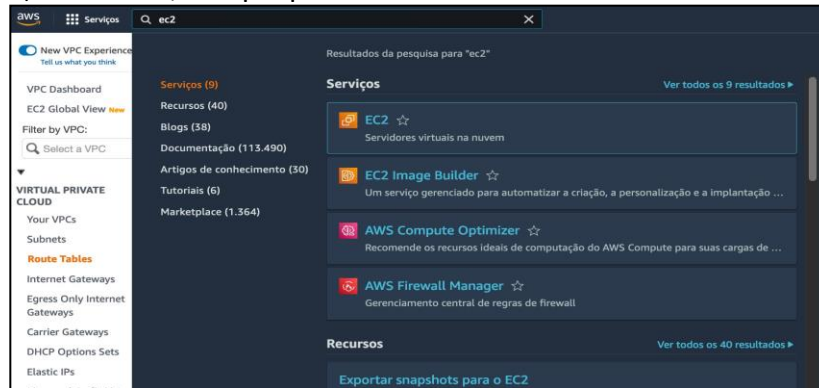


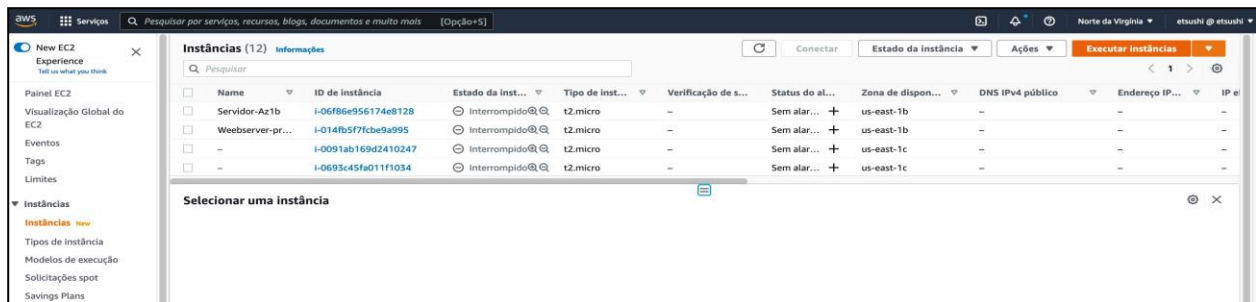
Cloud Security – Laboratório 1

Usuário, Role e registros de acesso no CloudTrail.

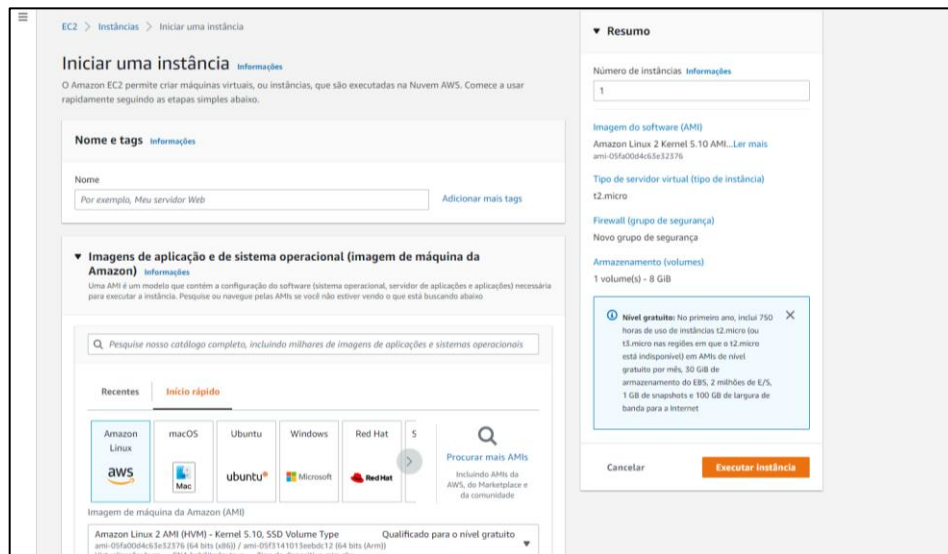
1) No menu, busque por EC2.



