

Ejercicio Crear VPC con EC2 pública y RDS privada

Edición 4 - Team 3

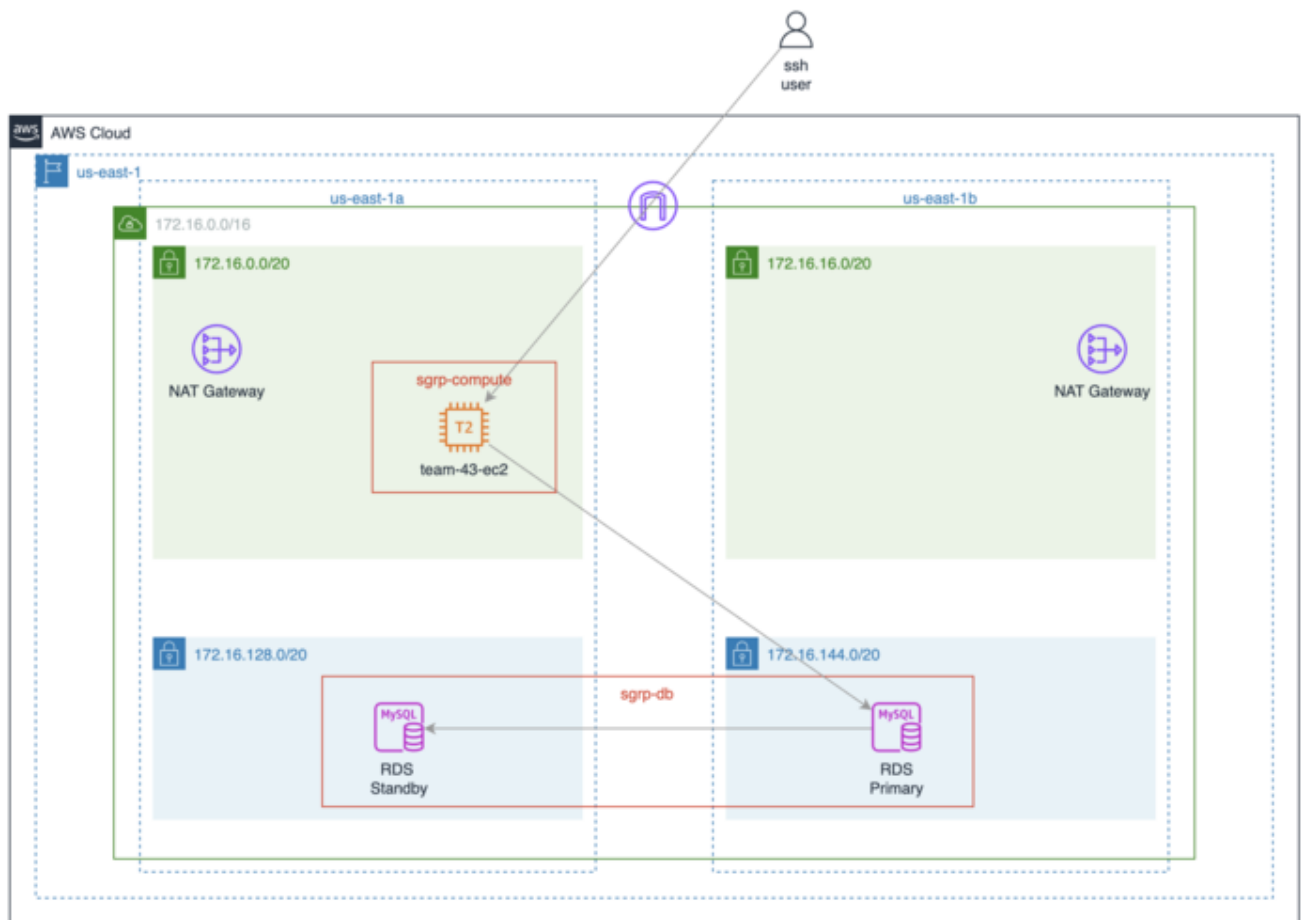
Valentina Muñoz, Fran Rey, Elisabeth Pañell

06/04/2025

Descripción del ejercicio:

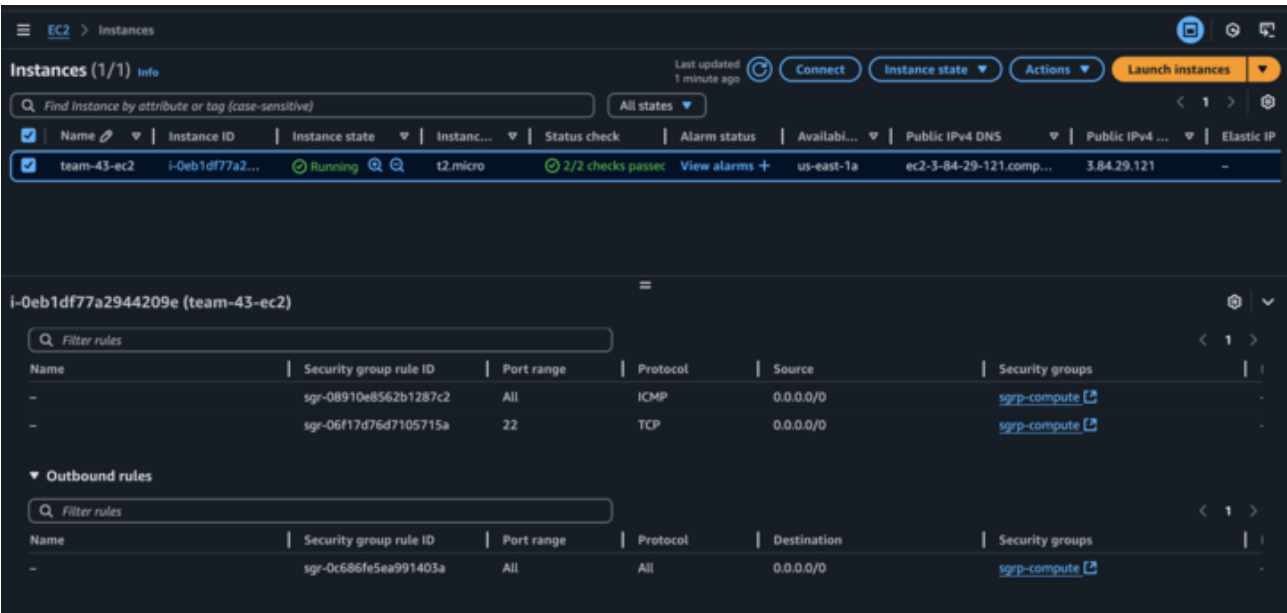
"Crear una VPC multi-az y dentro la zona publica desplegar una EC2 y en la zona privada una RDS y entonces acceder desde la EC2 a la RDS - cual es el challenge? jugar con los security groups para que estén bien configurados - RDS podemos acceder con el cliente de mysql o de postgresql y desde la EC2 ejecutamos una query."

Arquitectura que hemos creado:

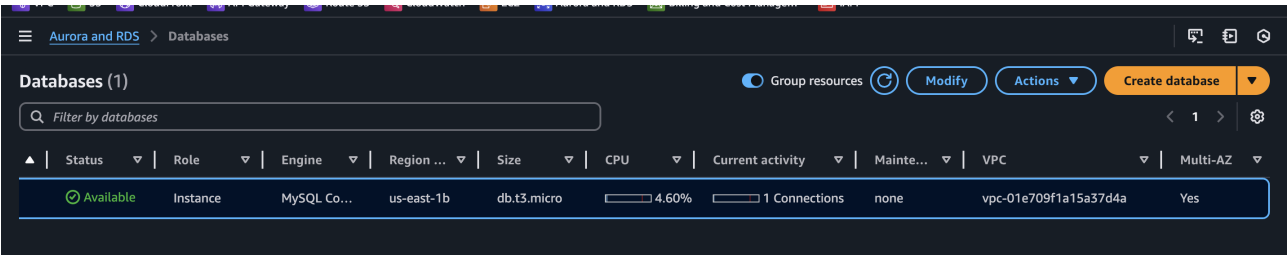


Capturas de la configuración de security groups:

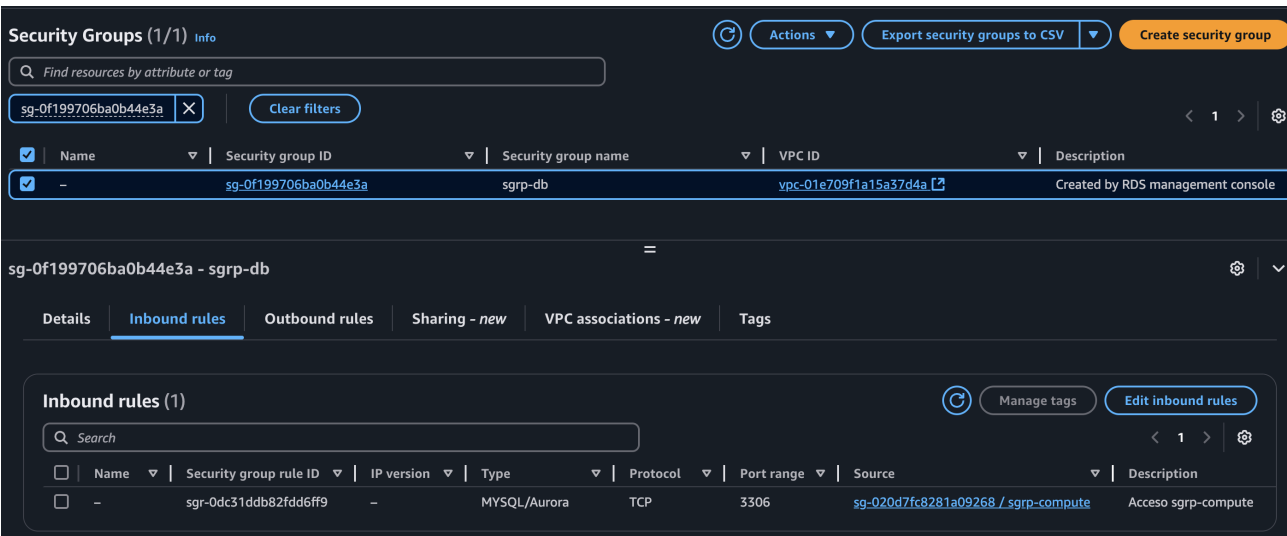
Security Group de la EC2:



Confirmamos que la RDS es multi-AZ:



Security Group de la RDS:




Capturas de conexión exitosa:

Del ordenador a RDS directamente: **falla** (ya que RDS tiene SG con solo acceso para EC2, y está en la subred privada):

```
valentinamunoz@MB2 Downloads %  
valentinamunoz@MB2 Downloads %  
valentinamunoz@MB2 Downloads % telnet rds-team-43.c7p8hbeig0f6.us-east-1.rds.amazonaws.com 3306  
Trying 172.16.150.58...
```

Del ordenador a EC2 directamente: **exitosa** (ya que EC2 tiene SG con acceso anywhere, y está en la subred pública):

```
valentinamunoz@MB2 Downloads %  
valentinamunoz@MB2 Downloads % telnet rds-team-43.c7p8hbeig0f6.us-east-1.rds.amazonaws.com 3306  
Trying 172.16.150.50...  
^C  
valentinamunoz@MB2 Downloads % ssh -i team43.pem ec2-user@3.84.29.121  
hostkeys_find_by_key_hostfile: hostkeys_foreach failed for /Users/valentinamunoz/.ssh/known_hosts: Permission denied  
The authenticity of host '3.84.29.121 (3.84.29.121)' can't be established.  
ED25519 key fingerprint is SHA256:Ngl3czu0eRmXis06vvT5fqss3XJQkv89pJaXaXM5Zns.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Failed to add the host to the list of known hosts (/Users/valentinamunoz/.ssh/known_hosts).  
client_input_hostkeys: hostkeys_foreach failed for /Users/valentinamunoz/.ssh/known_hosts: Permission denied
```



```
#  
#####  
Amazon Linux 2023  
  
#####  
\\###|  
\\#/  
V~' '~>  
  
https://aws.amazon.com/linux/amazon-linux-2023  
  
Last login: Sun Apr  6 17:47:26 2025 from 31.4.247.19  
[ec2-user@ip-172-16-0-64 ~]$ telnet rds-team-43.c7p8hbeig0f6.us-east-1.rds.amazonaws.com 3306  
Trying 172.16.150.50...  
Connected to rds-team-43.c7p8hbeig0f6.us-east-1.rds.amazonaws.com.  
Escape character is '^['.  
J  
8.0.40I  
Nx-N%?E]DjUmysql_native_password2#08501Got timeout reading communication packetsConnection closed by foreign host.  
[ec2-user@ip-172-16-0-64 ~]$
```

