

Enxeñaría de Infraestruturas Informáticas

Grao en Enxeñaría Informática



MEMORIA DE PRÁCTICAS DE AWS

SESIÓN 1: EC2

Para xustificar a realización desta actividade inclúe as capturas e explicacións que se indican. Podes acompañar as capturas cun breve comentario se o consideras necesario. Para a entrega xera un PDF a partir deste documento.

YERAY LOIS SÁNCHEZ

ACTIVIDADE 1

Lanza 3 instancias en 2 grupos de seguridade diferentes e comproba se existe conectividade entre elas.

Paso 1: Modifica o grupo de seguridade *default*.

- **Captura 1.1:** regras de entrada do grupo de seguridade *default*.

Ten que mostrar as regras de entrada modificadas do grupo de seguridade default. A captura ten que ser da consola EC2, incluído o menú superior no que poida verse o nome de usuario e rexión na que se está a traballar.

[EC2](#) > [Grupos de seguridade](#) > [sg-0e953b0ec07654dbb - default](#) > Editar regras de entrada

Editar regras de entrada [Información](#)

Las reglas de entrada controlan el tráfico entrante que puede llegar a la instancia.

Reglas de entrada [Información](#)

Regla de entrada 1 [Eliminar](#)

ID de la regla del grupo de seguridad
sgr-0da34826425002a84

Tipo [Información](#)
Todo el tráfico

Protocolo [Información](#)
Todo

Intervalo de puertos [Información](#)
Todo

Tipo de origen [Información](#)
Personalizada

Origen [Información](#)
sg-0e953b0ec07654dbb
sg-0e953b0ec07654dbb

Descripción: opcional [Información](#)

Regla de entrada 2 [Eliminar](#)

ID de la regla del grupo de seguridad
-

Tipo [Información](#)
SSH

Protocolo [Información](#)
TCP

Intervalo de puertos [Información](#)
22

Tipo de origen [Información](#)
Anywhere-IPv4

Origen [Información](#)
0.0.0.0/0

Descripción: opcional [Información](#)

[Agregar regla](#)

No ha realizado ningún cambio.

Cancelar

Previsualizar los cambios

Guardar reglas

Enxeñaría de Infraestruturas Informáticas - GEI - UDC

Pax.2 de 9

Paso 2: Modifica o teu grupo de seguridade.

- **Captura 2.1:** regras de entrada do teu grupo de seguridade.

Ídem que a captura 1.1 para o teu grupo de seguridade.

[EC2](#) > [Grupos de seguridade](#) > [sg-0ce211c5a47564d23 - yeray-lois-secgroup](#) > Editar regras de entrada

Editar regras de entrada [Información](#)

Las reglas de entrada controlan el tráfico entrante que puede llegar a la instancia.

Reglas de entrada [Información](#)

Regla de entrada 1 Eliminar

ID de la regla del grupo de seguridade

-

Tipo [Información](#)

Todo el tráfico ▼

Protocolo [Información](#)

Todo

Intervalo de puertos [Información](#)

Todo

Tipo de origen [Información](#)

Personalizada ▼

Origen [Información](#)

sg-0ce211c5a47564d23 X

sg-0ce211c5a47564d23 X

Descripción: opcional [Información](#)

Regla de entrada 2 Eliminar

ID de la regla del grupo de seguridade

-

Tipo [Información](#)

SSH ▼

Protocolo [Información](#)

TCP

Intervalo de puertos [Información](#)

22

Tipo de origen [Información](#)

Personalizada ▼

Origen [Información](#)

sg-0e953b0ec07654dbb X

sg-0e953b0ec07654dbb X

Descripción: opcional [Información](#)

