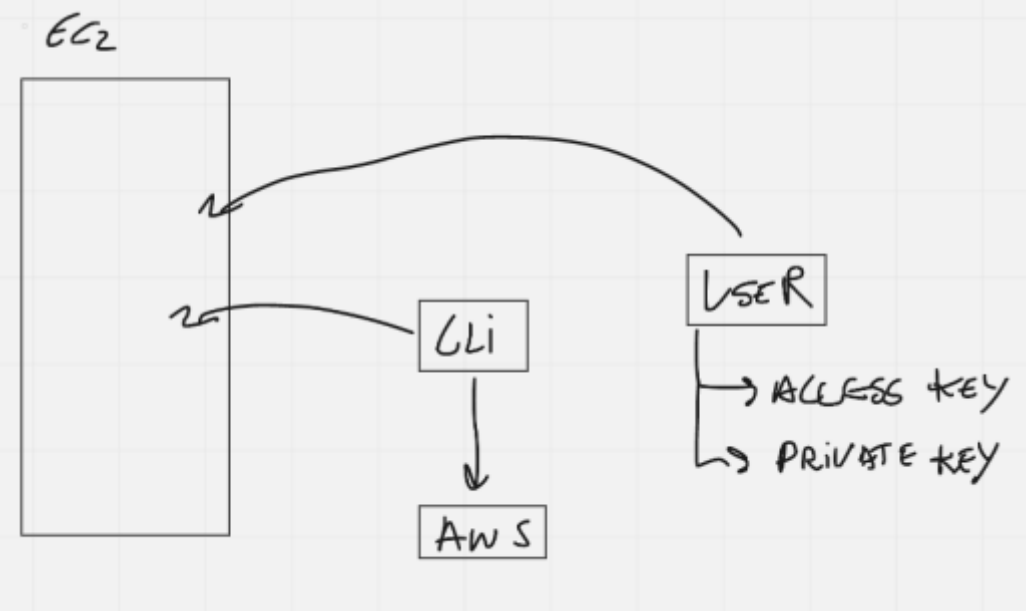
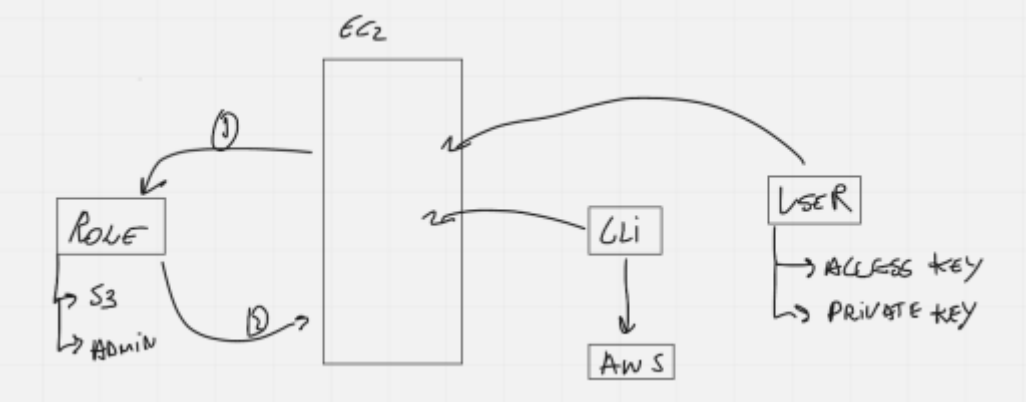
15 - APLICANDO ROLES EM UM SERVIDOR EC2

- Atualmente o que fazemos é o seguinte.

- Temos nossa instancia EC2 e atraves da CLI acessamos essa estrutura da aws.
- So que atraves da EC2 para que tenhamos acesso a AWS precisamos de um usuario com uma access key e uma private key.
- So que o grande problema em se utilizar isso, é que os dados ficam armazenados e se allguem hackear essa instancia EC2, com dois ou tres comandos eles conseguem visualizar em clear text (texto limpo) a sua access key e sua private key.
- É ai que entram as ROLES



- Voce cria uma role e fala que essa role possui acesso S3 e admin.
- Voce pega essa role e aplica na EC2, que irá verificar a role pra depois te dar permissão, com uma grande diferença, ela não armazena essa role localmente.



