LABORATORIO 181
SOLUCIÓN DE PROBLEMAS DE UNA VPC

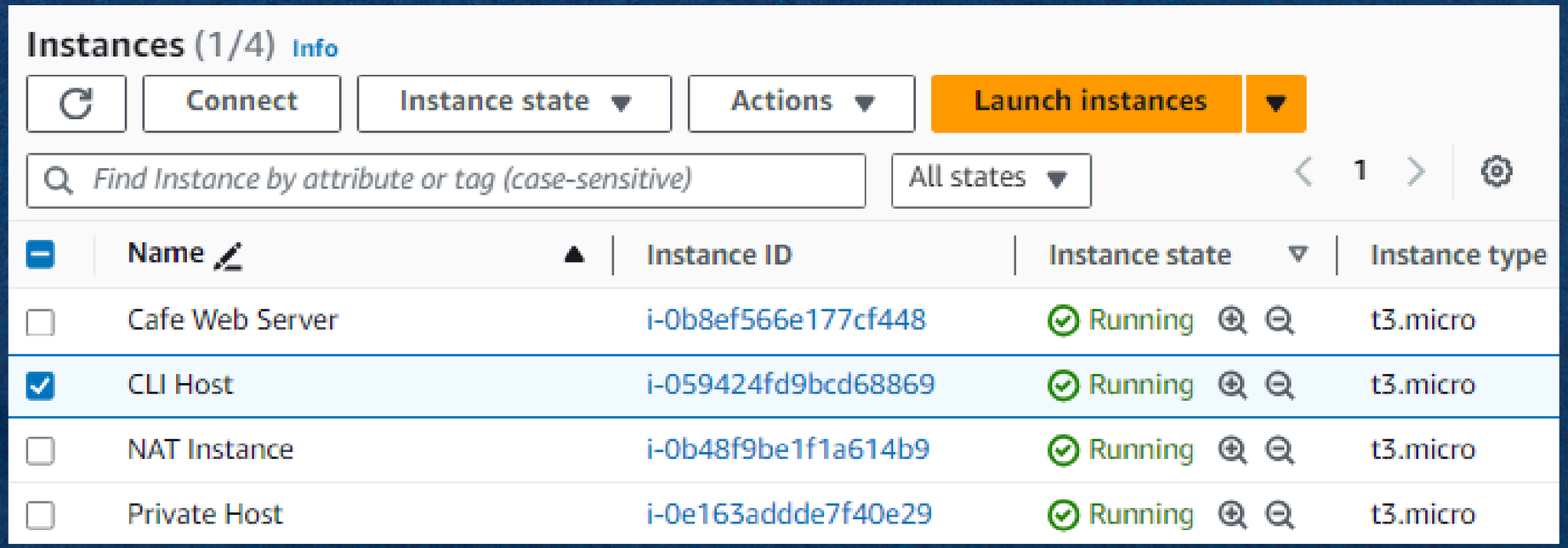
Hecho con sobredosis de amor por:
Sony Etcheverry, Gonzalo Rondeau, Agustín Esteche,
Sebastián Aguilera, Fidel Fernández, Ignacio Suárez, Elisa Gamarra.

OBJETIVOS

- Cree registros de flujo de VPC.
- Solucionar problemas de configuración de VPC.
- Analizar registros de flujo.

TAREA 1: CONECTARSE A LA INSTANCIA CLI HOST

- Nos conectaremos a la CLI Host mediante la opción directa desde la página de instancias de Amazon.



