar as permissões. Dessa forma, garantimos que nossa chave não seja pública.

```
MINGW64:/c/Users/nidio/Desktop/AWS/AULA 18

nidio@jarvis MINGW64 ~/Desktop/AWS/AULA 18
$ chmod 400 t1nidio.pem

nidio@jarvis MINGW64 ~/Desktop/AWS/AULA 18
$ |
```

Copie o exemplo de comando e cole no Git Bash:

EC2 > Instâncias > i-0e6967f368f6e781f > Conectar-se à instância

Conectar-se à instância [Informações](#)

Conecte-se à sua instância i-0e6967f368f6e781f (t101nidio) usando qualquer uma destas opções

[Conexão de instância do EC2](#) | [Gerenciador de sessões](#) | **[Cliente SSH](#)** | [Console de série do EC2](#)

ID de instância
i-0e6967f368f6e781f (t101nidio)

1. Abra um cliente SSH.
2. Localize o arquivo de chave privada. A chave usada para executar esta instância é t2-nidio.pem
3. Execute este comando, se necessário, para garantir que sua chave não fique visível publicamente.
chmod 400 t2-nidio.pem
4. Conecte-se à sua instância usando sua DNS pública:
ec2-35-182-237-107.ca-central-1.compute.amazonaws.com

Exemplo:

```
ssh -i "t2-nidio.pem" ubuntu@ec2-35-182-237-107.ca-central-1.compute.amazonaws.com
```

Observação: na maioria dos casos, o nome de usuário suposto está correto. No entanto, leia as instruções de uso da AMI para verificar se o proprietário da AMI alterou o nome de usuário da AMI padrão.

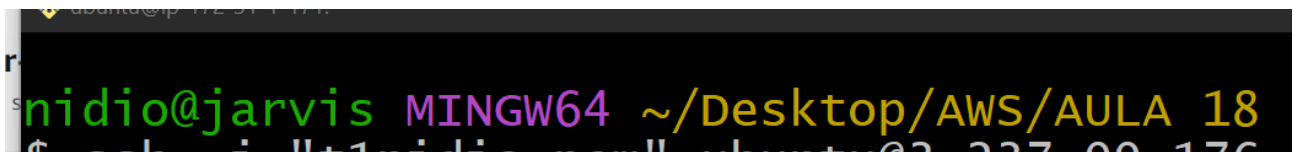
Para conectar, devemos fazer **ssh -i "chave que você criou.pem" ubuntu@endereço DNS da AWS**

```
MINGW64/c:/Users/nidio/Desktop/AWS/AULA 18
nidio@jarvis MINGW64 ~/Desktop/AWS/AULA 18
$ ssh -i "t2-nidio.pem" ubuntu@ec2-35-182-237-107.ca-central-1.compute.amazonaws.com
The authenticity of host 'ec2-35-182-237-107.ca-central-1.compute.amazonaws.com (35.182.237.107)' can't be established.
ED25519 key fingerprint is SHA256:Dqtm4PC2hTrBDEicF6v9liq8dN5K6KCwiCCiXoNu74.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-35-182-237-107.ca-central-1.compute.amazonaws.com' (ED25519) to the list of known hosts.
```

Confirme a chave digitando YES

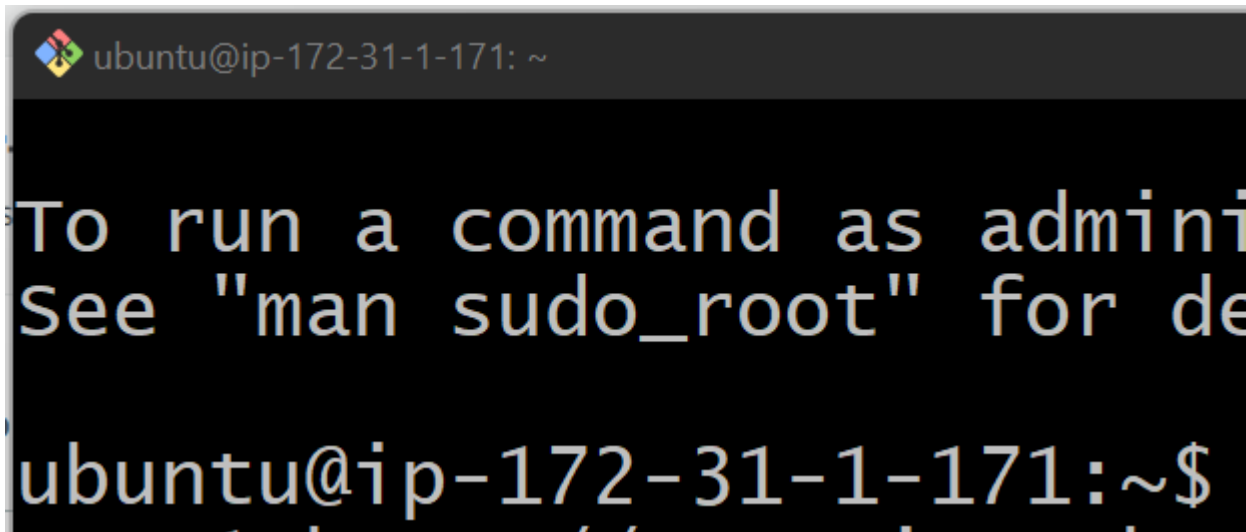
Uma vez logado em nossa instância, devemos instalar o servidor Apache. Para isso, teremos que executar os seguintes comandos (para saber que não está mais no seu terminal e sim no terminal SSH da instância na AWS verifique a diferença de usuários e nome do equipamento:

Usuário do meu computador @ nome do meu computador:



```
nidio@jarvis MINGW64 ~/Desktop/AWS/AULA 18
```

Usuário ubuntu da instância da AWS @ ip- nome da instância na AWS:



```
ubuntu@ip-172-31-1-171: ~
```

To run a command as admini
See "man sudo_root" for de

```
ubuntu@ip-172-31-1-171:~$
```

- **sudo apt-get update**
- **sudo apt-get install apache2**

Digite “y” para confirmar a instalação.



```
ubuntu@ip-172-31-93-236:~$ sudo apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libjansson4 liblua5.2-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
  openssl-blacklist
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libjansson4 liblua5.2-0 ssl-cert
0 upgraded, 11 newly installed, 0 to remove and 75 not upgraded.
Need to get 1865 kB of archives.
After this operation, 8091 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Para verificar se nosso servidor está rodando, teremos que fazer: **systemctl status apache2**. Devemos ver o seguinte retorno:

```
ubuntu@ip-172-31-93-236:~$ systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: en>
   Active: active (running) since Fri 2022-02-25 20:41:16 UTC; 16min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2138 (apache2)
    Tasks: 55 (limit: 1147)
   Memory: 5.1M
   CGroup: /system.slice/apache2.service
           └─2138 /usr/sbin/apache2 -k start
             └─2140 /usr/sbin/apache2 -k start
               └─2141 /usr/sbin/apache2 -k start