LABORATORIO

- Verificando se temos acesso

```
aws s3 ls
```

- Como sabemos que temos acesso, vamos voltar ao diretorio principal

```
cd
```

- e ver se possui algum arquivo

```
ls
```

- vemos que não tem nenhum arquivo, so que o formato que a amazon utilliza para armazenar esse usuario e senha é a do diretorio oculto

.aws

- para entrar nesse diretorio

```
cd .aws
```

- Dentro dele digitamos ls para ver o que tem. Existem dois arquivos, config e credentials, se usarmos o editor nano para abrir esses arquivos. Irá aparecer nossa Access Key e nossa Private eKey.

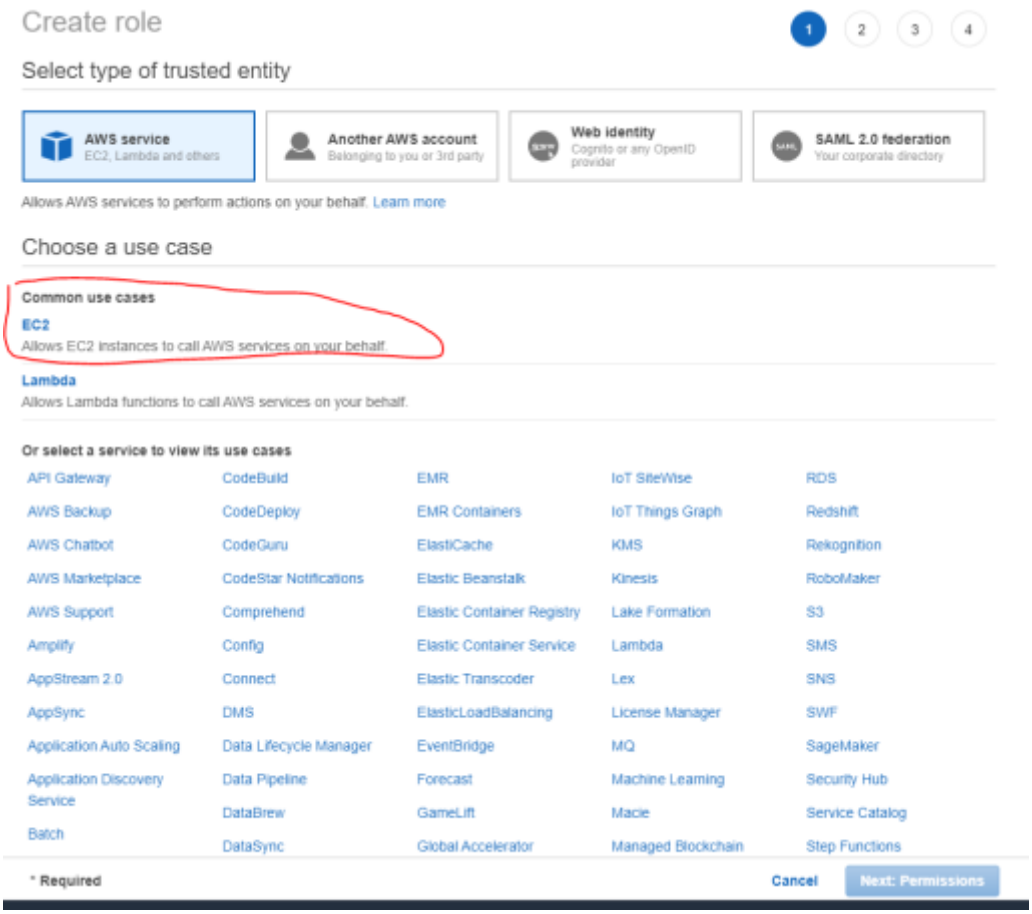
- Moral da historia, se o seu servidor for atacado e a pessoa tiver conhecimento que esta dentro do servidor da aws ele irá pegar suas keys e fazer o que quiser.

