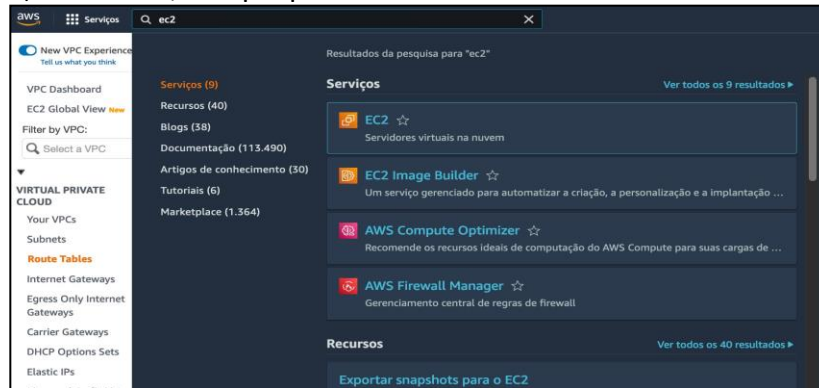


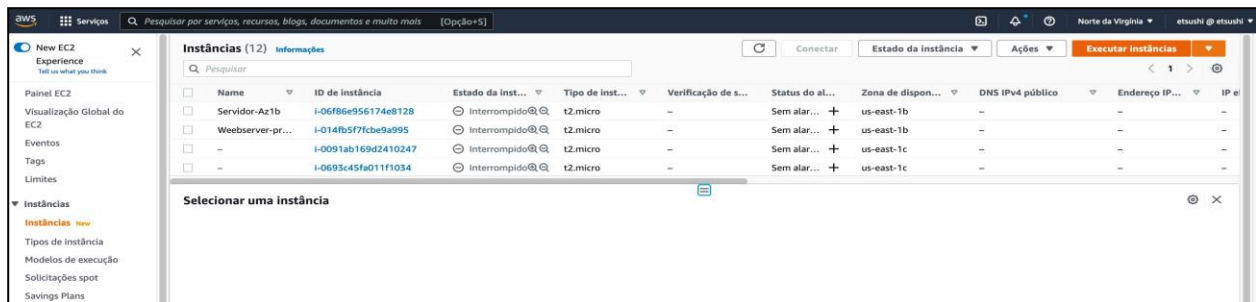
# Cloud Security – Laboratório 1

Usuário, Role e registros de acesso no CloudTrail.

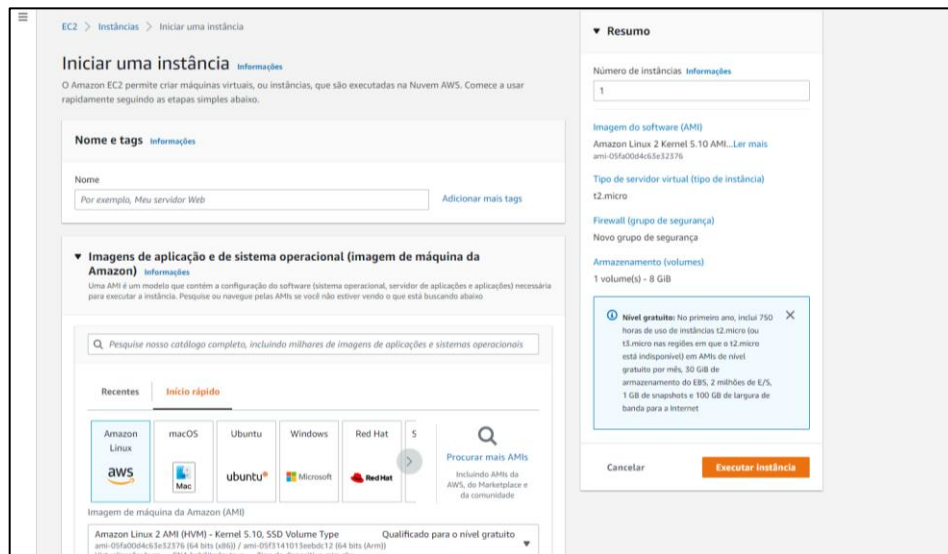
1) No menu, busque por EC2.



2) Clique em “Executar Instâncias”



3) Dê um nome para a instância e selecione o tipo Amazon Linux (primeira opção)



4) Selecione o tipo de instância – t2.micro, prossiga sem um par de chaves

NS **Serviços**  [Alt+S]

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

Tipo de instância

t2.micro Qualificado para o nível gratuito [Comparar tipos de instância](#)

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

**▼ 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*

Valor padrão [Criar novo par de chaves](#)

**▼ Configurações de rede** [Obtenha orientação](#) [Editar](#)

Rede [Informações](#)  
 vpc-07b6f3edf49180e04 | grup4-vpc-virginia

Sub-rede [Informações](#)  
 subnet-01af10b7169f6a388 | subnet-grupo4-virginia

Atribuir IP público automaticamente [Informações](#)  
 Desabilitar

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

Um grupo de segurança é um conjunto de regras de firewall que controlam o tráfego para sua instância. Adicione regras para permitir que o tráfego específico alcance sua instância.