Agregar regla

Cancelar

Previsualizar los cambios

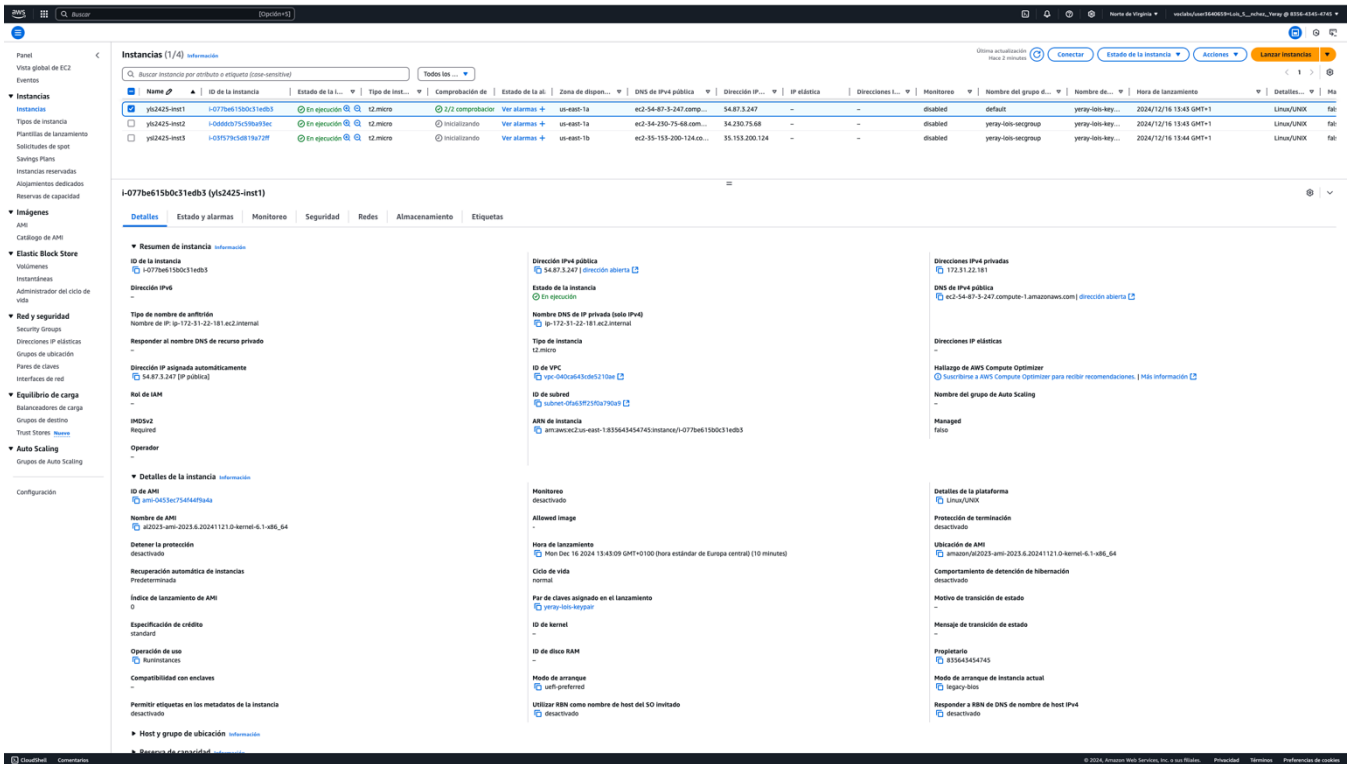
Guardar reglas

Paso 3: Lanza 3 instancias.

- **Captura 3.1:** propiedades da instancia no grupo *default* (instancia 1).