- A melhor pratica eh fazer ROLES

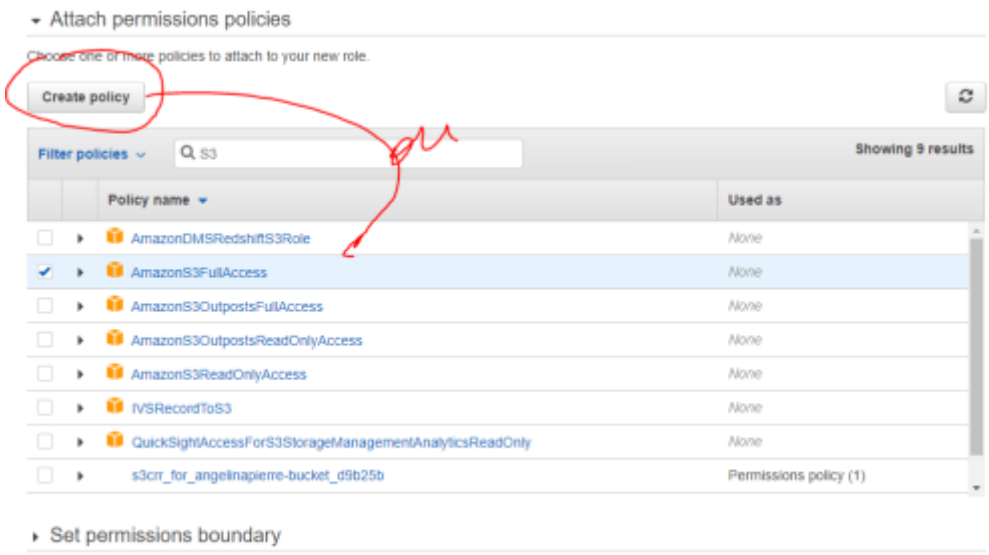
ROLES

1 - CRIAR A ROLE

AWS CONSOLE> IAM>ROLES

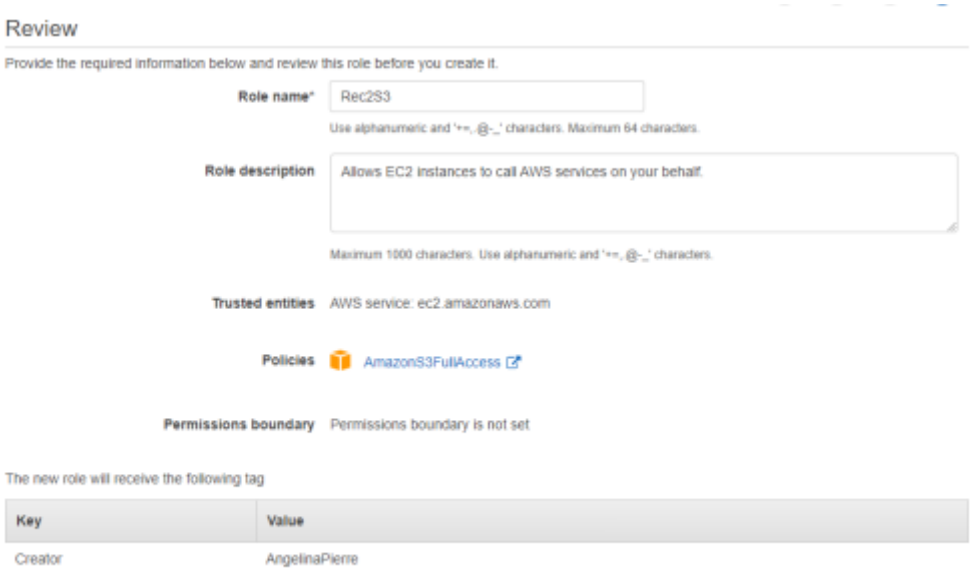


2 - CRIANDO POLITICA



3 - TAGS (SEMPRE COLOCAR)

4 - NOME DA ROLE



5 - Agora que a regra esta criada temos que conecta-la a maquina EC2

- Attach/replace IAM role

5.1 - Antes de fazermos isso, perceba que nossa maquinanão possui nenhuma ROLE mas temos acesso.

