

## Relatório de Configuração de Instância EC2 na AWS

Este relatório detalha o processo de implantação da aplicação ServeRest em uma instância EC2 da Amazon Web Services (AWS) pela Squad Level UP. O objetivo principal desta atividade foi praticar a configuração e o uso da AWS EC2, bem como a implantação de aplicações em ambientes de nuvem. Este documento aborda o passo a passo seguido, os comandos executados e os desafios superados durante o processo.

### Membros da Squad Level UP

Função	Nome
Lider	@Isa Reginabs
Membro	@Eric Lima da Silva
Membro	@Ivo Sobral dos Santos Junior
Membro	@João Gabriel Oliveira Magalhães
Membro	@Maycon Douglas Da Silva

### Ferramentas Utilizadas

Ferramenta	Descrição
AWS EC2	Serviço de computação em nuvem para provisionamento da instância.
Node.js	Ambiente de execução JavaScript para o ServeRest.
npm/npx	Gerenciador de pacotes Node.js para instalação e execução do ServeRest.
Curl	Ferramenta de linha de comando para transferência de dados.
Yum	Gerenciador de pacotes para sistemas Linux.
Git	Sistema de controle de versão para o repositório do projeto.

### 1. Criação e Organização da Pasta de Acesso

Antes de iniciar a configuração no Console AWS, foi criada **uma pasta local de fácil localização** para armazenar a chave de acesso (.pem) que será utilizada para autenticação na instância.

### 2. Criação do Par de Chaves

1. No **Console AWS**, acessou-se o campo de busca e digitou-se **EC2**, abrindo o **Dashboard EC2**.

- No menu lateral, dentro do grupo **Rede e segurança**, foi selecionada a opção **Pares de chaves**.
- Foi clicado em **Criar par de chaves**.

**Criar par de chaves** Informações

**Par de chaves**  
Um par de chaves, que consiste em uma chave privada e uma chave pública, é um conjunto de credenciais de segurança que você usa para provar sua identidade ao se conectar a uma instância.

**Nome**  
Insira o nome do par de chaves.  
O nome pode incluir até 255 caracteres ASCII. Ele não pode incluir espaços nem os caracteres . ou ~.

**Tipo de par de chaves** Informações  
☒ RSA ☐ ED25519

**Formato de arquivo de chave privada**  
☐ .pem  
Para uso com OpenSSH

☒ .pem  
Para uso com PuTTY

**Tag — opcional**  
Insira uma tag associada ao recurso.

[Adicionar nova tag](#)  
Você pode adicionar até mais 50 etiquetas.

[Cancelar](#) [Criar par de chaves](#)

- As configurações escolhidas para o par de chaves foram:
  - Nome:** Definido de acordo com o projeto.
  - Tipo de chave:** RSA
  - Formato do arquivo:** .pem
- Após a criação, o download da chave foi feito automaticamente.
- O arquivo foi movido para a pasta criada anteriormente.

### 3. Configuração do Internet Gateway e da Rede

No console, foi utilizada a barra de pesquisa para localizar o recurso **Internet Gateway**.

#### Observação:

*Antes de configurar o gateway, mudar o servidor para Norte da Virgínia us-east-1, para que futuramente não precise reconfigurar o gateway, já que ele fica vinculado ao servidor selecionado. No tutorial, no console já está definido us-east-1, mas só depois de configurado que é orientado mudar o servidor para us-east-1. Causando confusão e falha ao tentar conectar pelo terminal.*

#### 3.1 Criação e Associação do Internet Gateway

- No menu lateral, foi acessada a opção **Gateways da Internet**.
- Foi clicado em **Criar Gateway da Internet** e definido um nome para o recurso.

**Criar gateway da Internet** Informações

Um gateway da Internet é um roteador virtual que conecta uma VPC à Internet. Para criar um novo gateway da Internet, especifique o nome dele abaixo.

**Configurações do gateway da Internet**

**Tag de nome**  
Crie uma tag com uma chave de "Name" e um valor que você especifica.

**Tags - opcional**  
Uma tag é um rótulo que você atribui a um recurso da AWS. Cada tag consiste em uma chave e um valor opcional. Você pode usar tags para pesquisar e filtrar seu recurso.

**Chave** **Valor - opcional**

[Adicionar nova tag](#)  
Você pode adicionar mais 49 tags.

- Após criado, o sistema redirecionou para a tela de detalhes do gateway.