TAREA 1.1: CONFIGURAR LA AWS CLI EN LA INSTANCIA CLI HOST

- Configuraremos la CLI de Amazon en la instancia EC2.

```
[ec2-user@cli-host ~]$ aws configure
AWS Access Key ID [None]: AKIAX22UO3TBEXJ5X4NW
AWS Secret Access Key [None]:   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
Default region name [None]: us-west-2
Default output format [None]: json
[ec2-user@cli-host ~]$
```

TAREA 2: CREAR REGISTROS DE FLUJO DE VPC

```
[ec2-user@cli-host ~]$ aws s3api create-bucket --bucket flowlog890423 --region 'us-west-2' --create-bucket-confi
tion LocationConstraint='us-west-2'
{
    "Location": "http://flowlog890423.s3.amazonaws.com/"
}
```

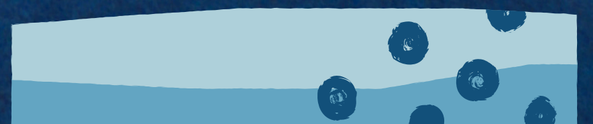
- Creamos un bucket.

```
[ec2-user@cli-host ~]$ aws ec2 describe-vpcs --query  'Vpcs[*].[VpcId,Tags[?Key== Name ].Value,CidrBlock]'  --fi
s  "Name=tag:Name,Values='VPC1'"
[
    [
        "vpc-06c60965dcaeb993c",
        [
            "VPC1"
        ],
        "10.0.0.0/16"
    ]
]
```

- Obtenemos el ID de VPC de la VPC1.

- Este comando creará los registros de flujos de la VPC1 dentro del bucket creado.

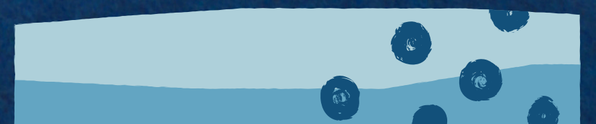
```
ec2-user@cli-host aws ec2 create-flow-logs --resource-type VPC --resource-ids vpc-06c60965dcaeb993c --traffic-t
pe ALL --log-destination-type s3 --log-destination arn:aws:s3:::890423

    "Unsuccessful": [
        {
            "ResourceId": "vpc-06c60965dcaeb993c",
            "Error": {
                "Message": "LogDestination: 890423 does not exist",
                "Code": "400"
            }
        }
    ],
    "FlowLogIds": [],
    "ClientToken": "SdRt5hDdIQcLlAO1PJUkXHZP6/3wVZBYDjTYyQyIorc="
```



TAREA 2: CONFIRMAR REGISTROS DE FLUJO DE VPC

Para confirmar que se creó el registro de flujo, ejecutamos:

```
[ec2-user@cli-host ~]$ aws ec2 describe-flow-logs
{
    "FlowLogs": [
        {
            "LogDestinationType": "s3",
            "Tags": [],
            "ResourceId": "vpc-0e236b6e549397bc3",
            "CreationTime": "2024-07-04T22:42:34.858Z",
            "TrafficType": "ALL",
            "FlowLogStatus": "ACTIVE",
            "LogFormat": "${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr} ${srcport} ${dstport} ${protocol} ${packets} ${bytes} ${
start} ${end} ${action} ${log-status}",
            "FlowLogId": "fl-0092b9247c07029b5",
            "MaxAggregationInterval": 600,
            "LogDestination": "arn:aws:s3:::flowlog435312",
            "DeliverLogsStatus": "SUCCESS"
        }
    ]
}
```



TAREA 3: SOLUCIONAR PROBLEMAS DE CONFIGURACIÓN DE LA VPC PARA PERMITIR EL ACCESO A LOS RECURSOS

```
[ec2-user@cli-host ~]$ aws ec2 describe-instances --filter "Name=ip-address,Values='35.91.217.45'"
r
' 'Reservations[*].Instances[*].[State,PrivateIpAddress,InstanceId,SecurityGroups,SubnetId,KeyName]'
[ec2-user@cli-host ~]$ aws ec2 describe-instances --filter "Name=ip-address,Values='35.91.217.45'" --query
ubnetId,KeyName]'Instances[*].[State,PrivateIpAddress,InstanceId,SecurityGroups,S
[
    [
        [
            {
                "Code": 16,
                "Name": "running"
            },
            "10.0.1.143",
            "i-00b9559c5def1fb27",
            [
                {
                    "GroupName": "c110983a2632494170440025t1w4006711207B2-WebSecurityGroup-OjxxOQJvx4LB",
                    "GroupId": "sg-004d4d6834edcfe7e"
                }
            ],
            "subnet-040ada20c1052036d",
            "vockey"
        ]
    ]
```

- Este comando buscará diversa información de la instancia para usarla más adelante

DESAFÍO NÚMERO 1:

Hemos establecido que la instancia del servidor web se encuentra en ejecución, pero la página web no se carga. ¿Cuál podría ser el problema?