- Conseguimos visualizar as buckets, temos que retirar esse acesso, para isso temos que remover a pasta oculta da AWS.

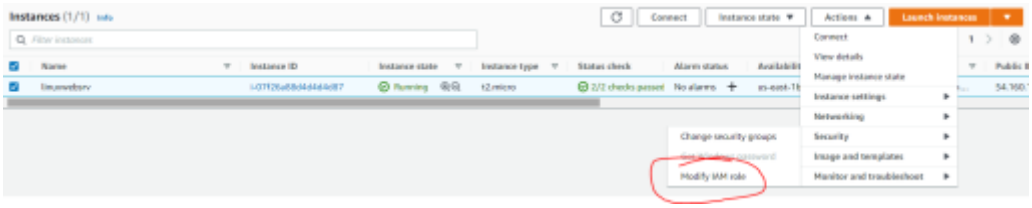
```
[root@ip-172-31-22-0 ec2-user]# aws s3 ls
2021-05-11 15:24:36 angelinapierre-bkp
2021-05-10 17:07:12 angelinapierre-bucket
2021-05-12 13:21:00 angelinapierre-mp4
2021-05-14 13:52:25 angelinapierre-site
2021-05-17 17:52:55 angelinapierrel
[root@ip-172-31-22-0 ec2-user]# cd
[root@ip-172-31-22-0 ~]# cd .aws
[root@ip-172-31-22-0 .aws]# ls
config  credentials
[root@ip-172-31-22-0 .aws]# nano credentials
[root@ip-172-31-22-0 .aws]# cd
[root@ip-172-31-22-0 ~]# rm -rf .aws
[root@ip-172-31-22-0 ~]# ls
[root@ip-172-31-22-0 ~]# cd .aws
bash: cd: .aws: No such file or directory
[root@ip-172-31-22-0 ~]#
```

- Removemos a credencial de dentro da instancia EC2, agora não devemos ter mais acessov ia CLI.
- Para verificar isso vamos tentar listar as pastas.

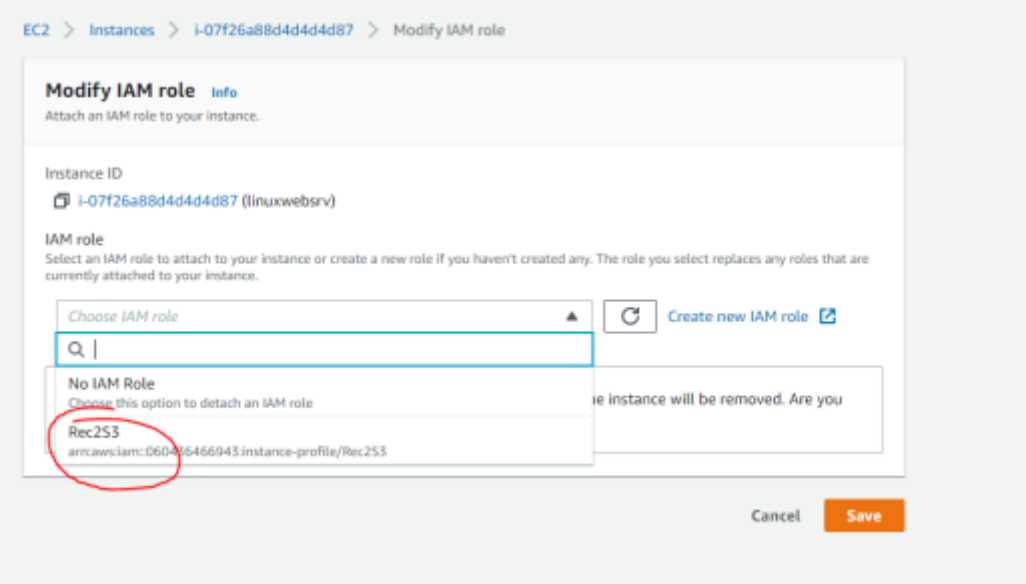
```
[root@ip-172-31-22-0 ~]#
[root@ip-172-31-22-0 ~]# aws s3 ls
Unable to locate credentials. You can configure credentials by running "aws conf
igure".
```

