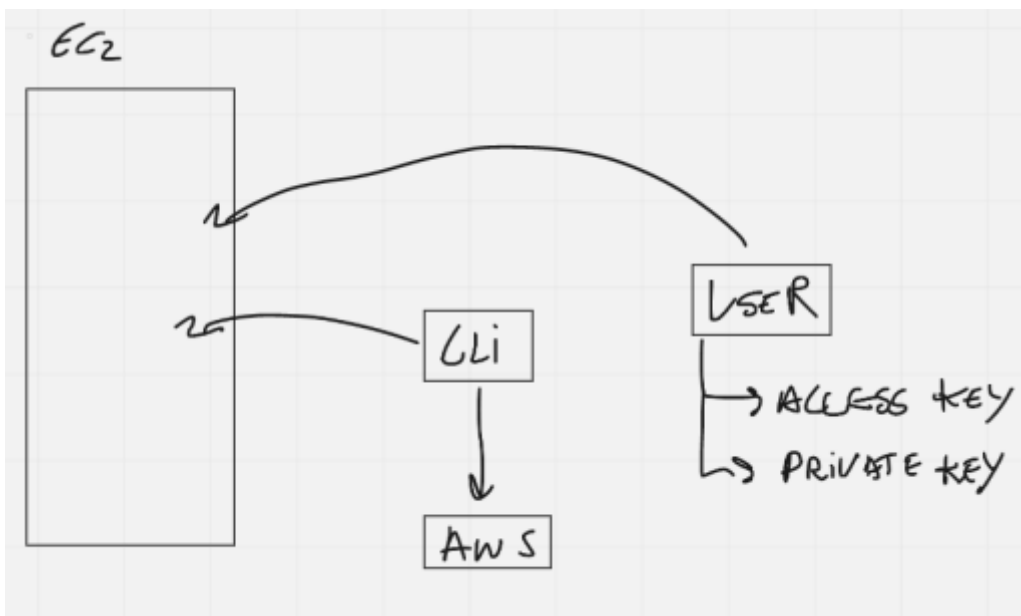
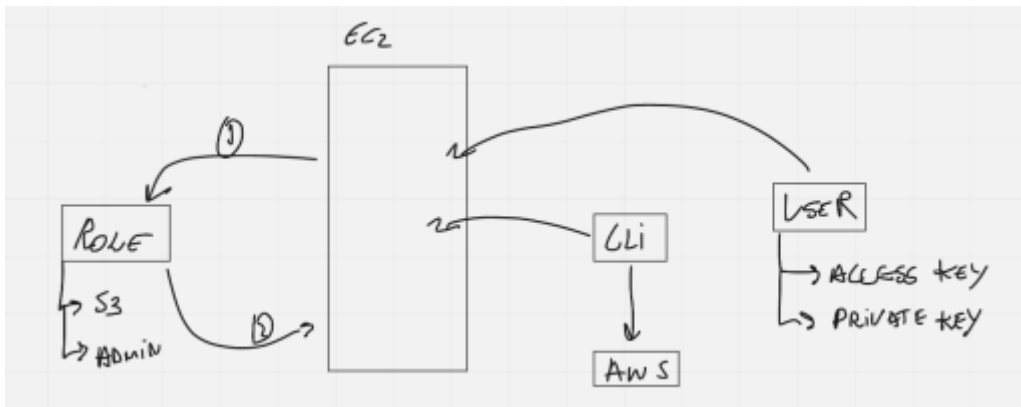


15 - APLICANDO ROLES EM UM SERVIDOR EC2

- 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 diretório principal

```
cd
```

- e ver se possui algum arquivo

```
ls
```

- vemos que não tem nenhum arquivo, só que o formato que a Amazon utiliza para armazenar esse usuário e senha é a do diretório oculto

```
.aws
```