- Utilizaremos el comando *nmap* para comprobar qué puertos están abiertos en la instancia EC2 del servidor web.

  - Primero instalaremos la utilidad.

```
ec2-user@cli-host ~]$ sudo yum install -y nmap
oaded plugins: extras_suggestions, langpacks, priorities, update-motd
mzn2-core
esolving Dependencies
-> Running transaction check
--> Package nmap.x86_64 2:6.40-19.amzn2.0.1 will be installed
-> Processing Dependency: nmap-ncat = 2:6.40-19.amzn2.0.1 for package: 2:nmap-6.40-19.amzn2.0.1.x86_64
-> Running transaction check
--> Package nmap-ncat.x86_64 2:6.40-19.amzn2.0.1 will be installed
-> Finished Dependency Resolution

ependencies Resolved
```

- Luego ejecutamos el comando nmap. Este comando tendremos que ejecutarlo en conjunto con nuestra dirección IP pública.

```
[ec2-user@cli-host ~]$ nmap 52.24.73.80

Starting Nmap 6.40 ( http://nmap.org ) at 2024-07-04 22:35 UTC
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.03 seconds
```

- Después verificaremos los detalles del grupo de seguridad utilizando el comando “aws ec2 describe-security-groups”.

```
[ec2-user@cli-host ~]$ aws ec2 describe-security-groups
{
    "SecurityGroups": [
        {
            "IpPermissionsEgress": [
                {
```

¿La configuración del grupo de seguridad que se aplicó a la instancia de EC2 del servidor web parece permitir la conectividad al puerto 22?

- *Se crea una nueva ruta indicando el ID de la Tabla de Ruta y el ID del Gateway.*

```
[ec2-user@cli-host ~]$ aws ec2 create-route --route-table-id rtb-066513396fa91617f --gateway-id  igw-0ce74d
ef669fa348e --destination-cidr-block '0.0.0.0/0'
{
    "Return": true
}
```

- *Vemos que el problema fue resuelto, podemos conectarnos a la aplicación web mediante la IP.*

DESAFÍO NÚMERO 2:

Intente conectarse a la instancia mediante EC2 Instance Connect.
Este intento también falla. Aparece en el navegador un error similar al mensaje que recibió anteriormente.

¿Cuál podría ser el problema restante?

Ya verificó que el servidor web se encuentra en ejecución. Creó correctamente una entrada en la tabla de enrutamiento para conectar la subred en la que se ejecuta la instancia del servidor web a internet. También verificó que el grupo de seguridad permite conexiones en el puerto 22, que es el puerto SSH predeterminado.

- *En el terminal de la instancia del host CLI, verifique la configuración de la lista de control de acceso a la red (ACL de red) para la ACL de red asociada con la subred donde se ejecuta la instancia.*