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

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

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

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

8) 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

Amazon S3 > Buckets > Criar bucket

Criar bucket [Informações](#)

Os buckets são contêineres para dados armazenados no S3. [Saiba mais](#)

Configuração geral

Nome do bucket

O nome do bucket deve ser globalmente exclusivo e não deve conter espaços ou letras maiúsculas. Consulte as regras de [nomenclatura de buckets](#)

Região da AWS
 Leste dos EUA (Norte da Virgínia) us-east-1

Copiar configurações do bucket existente - *opcional*
 Somente as configurações de bucket na configuração a seguir são copiadas.

Propriedade de objeto [Informações](#)

Controle a propriedade de objetos gravados nesse bucket a partir de outras contas da AWS e o uso de listas de controle de acesso (ACLs). A propriedade do objeto determina quem pode especificar o acesso aos objetos.

☒ **ACLs desabilitadas (recomendado)**
 Todos os objetos nesse bucket são de propriedade dessa conta. O acesso a esse bucket e seus objetos é especificado usando apenas políticas.

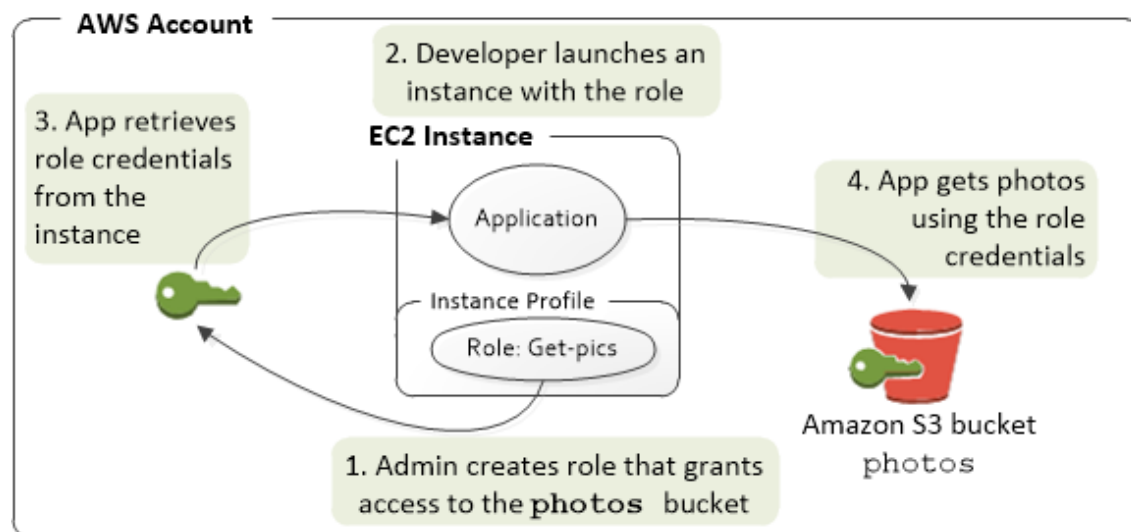
☐ **ACLs habilitadas**
 Os objetos nesse bucket podem ser de propriedade de outras contas da AWS. O acesso a esse bucket e seus objetos pode ser especificado usando ACLs.

Propriedade do objeto
 Imposto pelo proprietário do bucket

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**

aws

Serviços

Pesquisar por serviços, recursos, blogs, documentos e muito mais

[Alt+S]

CloudTrail

Introducing CloudTrail Lake

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

Painel

Histórico de eventos

Insights

Lake

Trilhas

Definição de preços

Documentação

Fóruns

Perguntas frequentes

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

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

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