- para entrar nesse diretório

```
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

Create role 1 2 3 4

Select type of trusted entity

AWS service
EC2, Lambda and others

Another AWS account
Belonging to you or 3rd party

Web identity
Cognito or any OpenID provider

SAML 2.0 federation
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose a use case

Common use cases

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

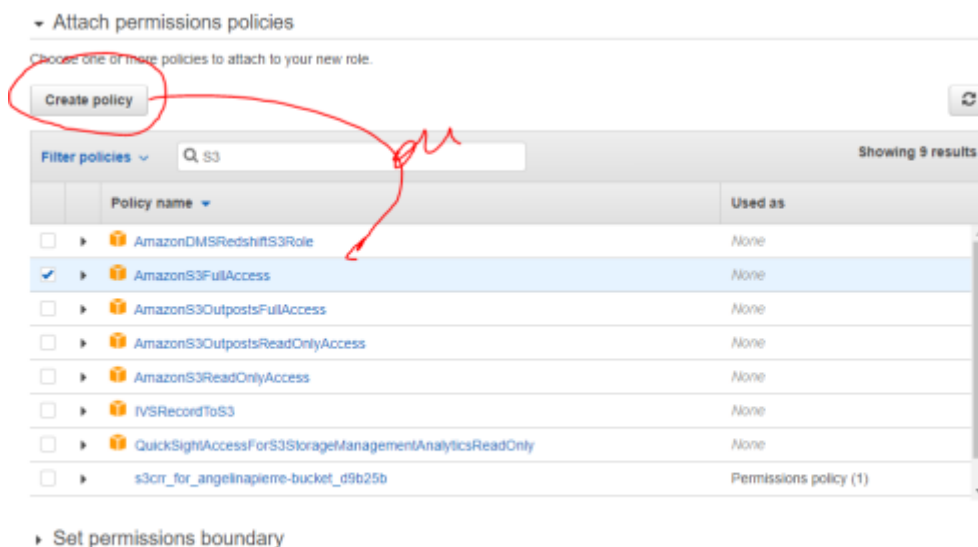
Or select a service to view its use cases

API Gateway	CodeBuild	EMR	IoT SiteWise	RDS
AWS Backup	CodeDeploy	EMR Containers	IoT Things Graph	Redshift
AWS Chatbot	CodeGuru	ElastiCache	KMS	Rekognition
AWS Marketplace	CodeStar Notifications	Elastic Beanstalk	Kinesis	RoboMaker
AWS Support	Comprehend	Elastic Container Registry	Lake Formation	S3
Amplify	Config	Elastic Container Service	Lambda	SMS
AppStream 2.0	Connect	Elastic Transcoder	Lex	SNS
AppSync	DMS	ElasticLoadBalancing	License Manager	SWF
Application Auto Scaling	Data Lifecycle Manager	EventBridge	MQ	SageMaker
Application Discovery Service	Data Pipeline	Forecast	Machine Learning	Security Hub
Batch	DataBrew	GameLift	Macie	Service Catalog
	DataSync	Global Accelerator	Managed Blockchain	Step Functions

* Required

Cancel **Next: Permissions**

2 - CRIANDO POLITICA



3 - TAGS (SEMPRE COLOCAR)

4 - NOME DA ROLE

Review

Provide the required information below and review this role before you create it.

Role name* Rec2S3
Use alphanumeric and '+', '@', '-' characters. Maximum 64 characters.

Role description Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and '+', '@', '-' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies AmazonS3FullAccess

Permissions boundary Permissions boundary is not set

The new role will receive the following tag

Key	Value
Creator	AngelinaPiere

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 maquina não 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 acesso via CLI.
- Para verificar isso vamos tentar listar as pastas.

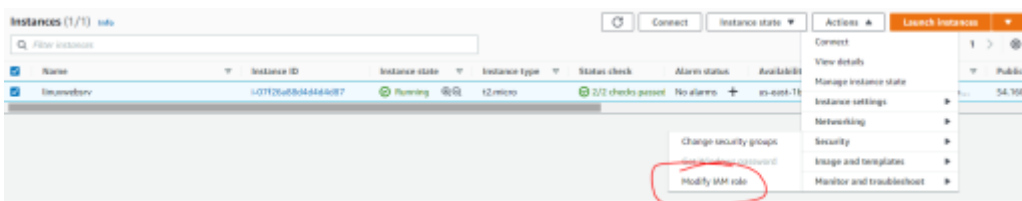
```

[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 configure".

```

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

6 - AWS console



7 - seleciona o ROle que criamos

EC2 > Instances > i-07f26a88d4d4d4d87 > Modify IAM role

Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID
i-07f26a88d4d4d4d87 (linuxwebsrv)

IAM role
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

Choose IAM role

No IAM Role
Choose this option to detach an IAM role

Rec253
arn:aws:iam:060436466943:instance-profile/Rec253

Create new IAM role

Warning: The instance will be removed. Are you sure?

Cancel **Save**

Instances (1/1) [Info](#)

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type
<input checked="" type="checkbox"/>	linuxwebsrv	i-07f26a88d4d4d4d87	Running	t2.m

Instance: i-07f26a88d4d4d4d87 (linuxwebsrv)

Details

Security

Networking

Storage

Status checks

Monitoring

Tags

▼ Security details

IAM Role

Rec253

Security groups

sg-0c009519392ceca76 (linuxweb-nv)

▼ Inbound rules

Owner ID

060436466943

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

```
[root@ip-172-31-22-0 ~]#  
[root@ip-172-31-22-0 ~]# 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 ~]#
```

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