**Gateways da internet (1)** Informações

<input type="checkbox"/>	Name	
<input type="checkbox"/>	ec2-serverest-gateway	jt

4. Clicou-se em **Ações > Associar à VPC**.
5. Na lista de VPCs disponíveis, foi selecionada a VPC já existente e clicado em **Associar Gateway da Internet**.



### 3.2 Configuração da Tabela de Rotas

1. Voltando ao menu lateral, foi selecionada **Tabelas de Rotas**.
2. Entre as tabelas disponíveis, foi escolhida a tabela **não marcada como principal** (a tabela principal já vem configurada por padrão).



3. Com a tabela selecionada, na aba **Rotas**, clicou-se em **Editar rotas**.
4. Foi adicionada uma nova rota:
- **Destino:** 0.0.0.0/0
  - **Alvo:** Gateway da Internet criado anteriormente.
5. A configuração foi salva, liberando acesso à internet para a VPC associada.

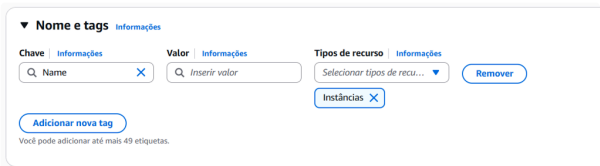
## 4. Criação da Instância EC2

Após a configuração de rede e segurança, iniciou-se a criação da instância EC2:

### 4.1. Nomeação e Tags

1. Voltando ao **Dashboard EC2**, clicou-se em **Executar Instâncias**.
2. Em **Nome e Tags**, foi adicionado:

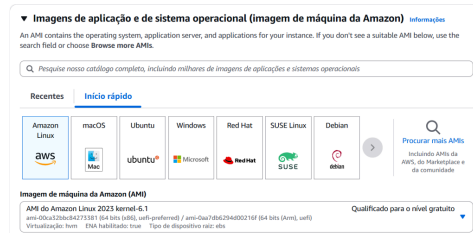
Chave	Valor	Tipo de
Name	Linux Serverest	Instâncias e Volumes
Project	Programa de Bolsas	Instâncias e Volumes
CostCenter	Quality Assurance	Instâncias e Volumes



3. Apenas estas três tags foram criadas, conforme orientado pelo tutorial.

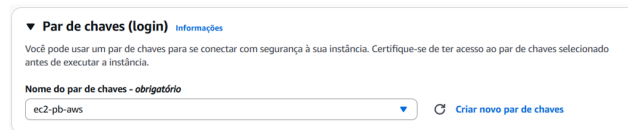
## 4.2. Configurações de Sistema Operacional e Instância

### 1. Imagem do Sistema Operacional: Amazon Linux (64 bits).



### 2. Tipo de Instância: t2.micro (padrão e elegível ao nível gratuito).

### 3. Par de Chaves: Selecionado o par de chaves criado anteriormente.

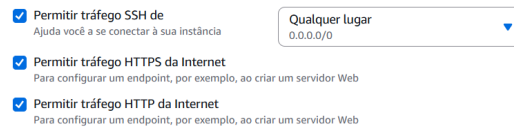


## 4.3. Configuração de Rede e Segurança

### 1. As regras de segurança foram configuradas para permitir:

- **SSH:** Acesso de qualquer lugar.
- **HTTPS:** Acesso da internet.
- **HTTP:** Acesso da internet.

Criaremos um novo grupo de segurança chamado "launch-wizard-4" com as seguintes regras:



### 2. O IP público da instância foi habilitado (opção padrão é desativada).



### 3. Uma nova regra de grupo de segurança foi adicionada para permitir tráfego na porta **3000/TCP**, que será utilizada pelo serviço Serverest:

- **Tipo:** TCP personalizado
- **Protocolo:** TCP
- **Intervalo de portas:** 3000
- **Origem:** Qualquer lugar

**Regras do grupo de segurança de entrada**

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

<b>Tipo</b>   <a href="#">Informações</a>	<b>Protocolo</b>   <a href="#">Informações</a>	<b>Intervalo de portas</b>   <a href="#">Informações</a>
ssh	TCP	22
<b>Tipo de origem</b>   <a href="#">Informações</a>	<b>Origem</b>   <a href="#">Informações</a>	<b>Descrição (opcional)</b>   <a href="#">Informações</a>
Qualquer lugar	Adicionar CIDR, lista de prefixos ou grupo de	p. ex. SSH para a área de trabalho do administrador
	0.0.0.0/0	