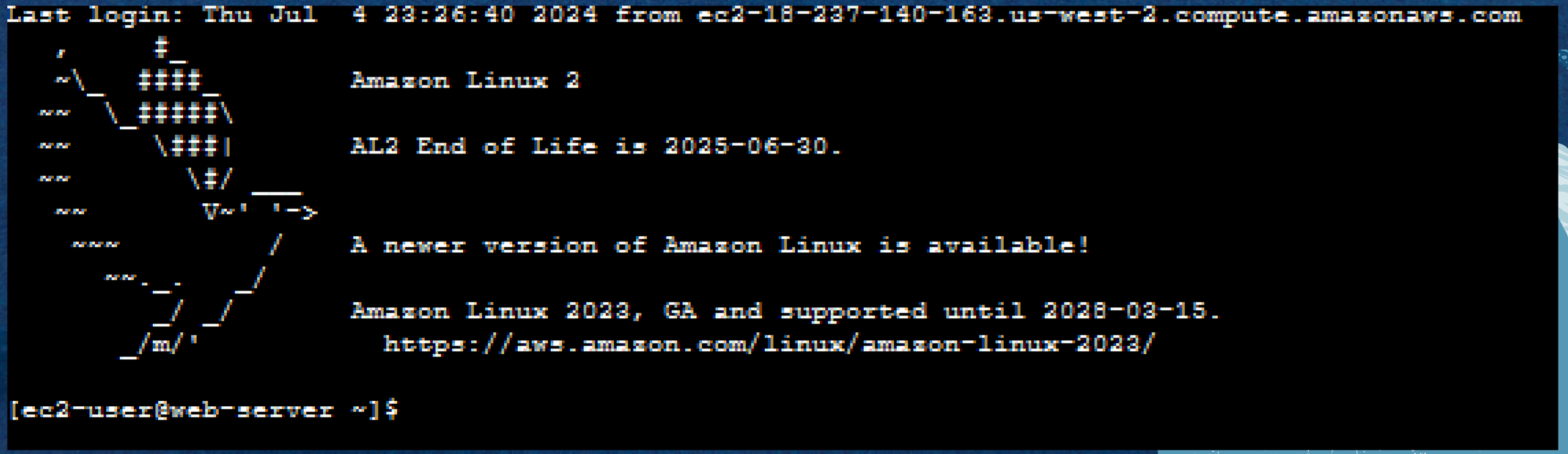
- *Analizamos el resultado de ejecutar el comando. ¿Parece que alguna de las entradas podría estar causando el problema?*

```
ada20c1052036d" --query 'NetworkAcls[*].[NetworkAclId,Entries]'
[
    [
        "acl-0b19f75f3388cf018",
        [
            {
                "RuleNumber": 100,
                "Protocol": "-1",
                "Egress": true,
                "CidrBlock": "0.0.0.0/0",
                "RuleAction": "allow"
            },
            {
                "RuleNumber": 32767,
                "Protocol": "-1",
                "Egress": true,
                "CidrBlock": "0.0.0.0/0",
                "RuleAction": "deny"
            },
            {
                "RuleNumber": 40,
                "Protocol": "6",
                "PortRange": {
                    "To": 22,
                    "From": 22
                },
                "Egress": false,
                "RuleAction": "deny",
                "CidrBlock": "0.0.0.0/0"
```

- *Usamos el comando “delete-acls” para eliminar la regla numero 40, esta no nos dejaba acceder a la instancia mediante instance connect por el bloqueo del puerto 22.*

```
[ec2-user@cli-host ~]$ aws ec2 delete-network-acl-entry --network-acl-id acl-0b19f75f3388cf018 --ingress --rule-number 40
[ec2-user@cli-host ~]$
[ec2-user@cli-host ~]$ aws ec2 describe-network-acls --filter "Name=association.subnet-id,Values=subnet-0
ada20c1052036d" --query 'NetworkAcls[*].[NetworkAclId,Entries]'
[
    [
        "acl-0b19f75f3388cf018",
        [
            {
                "RuleNumber": 100,
                "Protocol": "-1",
                "Egress": true,
                "CidrBlock": "0.0.0.0/0",
                "RuleAction": "allow"
            },
            {
                "RuleNumber": 32767,
                "Protocol": "-1",
                "Egress": true,
                "CidrBlock": "0.0.0.0/0",
                "RuleAction": "deny"
            },
            {
                "RuleNumber": 100,
                "Protocol": "-1",
                "Egress": false,
                "CidrBlock": "0.0.0.0/0",
                "RuleAction": "allow"
            },
            {
                "RuleNumber": 32767,
                "Protocol": "-1",
                "Egress": false,
                "CidrBlock": "0.0.0.0/0",
                "RuleAction": "deny"
```

- *Ahora mediante EC2 instance connect podemos conectarnos de manera satisfactoria a nuestra instancia*