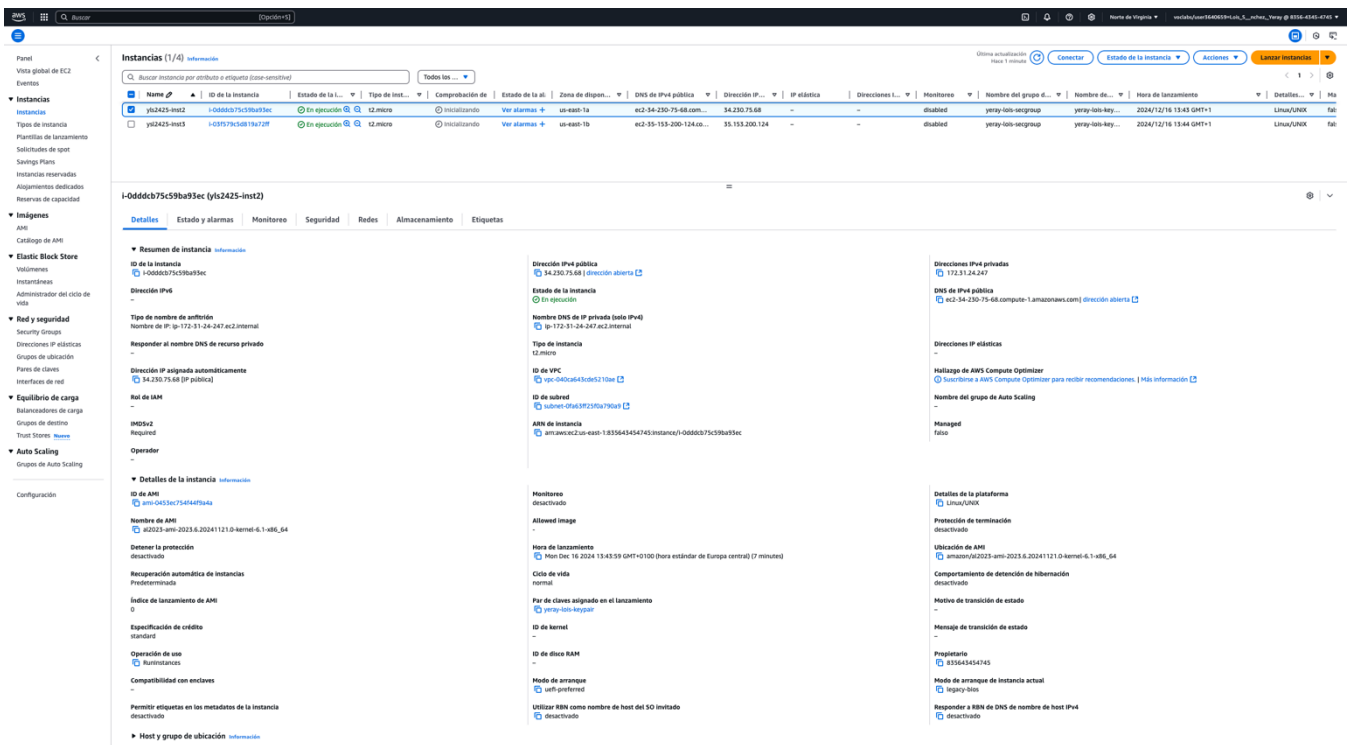
Ten que mostrar as propiedades da instancia lanzada no grupo de seguridade default, en particular: nome (coas túas iniciais e curso como prefixo), ID, tipo, zona de dispoñibilidade, grupo de seguridade, claves de seguridade, data de lanzamento, IP e DNS público e privado. A captura ten que ser da

consola EC2, incluído o menú superior no que poida verse o nome de usuario e rexión na que se está a traballar.



- **Captura 3.2:** propiedades da instancia no teu grupo de seguridade e mesma zona de dispoñibilidade que a instancia do grupo *default* (instancia 2).

Ídem que a captura 3.1 para as propiedades desta instancia.



- Ídem que a captura 3.1 para as propriedades desta instancia.*



- Ten que mostrar o terminal co resultado do intento de conexión SSH á instancia 1. Ten que verse o prompt do teu equipo e o comando SSH usado co nome de usuario e IP ou DNS da instancia. No caso de usar PuTTY teñen que verse tamén as opcións de conexión.*

```
#_
~\   ####_      Amazon Linux 2023
~~ \_ #####\_
~~  \|####|
~~   \|###|
~~~~ \|/_-- https://aws.amazon.com/linux/amazon-linux-2023
~~~~ V'-'>
~~~~ /
~~~~ _.-./-./-/
~~~~ -m/'
```

[ec2-user@ip-172-31-22-181 ~]\$ █

- Ídem que a captura 4.1 para o SSH á instancia 2.*

Pax.5 de 9

- Ídem que a captura 4.1 para o SSH á instancia 3.*

- **Captura 4.4:** conexión SSH desde a instancia 1 á instancia 2.