☒ Criar grupo de segurança ☐ Selecionar grupo de segurança existente

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

**▼ Resumo**

Número de instâncias [Informações](#)

**Imagem do software (AMI)**  
 Amazon Linux 2 Kernel 5.10 AMI...[Ler mais](#)  
 ami-05fa00d4c63e32376

**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:** No primeiro ano, inclui 750 horas de uso de instâncias t2.micro (ou t3.micro nas regiões em que o t2.micro está indisponível) em AMIs de nível gratuito por mês, 30 GiB de armazenamento do EBS, 2 milhões de E/S, 1 GB de snapshots e 100 GB de largura de banda para a Internet

[Cancelar](#) [Executar instância](#)

5) Mantenha as configurações de rede, tenha certeza da opção: Auto-assign Public IP: Habilitar.

6) Nos grupos de segurança, adicione uma regra para permitir conexão na porta 80 (HTTP):

Desabilitar [▼](#)

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

Um grupo de segurança é um conjunto de regras de firewall que controlam o tráfego para sua instância. Adicione regras para permitir que o tráfego específico alcance sua instância.

☒ Criar grupo de segurança ☐ Selecionar grupo de segurança existente

Nome do grupo de segurança - *obrigatório*

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](#)

**Regras do grupo de segurança de entrada**

▶ Regra de grupo de segurança 1 (TCP, 22, 0.0.0.0/0) [Remover](#)

▼ Regra de grupo de segurança 2 (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>
<input type="text" value="HTTP"/>	<input type="text" value="TCP"/>	<input type="text" value="80"/>
<b>Tipo de origem</b> <a href="#">Informações</a>	<b>Origem</b> <a href="#">Informações</a>	<b>Descrição - optional</b> <a href="#">Informações</a>
<input type="text" value="Qualquer lugar"/>	<input type="text" value="Adicionar CIDR, lista de prefixo"/> <input type="text" value="0.0.0.0/0"/>	<input type="text" value="p. ex. SSH para a área de trabalho"/>

**⚠ 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.**

[Adicionar regra de grupo de segurança](#)

**▼ Resumo**

Número de instâncias [Informações](#)

**Imagem do software (AMI)**  
 Amazon Linux 2 Kernel 5.10 AMI...[Ler mais](#)  
 ami-05fa00d4c63e32376

**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:** No primeiro ano, inclui 750 horas de uso de instâncias t2.micro (ou t3.micro nas regiões em que o t2.micro está indisponível) em AMIs de nível gratuito por mês, 30 GiB de armazenamento do EBS, 2 milhões de E/S, 1 GB de snapshots e 100 GB de largura de banda para a Internet

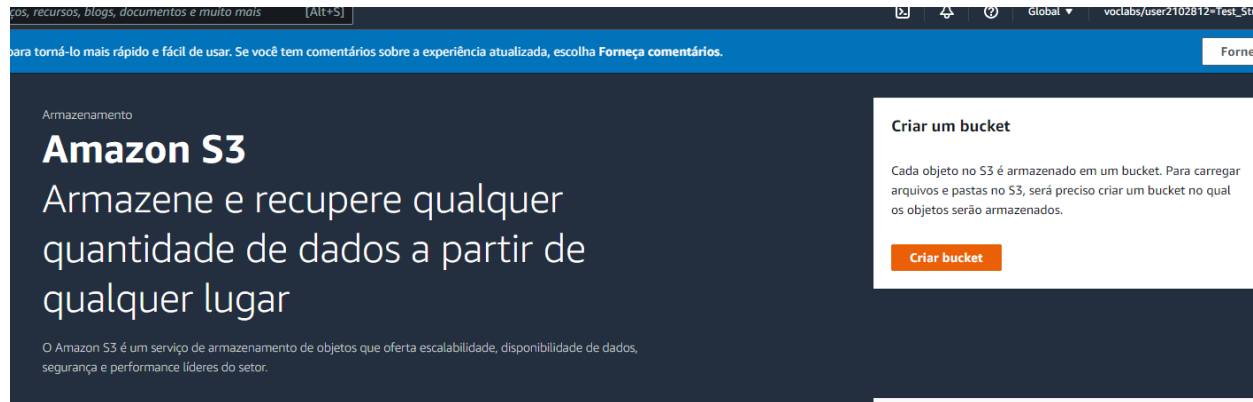
[Cancelar](#) [Executar instância](#)