Feb 25 20:41:16 ip-172-31-93-236 systemd[1]: Starting The Apache HTTP Server...
Feb 25 20:41:16 ip-172-31-93-236 systemd[1]: Started The Apache HTTP Server.
lines 1-14/14 (END)
```

Como último passo, teremos que modificar o **security group** do nosso servidor para aceitar conexões da porta 80. Para isso, teremos que abrir o security group de nossa instância para saber o nome da nossa porta. Podemos vê-lo na instância:

EC2 > Instâncias > i-026a39116b70f2f5d

Resumo da instância para i-026a39116b70f2f5d [Informações](#)
Atualizado há less than a minute

[Conectar](#) [Estado da instância](#) [Ações](#)

ID de instância i-026a39116b70f2f5d	Endereço IPv4 público 44.203.72.3 endereço aberto
Endereço IPv6 -	Estado da instância Executando
Tipo de nome do host Nome do IP: ip-172-31-93-236.ec2.internal	Nome do DNS de IP privado (somente) ip-172-31-93-236.ec2.internal
Tipo de instância t2.micro	Endereços IP elásticos -
Descoberta do AWS Compute Optimizer Opte por participar do AWS Compute Optimizer para obter recomendações. Saiba mais	Função do IAM -

Detalhes **Segurança** Redes Armazenamento Verificações de st

▼ Detalhes de segurança

Função do IAM -	ID do proprietário 405378853534
Grupos de segurança sg-0efd0971414a759f5 (launch-wizard-2)	

Lá, vamos seleccionar o grupo da nossa instância e ir em “Editar regras de entrada”.

Regras de entrada | Regras de saída | Tags

Agora, você pode verificar a conectividade de rede com o Reachability Analyzer [Executar Reachability Analyzer](#)

Regras de entrada (1/1) [Gerenciar tags](#) [Editar regras de entrada](#)

<input checked="" type="checkbox"/>	Name	ID da regra do grup...	Versão do IP	Tipo	Protocolo
<input checked="" type="checkbox"/>	-	sgr-0431dff7fd755a4f7	IPv4	SSH	TCP

Em seguida, precisamos adicionar uma regra. Procuramos **HTTP** para seleccionar a porta 80 e em “Origem” seleccionamos “Qualquer local-Ipv4”. Salvamos as alterações.

Editar regras de entrada [Informações](#)

As regras de entrada controlam o tráfego de entrada que tem permissão para acessar a instância.

Regras de entrada [Informações](#)

ID da regra do grupo de segurança	Tipo Informações	Protocolo Informações	Intervalo de portas Informações	Origem Informações	Descrição - opcional Informações	
sgr-0431dff7fd755a4f7	SSH	TCP	22	Qualqu... <input type="text" value="0.0.0.0/0"/>		Excluir
-	HTTP	TCP	80	Qualqu... <input type="text" value="0.0.0.0/0"/>		Excluir

Adicionar regra

Cancelar

Visualizar alterações

Salvar regras

Por fim, precisaremos encontrar o endereço de nossa instância e copiá-lo para barra de endereços do nosso navegador. Ele irá copiá-lo para nós com "https", então teremos que corrigi-lo para que seja "http", ou podemos digitar o IPv4 público na barra de endereço do navegador.

EC2 > Instâncias > i-026a39116b70f2f5d

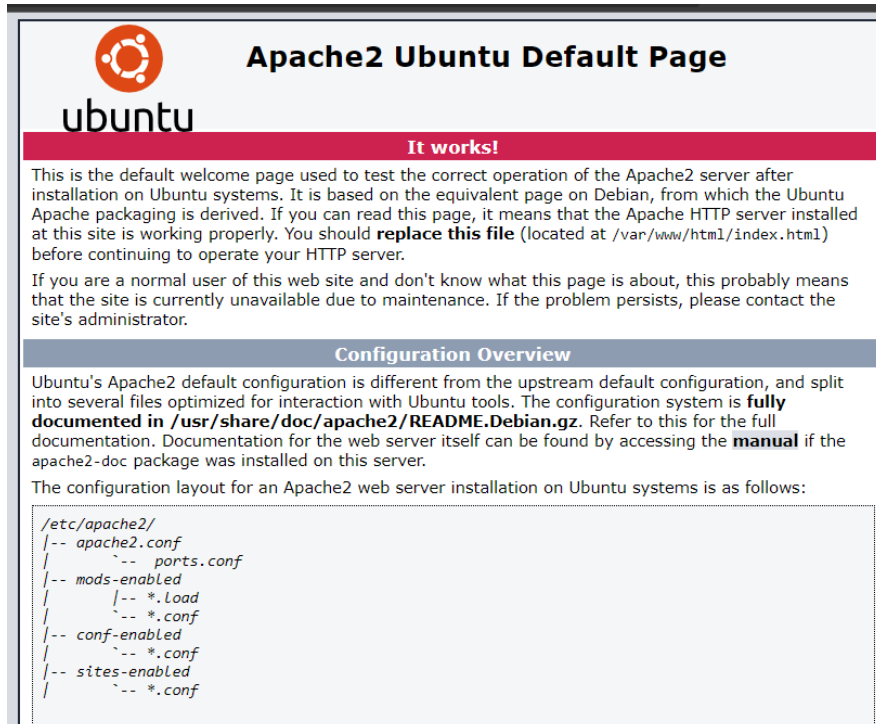
Resumo da instância para i-026a39116b70f2f5d [Informações](#)

Atualizado há less than a minute

[Atualizar](#) [Conectar](#) [Estado da instância](#) [Ações](#)

ID de instância i-026a39116b70f2f5d	Endereço IPv4 público 44.203.72.3 endereço aberto	Endereços IPv4 privados 172.31.93.236
Endereço IPv6 -	Estado da instância Executando	DNS IPv4 público ec2-44-203-72-3.compute-1.amazonaws.com endereço aberto
Tipo de nome do host Nome do IP: ip-172-31-93-236.ec2.internal	Nome do DNS de IP privado (somente IPv4) ip-172-31-93-236.ec2.internal	Nome do DNS do recurso privado de resposta -
Tipo de instância t2.micro	Endereços IP elásticos -	ID da VPC vpc-0b8469a0f1535c075

Se você vir a tela a seguir, parabéns, você concluiu o exercício!



The screenshot shows the Apache2 Ubuntu Default Page. At the top, there is a header with the Ubuntu logo and the text "ubuntu". Below this, a red banner reads "It works!". The main content area contains a paragraph explaining that this is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It mentions that the page is based on the equivalent page on Debian and that if you can read this page, it means that the Apache HTTP server installed at this site is working properly. It also states that you should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server. Below this, a section titled "Configuration Overview" explains that Ubuntu's Apache2 default configuration is different from the upstream default configuration and is split into several files optimized for interaction with Ubuntu tools. It mentions that the configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz and refers to this for the full documentation. It also states that documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server. Finally, it states that the configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/  
|-- apache2.conf  
|   |-- ports.conf  
|-- mods-enabled  
|   |-- *.load  
|   |-- *.conf  
|-- conf-enabled  
|   |-- *.conf  
|-- sites-enabled  
|   |-- *.conf  
|
```