TAREA 4.1: DESCARGAR Y EXTRAER REGISTROS DE FLUJO

- *Ejecutamos el comando **mkdir flowlogs** para para crear un directorio local donde pueda descargar los archivos de registro de flujo y **cd flowlogs** para movernos al mismo.*

- *Para obtener una lista de los buckets de S3 y recordar el nombre del bucket, usamos **aws s3 ls***

```
[ec2-user@cli-host ~]$ mkdir flowlogs
[ec2-user@cli-host ~]$ ls
flowlogs
[ec2-user@cli-host ~]$ cd flowlogs
[ec2-user@cli-host flowlogs]$ aws s3 ls
2024-07-04 22:42:36 flowlog435312
[ec2-user@cli-host flowlogs]$ aws s3 cp s3://<flowlog435312>/ . --recursive
-bash: flowlog435312: No such file or directory
[ec2-user@cli-host flowlogs]$ aws s3 cp s3://flowlog435312/ . --recursive
download: s3://flowlog435312/AWSLogs/400671120782/vpcflowlogs/us-west-2/2024/07/04/40
07/04/400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2240Z_fb49bb9a
```

- *Ejecutamos el comando que le sigue (reemplazando <flowlog....> por el nombre de tu bucket, creado previamente al laboratorio) para descargar los registros de bucket.*

- *Ejecutamos un cd para ubicarnos en la carpeta de flowlogs elegida*
- *Luego procedemos a listarlos*

```
[ec2-user@cli-host flowlogs]$ cd AWSLogs/400671120782/vpcflowlogs/us-west-2/2024/07/04/
[ec2-user@cli-host 04]$ ls
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2240Z_dfb2d082.log.gz
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2240Z_fb49bb9a.log.gz
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2245Z_2f6b244b.log.gz
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2245Z_754b1424.log.gz
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2250Z_63637df2.log.gz
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2255Z_7d2f8190.log.gz
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2255Z_9e7166fb.log.gz
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2255Z_a2439b33.log.gz
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2300Z_cd1ecf9e.log.gz
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2305Z_324c672d.log.gz
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2305Z_84961fca.log.gz
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2310Z_dcf88c53.log.gz
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2310Z_ec742ae2.log.gz
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2315Z_795688d3.log.gz
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2320Z_6742da14.log.gz
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2320Z_723adee5.log.gz
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2325Z_14607aa4.log.gz
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2325Z_d9aab47b.log.gz
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log.gz
[ec2-user@cli-host 04]$
```

- *Ejecutamos el comando gunzip para extraer los registros.*

- *Tras eso, utilizamos el comando ls para verificar que todos los archivos se extrajeron correctamente.*

```
[ec2-user@cli-host 04]$ gunzip *.gz
[ec2-user@cli-host 04]$ ls
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2240Z_dfb2d082.log
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2240Z_fb49bb9a.log
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2245Z_2f6b244b.log
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2245Z_754b1424.log
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2250Z_63637df2.log
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2255Z_7d2f8190.log
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2255Z_9e7166fb.log
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2255Z_a2439b33.log
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2300Z_cd1ecf9e.log
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2305Z_324c672d.log
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2305Z_84961fca.log
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2310Z_dcf88c53.log
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2310Z_ec742ae2.log
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2315Z_795688d3.log
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2320Z_6742da14.log
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2320Z_723adee5.log
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2325Z_14607aa4.log
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2325Z_d9aab47b.log
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log
[ec2-user@cli-host 04]$
```