7) Clique em “Detalhes avançados” e selecione um Perfil de instância: LabInstanceProfile

8) Revise as opções selecionadas e clique em “Executar Instância”

## 9) Criar Bucket S3:

1. Do console de gerenciamento AWS, escolha **serviços** e selecione **S3** em armazenamento
2. Clique em **Criar Bucket**



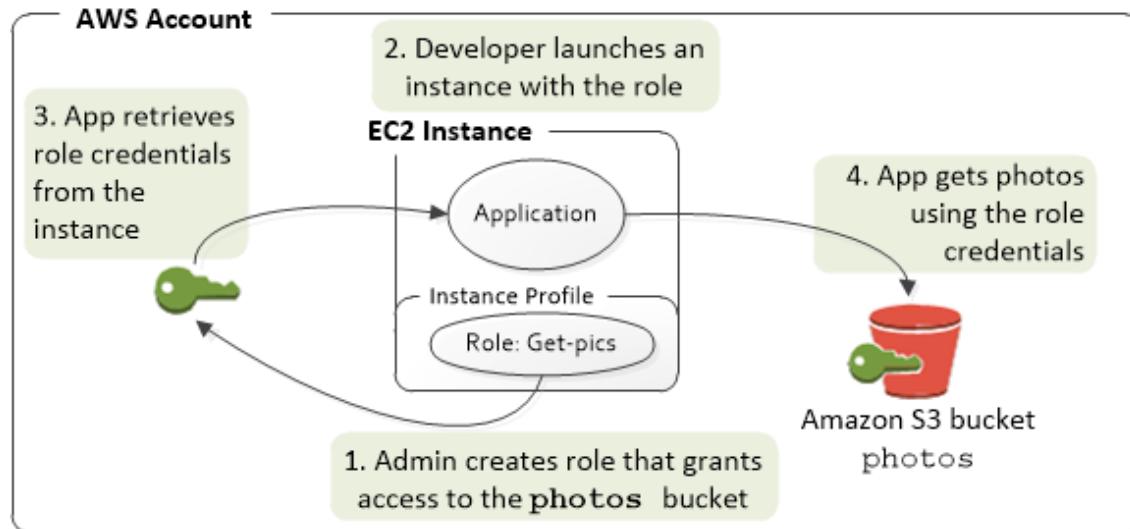
3. Para o **nome do bucket**, digite um nome de bucket único
4. Para **Região**, escolha us-east-1

A screenshot of the Amazon S3 console's 'Criar bucket' (Create bucket) page, showing the configuration form. The 'Nome do bucket' (Bucket name) field is filled with 'meunovobucket'. The 'Região da AWS' (AWS Region) dropdown is set to 'Leste dos EUA (Norte da Virgínia) us-east-1'. The 'Propriedade de objeto' (Object ownership) section shows 'ACLs desabilitadas (recomendado)' (Disabled ACLs (recommended)) selected. The 'Copiar configurações do bucket existente' (Copy bucket configuration from existing bucket) section has an 'Escolher bucket' button.

5. Mantenha as outras configurações padrão
6. Clique em **Criar**
7. Clique no bucket que você acabou de criar e faça upload de algum arquivo para o seu novo bucket. Pode ser um simples arquivo de texto.

Use a instância EC2 para acessar o recurso S3:

Você lançou a instância EC2 assumindo o papel IAM que tem permissão para o S3. Agora vamos usar a instância EC2 para acessar o S3 usando o AWS CLI.



1. Conecte-se à sua instância EC2 usando O SSH
2. comando de execução: **aws --version**
3. Mostrando a versão atual do AWS CLI
4. Por padrão, a ferramenta AWS CLI está incluída no Amazon Linux AMI:
5. Execute o seguinte comando: **aws s3 ls**
6. Você deve ver uma lista de buckets da sua conta
7. Execute o seguinte comando: **aws s3 ls <nome-do-seu-bucket>**
8. Você deve ver o arquivo que está dentro do bucket.

### Encontre a Access Key de instância EC2 e a Secret Key

Até agora, notei que você nunca gera ou codificar qualquer chave de acesso / chave secreta para o seu aplicativo no EC2 para acessar o S3.

Porque quando você lança a instância Ec2 você a associa com o **IAM Role**. Esta é a melhor prática para permitir que a AWS gere **credencial temporária (chave de acesso/chave secreta)**

A **credencial temporária** é armazenada em metadados de instância EC2.