```
yeray@MacBook-Pro-de-Yeray Downloads % ssh -i "yeray-lois-keypair.pem" ec2-user@ec2-54-175-138-116.compute-1.amazonaws.com
```

```
'#_
~\_-####_      Amazon Linux 2023
~~ \_#####\
~~   \|###|
~~    \|#/     https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~~
~~~.-.-/_-/
        _/_/_/_/m/' '->
```

```
Last login: Mon Dec 16 14:24:55 2024 from 193.144.61.240
[ec2-user@ip-172-31-22-181 ~]$ ssh -i "yeray-lois-keypair.pem" ec2-user@ec2-35-172-199-6.compute-1.amazonaws.com
The authenticity of host 'ec2-35-172-199-6.compute-1.amazonaws.com (172.31.24.247)' can't be established.
ED25519 key fingerprint is SHA256:yYvhCP2plxAgqlhSbRyCnSBdLdOE7OrUq/x1mI2N4VA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-35-172-199-6.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
```

```
'#_
~\_-####_      Amazon Linux 2023
~~ \_#####\
~~   \|###|
~~    \|#/     https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~~
~~~.-.-/_-/
        _/_/_/_/m/' '->
```

```
[ec2-user@ip-172-31-24-247 ~]$
```

- **Captura 4.5:** conexión SSH desde a instancia 1 á instancia 3.

Ídem que a captura 4.4 para o SSH desde a instancia 1 á instancia 3.

```
[yera@MacBook-Pro-de-Yeray Downloads % ssh -i "yera-y-lois-keypair.pem" ec2-user@ec2-54-175-138-116.compute-1.amazonaws.com]
_#_
~\_ #####_      Amazon Linux 2023
~~ \#####\
~~  \###|
~~   \#/ --- https://aws.amazon.com/linux/amazon-linux-2023
~~    V~' '->
~~~~
~~~~_. _/_/_/_/
~~~~_/m/'

Last login: Mon Dec 16 14:25:29 2024 from 193.144.61.240
[ec2-user@ip-172-31-22-181 ~]$ ssh -i "yera-y-lois-keypair.pem" ec2-user@ec2-54-225-31-24.compute-1.amazonaws.com
The authenticity of host 'ec2-54-225-31-24.compute-1.amazonaws.com (172.31.43.61)' can't be established.
ED25519 key fingerprint is SHA256:hDRuG1woRF5zStsKeJUV320Iw6OUmnziUJQ4e248Nko.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-54-225-31-24.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
_#_
~\_ #####_      Amazon Linux 2023
~~ \#####\
~~  \###|
~~   \#/ --- https://aws.amazon.com/linux/amazon-linux-2023
~~    V~' '->
~~~~
~~~~_. _/_/_/_/
~~~~_/m/'

[ec2-user@ip-172-31-43-61 ~]$
```

- **Captura 4.6:** conexión PING de instancia 1 a instancia 2.

Ten que mostrar o terminal co resultado do intento de conexión PING desde a instancia 1 á 2 usando tanto a IP privada como a pública. Teñen que verse o prompt da instancia 1, os comandos PING usados e o resultado dos mesmos.

```
[ec2-user@ip-172-31-22-181 ~]$ ping -c 3 172.31.24.247
PING 172.31.24.247 (172.31.24.247) 56(84) bytes of data.

--- 172.31.24.247 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2111ms

[ec2-user@ip-172-31-22-181 ~]$ ping -c 3 35.172.199.6
PING 35.172.199.6 (35.172.199.6) 56(84) bytes of data.

--- 35.172.199.6 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2069ms
```

- **Captura 4.7:** conexión PING de instancia 1 a instancia 3.

Ídem que a captura 4.6 para o PING da instancia 1 á 3.

```
[ec2-user@ip-172-31-22-181 ~]$ ping -c 3 172.31.43.61
PING 172.31.43.61 (172.31.43.61) 56(84) bytes of data.

--- 172.31.43.61 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2103ms

[ec2-user@ip-172-31-22-181 ~]$ ping -c 3 54.225.31.24
PING 54.225.31.24 (54.225.31.24) 56(84) bytes of data.