TAREA 4.2: ANALIZAR LOS REGISTROS

- *La fila del encabezado indica el tipo de datos que contiene cada entrada del registro. Cada entrada contiene información, como la dirección IP del origen del evento (en la cuarta columna), el puerto de destino (séptima columna), las marcas temporales de inicio y fin (en formato de marca temporal Unix) y la acción resultante (ACCEPT [Aceptar]) o REJECT [Rechazar]).*

```
[ec2-user@cli-host 04]$ head 400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2240Z_dfb2d082.log
version account-id interface-id srcaddr dstaddr srcport dstport protocol packets bytes start end action log-status
2 400671120782 eni-0b0f77765f97c62aa 80.75.212.75 10.0.1.251 51299 58500 6 1 40 1720132986 1720133008 REJECT OK
2 400671120782 eni-0b0f77765f97c62aa 188.166.237.80 10.0.1.251 52077 5039 6 1 40 1720132986 1720133008 REJECT OK
2 400671120782 eni-0b0f77765f97c62aa 162.216.149.238 10.0.1.251 54230 63239 6 1 44 1720132986 1720133008 REJECT OK
2 400671120782 eni-0b0f77765f97c62aa 35.203.210.54 10.0.1.251 52298 14894 6 1 44 1720132986 1720133008 REJECT OK
2 400671120782 eni-0b0f77765f97c62aa 208.100.26.241 10.0.1.251 43318 873 6 1 40 1720132986 1720133008 REJECT OK
2 400671120782 eni-0b0f77765f97c62aa 147.185.132.41 10.0.1.251 55062 8400 6 1 44 1720132986 1720133008 REJECT OK
2 400671120782 eni-0b0f77765f97c62aa 206.168.34.152 10.0.1.251 49783 43342 6 1 60 1720132986 1720133008 REJECT OK
2 400671120782 eni-069cdb38de46ac440 143.42.1.213 10.0.1.143 59584 9303 6 1 44 1720132967 1720132988 REJECT OK
2 400671120782 eni-069cdb38de46ac440 185.242.226.39 10.0.1.143 47664 1054 6 1 40 1720132967 1720132988 REJECT OK
[ec2-user@cli-host 04]$
```

- *Vemos todas las solicitudes que han sido rechazadas*

```
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log:137:2 400671120782 eni-0b0f77765f97c62aa 147.185.132.196 10.0.1.251 52507 8073 6 1 44 1720135988 1720136006 REJECT O
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log:138:2 400671120782 eni-0b0f77765f97c62aa 162.216.150.7 10.0.1.251 57121 9277 6 1 44 1720135988 1720136006 REJECT OK
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log:139:2 400671120782 eni-0b0f77765f97c62aa 184.185.19.119 10.0.1.251 62577 23 6 1 40 1720135988 1720136006 REJECT OK
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log:140:2 400671120782 eni-0b0f77765f97c62aa 8.222.189.128 10.0.1.251 50855 7780 6 1 52 1720135988 1720136006 REJECT OK
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log:147:2 400671120782 eni-069cdb38de46ac440 4.156.20.204 10.0.1.143 40938 8087 6 1 40 1720135989 1720136015 REJECT OK
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log:148:2 400671120782 eni-069cdb38de46ac440 206.168.35.85 10.0.1.143 47490 831 6 1 60 1720135989 1720136015 REJECT OK
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log:151:2 400671120782 eni-069cdb38de46ac440 134.122.65.114 10.0.1.143 60382 6006 6 1 40 1720135989 1720136015 REJECT OK
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log:152:2 400671120782 eni-069cdb38de46ac440 162.216.150.198 10.0.1.143 53762 12084 6 1 44 1720135989 1720136015 REJECT
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log:153:2 400671120782 eni-069cdb38de46ac440 162.216.149.228 10.0.1.143 51320 9288 6 1 44 1720135989 1720136015 REJECT O
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log:154:2 400671120782 eni-069cdb38de46ac440 147.185.133.224 10.0.1.143 53285 9643 6 1 44 1720135989 1720136015 REJECT O
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log:158:2 400671120782 eni-069cdb38de46ac440 198.235.24.96 10.0.1.143 52155 4332 6 1 44 1720135989 1720136015 REJECT OK
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log:160:2 400671120782 eni-069cdb38de46ac440 162.216.150.170 10.0.1.143 54995 2324 6 1 44 1720135989 1720136015 REJECT O
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log:162:2 400671120782 eni-069cdb38de46ac440 147.185.133.137 10.0.1.143 53739 9438 6 1 44 1720136019 1720136044 REJECT O
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log:164:2 400671120782 eni-069cdb38de46ac440 18.118.5.163 10.0.1.143 49513 5061 6 1 40 1720136019 1720136044 REJECT OK
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log:165:2 400671120782 eni-069cdb38de46ac440 167.94.138.101 10.0.1.143 47641 23029 6 1 60 1720136019 1720136044 REJECT O
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log:167:2 400671120782 eni-069cdb38de46ac440 35.203.210.53 10.0.1.143 52306 9847 6 1 44 1720136019 1720136044 REJECT OK
400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2330Z_c51bba4b.log:173:2 400671120782 eni-069cdb38de46ac440 147.185.133.48 10.0.1.143 53587 450 6 1 44 1720136019 1720136044 REJECT OK
```