Veja como ver a credencial temporária da EC2 atual

- Acesse a sua EC2 para linha de comando
- Execute o comando:
  - `TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" \`
  - `&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/iam/security-credentials/LabRole`
- A credencial temporária deve ser algo como:

```
{
  "Code" : "Success",
```

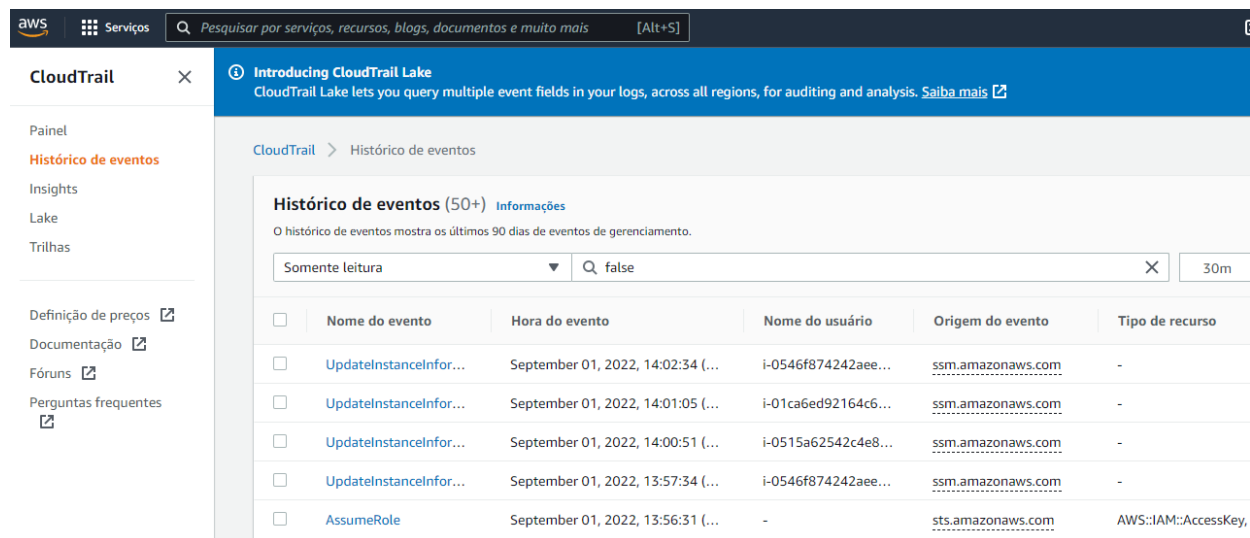
```

"LastUpdated" : "2012-04-26T16:39:16Z",
"Type" : "AWS-HMAC",
"AccessKeyId" : "ASIAIOSFODNN7EXAMPLE",
"SecretAccessKey" : "wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY",
"Token" : "token",
"Expiration" : "2017-05-17T15:09:54Z"
}

```

Exibir atividade da API através do console **CloudTrail**:

1. Do console de gerenciamento AWS, escolha **serviços** e selecione **CloudTrail**
2. No painel de navegação, escolha o **Histórico de eventos**



**CloudTrail** ×

**Introducing CloudTrail Lake**  
CloudTrail Lake lets you query multiple event fields in your logs, across all regions, for auditing and analysis. [Saiba mais](#)

CloudTrail > Histórico de eventos

**Histórico de eventos (50+)** [Informações](#)

O histórico de eventos mostra os últimos 90 dias de eventos de gerenciamento.

Somente leitura ▼ Q false X 30m

<input type="checkbox"/>	Nome do evento	Hora do evento	Nome do usuário	Origem do evento	Tipo de recurso
<input type="checkbox"/>	<a href="#">UpdateInstanceInfor...</a>	September 01, 2022, 14:02:34 (...)	i-0546f874242aee...	ssm.amazonaws.com	-
<input type="checkbox"/>	<a href="#">UpdateInstanceInfor...</a>	September 01, 2022, 14:01:05 (...)	i-01ca6ed92164c6...	ssm.amazonaws.com	-
<input type="checkbox"/>	<a href="#">UpdateInstanceInfor...</a>	September 01, 2022, 14:00:51 (...)	i-0515a62542c4e8...	ssm.amazonaws.com	-
<input type="checkbox"/>	<a href="#">UpdateInstanceInfor...</a>	September 01, 2022, 13:57:34 (...)	i-0546f874242aee...	ssm.amazonaws.com	-
<input type="checkbox"/>	<a href="#">AssumeRole</a>	September 01, 2022, 13:56:31 (...)	-	sts.amazonaws.com	AWS::IAM::AccessKey,

3. Uma lista de eventos aparece no painel de conteúdo com o evento mais recente primeiro.
4. Role para baixo para ver mais eventos. Procure pelo evento “ListBuckets” com o access key que voce usou na sua role.
5. Se você quiser ações de usuário específico
  1. Para **filtrar**, selecione o **nome do usuário**
  2. **Digite o Usuário IAM** que você criou anteriormente
  3. Clique **em Entrar** ou **Atualizar** ícone no lado direito
  4. Ele mostrará os registros relacionados