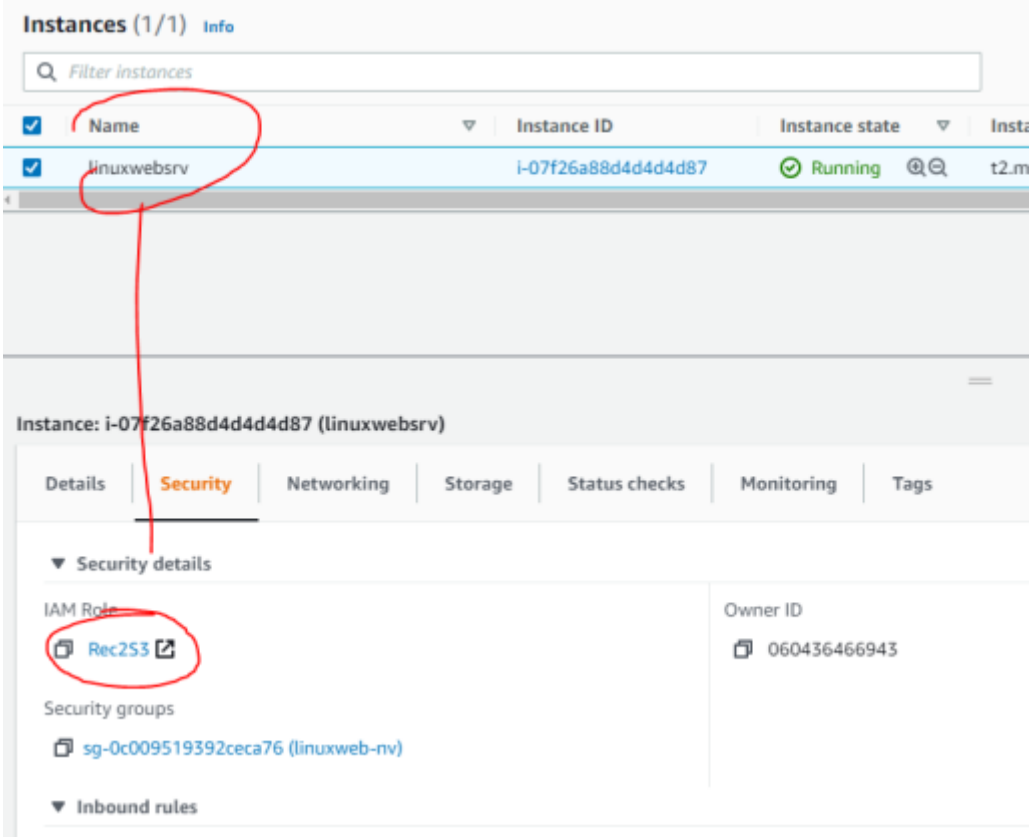
- Podemos reconfigurar utilizando o aws config, ou podemos aplicar a ROLE.

6 - AWS console

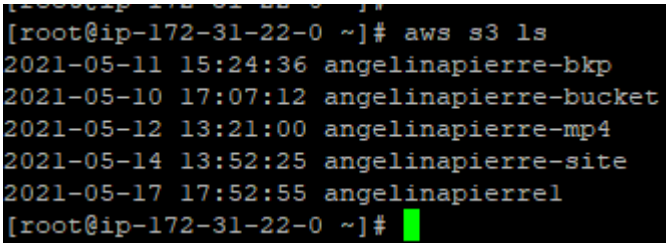


7 - seleciona o ROle que criamos





8 - Voltando a CLI para verificar se o acesso foi liberado.,



9- Veja que a pasta de credenciais nao existe mais.