- *Con este comando podemos ver que son 1326 solicitudes rechazadas en total*

```
[ec2-user@cli-host 04]$ grep -rn REJECT . | wc -l
1326
[ec2-user@cli-host 04]$
```

- *Acá agarramos todas las solicitudes rechazadas pero que sean también del puerto 22*

```
[ec2-user@cli-host 04]$ grep -rn 22 . | grep REJECT
./400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2245Z_2f6b244b.log:2:2 400671120782 eni-
069cdb38de46ac440 147.185.132.101 10.0.1.143 56225 50258 6 1 44 1720133083 1720133108 REJECT OK
./400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2245Z_2f6b244b.log:7:2 400671120782 eni-
069cdb38de46ac440 35.203.210.220 10.0.1.143 53645 2888 6 1 44 1720133083 1720133108 REJECT OK
./400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2245Z_2f6b244b.log:14:2 400671120782 eni
-0b0f77765f97c62aa 147.185.132.240 10.0.1.251 51778 22 6 1 44 1720133101 1720133130 REJECT OK
./400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2245Z_2f6b244b.log:25:2 400671120782 eni
-0b0f77765f97c62aa 79.110.62.75 10.0.1.251 52699 2213 6 1 40 1720133135 1720133156 REJECT OK
./400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2245Z_2f6b244b.log:27:2 400671120782 eni
-069cdb38de46ac440 152.32.226.8 10.0.1.143 43247 8480 6 1 60 1720133127 1720133136 REJECT OK
./400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2245Z_2f6b244b.log:29:2 400671120782 eni
-069cdb38de46ac440 35.203.210.7 10.0.1.143 49722 48632 6 1 44 1720133127 1720133136 REJECT OK
./400671120782_vpcflowlogs_us-west-2_fl-0092b9247c07029b5_20240704T2245Z_2f6b244b.log:31:2 400671120782 eni
-069cdb38de46ac440 18.222.174.25 10.0.1.143 49448 21001 6 1 40 1720133139 1720133168 REJECT OK
```

```
[ec2-user@cli-host 04]$ grep -rn 22 . | grep REJECT | grep my IP
[ec2-user@cli-host 04]$
```

- *Acá agarramos todas las solicitudes rechazadas, del puerto 22 y que provengan de la IP que nosotros utilizamos para realizar las solicitudes SSH.*

- *Confirmamos que el ID de la interfaz de red que se registra en el registro de flujo coincide con la interfaz de red que se asigna a la instancia del servidor web*

```
[ec2-user@cli-host 04]$ aws ec2 describe-network-interfaces --filters "Name=association.public-ip,Values='3

       5.91.217.45'" --query 'NetworkInterfaces[*].[NetworkInterfaceId,Association.PublicIp]'
[
    [
        "eni-069cdb38de46ac440",
        "35.91.217.45"
    ]
]
[ec2-user@cli-host 04]$ date -d @1554496931
Fri Apr  5 20:42:11 UTC 2019
[ec2-user@cli-host 04]$ date
Fri Jul  5 00:00:46 UTC 2024
[ec2-user@cli-host 04]$
```

- *Las marcas temporales se pueden convertir a un formato legible para el ser humano a través del comando date.*


MUCHAS
GRACIAS