

AWS CLI

Instala y configura la AWS CLI en tu máquina local para el acceso a tu Learner Lab Con la AWS CLI realiza lo siguiente:

1. Crea un grupo de seguridad para acceder a Bases de Datos MySQL

```
aws ec2 create-security-group --group-name mysql-security-group --description "Grupo de seguridad para acceso a mysql"
```

-acceso al puerto 3306:

```
aws ec2 authorize-security-group-ingress --group-name mysql-security-group --protocol tcp --port 3306 --cidr 0.0.0.0/0
```

2. Crea un grupo de seguridad para acceso SSH, HTTP, HTTPS

```
aws ec2 create-security-group --group-name ssh-http-https-security-group --description "Grupo de seguridad para acceso a ssh, http, https"
```

-acceso SSH:

```
aws ec2 authorize-security-group-ingress --group-name ssh-http-https-security-group --protocol tcp --port 22 --cidr 0.0.0.0/0
```

-acceso HTTP:

```
aws ec2 authorize-security-group-ingress --group-name ssh-http-https-security-group --protocol tcp --port 80 --cidr 0.0.0.0/0
```

-acceso HTTPS:

```
aws ec2 authorize-security-group-ingress --group-name ssh-http-https-security-group --protocol tcp --port 443 --cidr 0.0.0.0/0
```

3. Lista la información de este último grupo de seguridad en formato de tabla.

```
aws ec2 describe-security-groups --group-names ssh-http-https-security-group
```

4. Crea un par de claves para acceder por SSH

```
aws ec2 create-key-pair --key-name ClaveEjercicio --query 'KeyMaterial' --output text > ClaveEjercicio.pem
```

5. Crea una IP Elástica

```
aws ec2 allocate-address --query 'PublicIp' --output text
```

6. Crea una instancia EC2 sencilla:

- a. RAM: 2 GB
- b. AMI: Un Ubuntu Server 22.04
- c. Utiliza el par de claves creado en el paso 4
- d. Asígnale el último grupo de seguridad que has creado
- e. Asigna la ip elástica a la instancia EC2

```
aws ec2 run-instances --image-id ami-005fc0f236362e99f --count 1 --instance-type t3.small --key-name ClaveEjercicio --security-groups ssh-http-https-security-group
```

-Ver id instancia:

```
aws ec2 describe-instances --query 'Reservations[*].Instances[*].InstanceId' --output text
```

-Ver id ip elástica:

```
aws ec2 describe-addresses --query 'Addresses[0].AllocationId' --output text
```

```
aws ec2 associate-address --instance-id i-03d273a8c984d18d4 --allocation-id eipalloc-07d6d42a00389e2d4
```

7. Lista la ip pública y privada de la última instancia que acabas de crear en tu laboratorio.

```
aws ec2 describe-instances --instance-ids i-03d273a8c984d18d4 --query 'Reservations[*].Instances[*].{PublicIP:PublicIpAddress,PrivateIP:PrivateIpAddress}'
```

8. Termina la instancia EC2

```
aws ec2 terminate-instances --instance-ids i-03d273a8c984d18d4
```

9. Elimina los grupos de seguridad

-Listar grupos de seguridad:

```
aws ec2 describe-security-groups --query 'SecurityGroups[*].{GroupId:GroupId,GroupName:GroupName}'
```

```
aws ec2 delete-security-group --group-id sg-0558a087e97df028b  
aws ec2 delete-security-group --group-id sg-0ddf331d9432871f3
```

10. Lista todos los buckets de tu laboratorio

```
aws s3 ls
```