--- 54.225.31.24 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2088ms
```

- **Captura 4.8:** conexión PING de instancia 2 a instancia 1.

Ídem que a captura 4.6 para o PING da instancia 2 á 1.

```
[ec2-user@ip-172-31-24-247 ~]$ ping -c 3 172.31.22.181
PING 172.31.22.181 (172.31.22.181) 56(84) bytes of data.

--- 172.31.22.181 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2046ms

[ec2-user@ip-172-31-24-247 ~]$ ping -c 3 54.175.138.116
PING 54.175.138.116 (54.175.138.116) 56(84) bytes of data.

--- 54.175.138.116 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2092ms
```

- **Captura 4.9:** conexión PING de instancia 2 a instancia 3.

Ídem que a captura 4.6 para o PING da instancia 2 á 3.

```
[ec2-user@ip-172-31-24-247 ~]$ ping -c 3 172.31.43.61
PING 172.31.43.61 (172.31.43.61) 56(84) bytes of data.
64 bytes from 172.31.43.61: icmp_seq=1 ttl=127 time=4.18 ms
64 bytes from 172.31.43.61: icmp_seq=2 ttl=127 time=1.48 ms
64 bytes from 172.31.43.61: icmp_seq=3 ttl=127 time=1.83 ms

--- 172.31.43.61 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.482/2.494/4.176/1.197 ms
[ec2-user@ip-172-31-24-247 ~]$ ping -c 3 54.225.31.24
PING 54.225.31.24 (54.225.31.24) 56(84) bytes of data.

--- 54.225.31.24 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2110ms
```


- **Captura 4.10:** conexión PING de instancia 3 a instancia 1.

Ídem que a captura 4.6 para o PING da instancia 3 á 1.

```
[ec2-user@ip-172-31-43-61 ~]$ ping -c 3 172.31.22.181
PING 172.31.22.181 (172.31.22.181) 56(84) bytes of data.

--- 172.31.22.181 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2103ms

[ec2-user@ip-172-31-43-61 ~]$ ping -c 3 54.175.138.116
PING 54.175.138.116 (54.175.138.116) 56(84) bytes of data.

--- 54.175.138.116 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2112ms
```

- **Captura 4.11:** conexión PING de instancia 3 a instancia 2.

Ídem que a captura 4.6 para o PING da instancia 3 á 2.

```
[ec2-user@ip-172-31-43-61 ~]$ ping -c 3 172.31.24.247
PING 172.31.24.247 (172.31.24.247) 56(84) bytes of data.
64 bytes from 172.31.24.247: icmp_seq=1 ttl=127 time=1.75 ms
64 bytes from 172.31.24.247: icmp_seq=2 ttl=127 time=1.65 ms
64 bytes from 172.31.24.247: icmp_seq=3 ttl=127 time=1.65 ms

--- 172.31.24.247 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.647/1.684/1.751/0.047 ms
[ec2-user@ip-172-31-43-61 ~]$ ping -c 3 35.172.199.6
PING 35.172.199.6 (35.172.199.6) 56(84) bytes of data.

--- 35.172.199.6 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2101ms
```

Xustifica aquí os resultados obtidos nas probas de PING (usa o espazo que precises, tenta ser breve).

En las pruebas de PING, todas fallan excepto la comunicación entre las IPs privadas de las instancias 2 y 3 ('yls2425-inst2' e 'yls2425-inst3' respectivamente). Esto sucede porque el grupo de seguridad (yls2425-secgroup) permite todo el tráfico de salida, pero el tráfico de entrada solo está permitido si proviene de una instancia que usa el mismo grupo de seguridad (con la excepción del tráfico TCP en el puerto 22).

Debido a esto:

1. Los PINGS desde la instancia 1 hacia la instancia 2 o 3 fallan, independiente de si se usan IPs privadas o públicas, ya que la instancia 1 está fuera del grupo de seguridad de las otras instancias.
2. Los PINGS desde la instancia 2 o 3 entre sí fallan usando sus IPs privadas. Aunque el tráfico sale del grupo, al intentar reingresar con una IP pública, es bloqueado por el grupo de seguridad ya que no está configurado para permitir este tipo de tráfico.