▼ Regra de grupo de segurança 2 (TCP: 443, 0.0.0.0/0) Remover

<b>Tipo</b>   <a href="#">Informações</a>	<b>Protocolo</b>   <a href="#">Informações</a>	<b>Intervalo de portas</b>   <a href="#">Informações</a>
HTTPS	TCP	443
<b>Tipo de origem</b>   <a href="#">Informações</a>	<b>Origem</b>   <a href="#">Informações</a>	<b>Descrição (opcional)</b>   <a href="#">Informações</a>
Qualquer lugar	Adicionar CIDR, lista de prefixos ou grupo de	p. ex. SSH para a área de trabalho do administrador
	0.0.0.0/0	

▼ Regra de grupo de segurança 3 (TCP: 80, 0.0.0.0/0) Remover

<b>Tipo</b>   <a href="#">Informações</a>	<b>Protocolo</b>   <a href="#">Informações</a>	<b>Intervalo de portas</b>   <a href="#">Informações</a>
HTTP	TCP	80
<b>Tipo de origem</b>   <a href="#">Informações</a>	<b>Origem</b>   <a href="#">Informações</a>	<b>Descrição (opcional)</b>   <a href="#">Informações</a>
Qualquer lugar	Adicionar CIDR, lista de prefixos ou grupo de	p. ex. SSH para a área de trabalho do administrador
	0.0.0.0/0	

▼ Regra de grupo de segurança 4 (TCP: 3000, 0.0.0.0/0) Remover

<b>Tipo</b>   <a href="#">Informações</a>	<b>Protocolo</b>   <a href="#">Informações</a>	<b>Intervalo de portas</b>   <a href="#">Informações</a>
TCP personalizado	TCP	3000
<b>Tipo de origem</b>   <a href="#">Informações</a>	<b>Origem</b>   <a href="#">Informações</a>	<b>Descrição (opcional)</b>   <a href="#">Informações</a>
Qualquer lugar	Adicionar CIDR, lista de prefixos ou grupo de	p. ex. SSH para a área de trabalho do administrador
	0.0.0.0/0	

#### 4.4. Armazenamento

O armazenamento padrão foi mantido em **8 GiB**, **tipo gp3**, garantindo desempenho básico para a instância.

**Configurar armazenamento** | [Informações](#) Avançado

1x 8 GiB gp3 | Volume raiz, 3000 IOPS, Não criptografado

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

[Adicionar novo volume](#)

Clique em atualizar para visualizar as informações de backup

As tags que você atribui determinam se o backup da instância será feito por alguma política do Data Lifecycle Manager.

0 x Sistemas de arquivos Editar

#### 4.5. Execução da Instância

Após revisão das configurações, clicou-se em **Executar Instâncias**, concluindo com sucesso a criação da instância EC2.

### 5. Conexão à Instância EC2 via SSH

Após a configuração da instância, foi necessário acessar a máquina virtual na AWS via SSH para instalar dependências e configurar o ambiente.

#### 1. Acesso ao Painel de Conexão:

- No **Console da AWS**, selecionou-se a instância EC2 e clicou-se em **Conectar-se à instância**.
- Na aba **Conexão de instância do EC2**, foi exibido o **IP público** da instância, que foi **anotado para uso posterior**.
- Em seguida, acessou-se a aba **Cliente SSH**, onde são fornecidos os comandos de conexão.

**Conectar** | [Informações](#)

Conecte-se a uma instância usando o cliente baseado em navegador.

Conexão de instância do EC2 | Gerenciador de sessões | **Cliente SSH** | Console de série do EC2

**ID da instância**

i-0ae3d3b08641034b2 (Linux Server)

- Abra um cliente SSH.
- Localize o arquivo de chave privada. A chave usada para executar esta instância é ec2-aws.pem
- Execute este comando, se necessário, para garantir que sua chave não fique visível publicamente.
- Conecte-se à sua instância usando sua DNS pública:

Exemplo:

ssh -i [chave privada] [nome de usuário]@compute-1.amazonaws.com

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

#### 2. Acesso ao Diretório da Chave de Acesso:

- No terminal, acessou-se a pasta onde o arquivo **.pem** foi armazenado:

```
1 cd /home/usuario/pasta
```

- Em seguida, listou-se o conteúdo da pasta para confirmar a presença da chave:

```
1 ls
```

A chave `ec2-pb-aws.pem` estava disponível no diretório.

### 3. Ajuste de Permissões da Chave:

Para garantir a segurança do arquivo `.pem`, foi aplicado o comando sugerido:

```
1 chmod 400 ec2-pb-aws.pem
```

### 4. Conexão via SSH:

Utilizando o IP público anotado, foi executado:

```
1 ssh -i "ec2-pb-aws.pem" ec2-user@<IP_PÚBLICO>
```

Ao aparecer a mensagem:

```
Are you sure you want to continue connecting (yes/no)?
```

Foi digitado `yes` e pressionado `Enter`.

A partir desse ponto, a sessão SSH com a instância EC2 foi estabelecida com sucesso.

## 6. Atualização e Instalação de Pacotes Essenciais

Com a conexão estabelecida, iniciou-se a configuração do ambiente:

### 1. Atualização do Sistema:

```
1 sudo yum update -y
```

Esse comando garantiu que todos os pacotes da distribuição Amazon Linux estivessem atualizados.

### 2. Instalação de Compiladores e Ferramentas:

```
1 sudo yum install gcc-c++ make -y
```

### 3. Verificação e Instalação do cURL:

◦ Verificação:

```
1 curl --version
```

◦ Caso o `curl` não estivesse instalado, foi executado:

```
1 sudo yum install curl -y
```

## 7. Criação do Diretório de Projeto e Instalação do Node.js

### 1. Criação da pasta para o Serverest:

```
1 mkdir serverestApi
2 cd serverestApi
```

### 2. Instalação do Node.js:

A instalação recomendada no tutorial com `curl` não funcionou. Utilizou-se a instalação direta com:

```
1 sudo yum install -y nodejs
```

## 8. Inicialização do Serverest

Para instalar e executar a API Serverest diretamente:

```
1 npx serverest@latest
```

Ao iniciar o Serverest, a API ficou disponível na **porta 3000** da instância EC2.

Com isso, foi possível acessar a interface Swagger do Serverest diretamente pelo navegador utilizando:

```
1 http://<IP_PÚBLICO>:3000
```

Substituindo **<IP\_PÚBLICO>** pelo endereço anotado anteriormente.

A página do Swagger confirmou que o **Serverest** estava em execução e acessível pela internet.

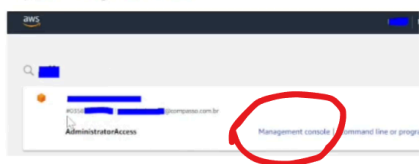
## 9. Desafios:

- **Desafio:** Um dos desafios encontrado pelos integrantes do squad é que há mudanças, mesmo que sutis, entre a plataforma da AWS e as vídeos aulas, por exemplo:
  - Na vídeo aula, no momento da criação do gateway da internet, mostra que não há nenhuma VPC associado a outro gateway, mas na plataforma o VPC está associado a outro gateway automaticamente criado. Isso causou um pouco de confusão.
- **Desafio:** Outro desafio que deve ser citado é a ocorrência de erro, especificamente o erro timeout, que poderia ter sido evitado se na vídeo aula fosse abordado primeiramente que a região deveria ser alterada para Norte-Virgina us-east-1, pois essa informação foi falada em um momento que o gateway de internet já tinha sido criado e associado a uma vpc em outra região, causando assim o erro.
- **Desafio:** Um dos desafios aconteceu quando foi acessado o link disponibilizado e redirecionado para uma página relativamente diferente do tutorial. Enquanto o instrutor falava para clicarmos em **management console**, essa opção não existia na plataforma atual.
  - **Resolução:** Foi realizado uma reunião com outro integrante e dessa forma descobrimos que a opção correta para seguir com os passo a passo era **AdministratorAccess**.

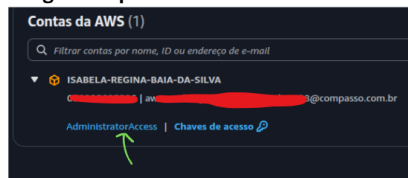
### Imagem do tutorial

Após o login irá aparecer a sua conta de lab com o seu nome.

Clique em <Management Console>



### Imagem da plataforma atual



- **Desafio:** No momento de copiar o IP publica (conforme o instrutor nos ensinou) para a URL, gerou erro.
  - **Resolução:** Mesmo que essa instrução de copiar o IP publico tenha funcionado com outros colegas da squad, não foi o caso de outros. Desse modo, foi necessário especificar a rota assim: <http://3.236.177.234:3000/>

**Instâncias (1)** [Informações](#)

Localizar instância por atributo ou tag (case-sensitive) Todos os ...

Estado da inst...	Tipo de inst...	Verificação de stat	Status do alarm	Zona de dispon...	DNS IPv4 público	Endereço IP...
Executando	t2.micro	2/2 verificações a	Exibir alarmes +	us-east-1b	ec2-3-236-177-234.co...	3.236.177.234