De la EC2 a RDS directamente: **exitosa** (ya que RDS en subred privada tiene SG con acceso al SG de la EC2):

```
mariadb105-common-3:10.5.25-1.amzn2023.0.1.x86_64 perl-Sys-Hostname-1.23-477.amzn2023.0.6.x86_64
Complete!
[ec2-user@ip-172-16-0-64 ~]$ mysql -h rds-team-43.c7p8hbeig0f6.us-east-1.rds.amazonaws.com -P 3306 -u admin43 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 34
Server version: 8.0.40 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

Paso por paso detallado:

(Quizás no hace falta leerlo todo, era para tenerlo todo documentado como parte del proceso de aprendizaje)

Pasos que hemos ido haciendo:

1. Crear VPC:

- Escogemos IPv4 CIDR block eg. 172.16.0.0/16
- (privada y no coincide con otras IPs de nuestro on premise que podrían overlap)
- Nombre team-43
- 2 AZs: (HA)
- 2 subredes públicas
- 2 subredes privadas
- 3 custom route tables
 - (1 compartida por las 2 públicas,
 - 2 una para cada privada)
- 2 network connections:
 - (1 internet gateway - para privada) igw
 - (2 nat gateways - para pública) nat

2. Creamos EC2 en la pública (nos parece raro, pero así lo pide el ejercicio, quizás no es 'best practices')

- Amazon linux 2023
- Instance type: t2.micro (free layer)
- Key pair (creamos una nueva llave .pem)
- Network settings escogemos nuestra VPC, y la primera subred pública
- **Enable auto-assign public IP!!** porque la red que hemos creado nosotros "pública" tiene IP privada
- Create security Group de EC2 (sgrp-compute)
 - de entrada y salida de shell EC2 a anywhere (aka ssh - secure shell)
 - también una de ICMP para poder hacer test de la conexión haciendo 'ping'
- Disco duro dejamos default
 - (aquí podríamos añadir user data, pero lo haremos manualmente para ver proceso)
si fuese por user data:
en el EC2 añadimos user data para amazon linux 2023 que tenga instalado el cliente de mysql para usar directamente desde la shell, y ya tenerlo una vez abierto
- **EC2 creado y hemos comprobado conexión anywhere con el ping:**
nos conectamos:

```
bethpanell@portatilBeth ~  
$ ping 3.84.29.121  
PING 3.84.29.121 (3.84.29.121): 56 data bytes  
64 bytes from 3.84.29.121: icmp_seq=0 ttl=114 time=117.289 ms  
64 bytes from 3.84.29.121: icmp_seq=1 ttl=114 time=118.378 ms  
64 bytes from 3.84.29.121: icmp_seq=2 ttl=114 time=115.271 ms  
64 bytes from 3.84.29.121: icmp_seq=3 ttl=114 time=113.074 ms  
64 bytes from 3.84.29.121: icmp_seq=4 ttl=114 time=114.961 ms  
64 bytes from 3.84.29.121: icmp_seq=5 ttl=114 time=116.396 ms  
64 bytes from 3.84.29.121: icmp_seq=6 ttl=114 time=117.089 ms  
64 bytes from 3.84.29.121: icmp_seq=7 ttl=114 time=116.198 ms  
64 bytes from 3.84.29.121: icmp_seq=8 ttl=114 time=115.712 ms  
64 bytes from 3.84.29.121: icmp_seq=9 ttl=114 time=114.204 ms
```

- [illegible]

- Hemos elegido mysql
- Escogemos dev/test (free tier no nos deja multi-az)
- Escogemos multi-az db instance deployment con write endpoint + standby
- Credential setting (self managed para no depender de AWS secrets manager para este use case)
- Instance configuration
 - Usamos t3.micro por limitación de laboratorio
- Storage ssd gp3 (general), y 20 GiB porque en este caso no necesitaremos más
 - con enabled auto scaling hasta 30GiB
- Connectivity

- no conectamos con ec2 ya que lo haremos manualmente como parte de este challenge
- y subnet group nuestro
- y public access NO (ya que queremos la RDS en privado, y el subnet group es privado)
- crear new security group: sggrp-db
 - (aquí no nos da la opción de configurarlo solo lo creamos y luego lo conectaremos con EC2)
- puerto por defecto 3306 por defecto de mysql
- sin monitoring *
- le llamamos a nuestro database: db1team43 (podríamos añadir más databases)
- sin backups *
- sin encryptions *
 - * estos los quitamos porque aunque son importantes van a ser más lentos

5. Configuramos security groups

- El de la rds sggrp-db por defecto nos ha dado acceso al IP del pc (no vamos a llegar ya que está en la privada, esto lo tenemos que cambiar)
- Editamos y borramos el default
- Agregamos regla de mysql (3306) a la EC2 (sg)
 - para hacerlo en vez de hacer EC2 (y luego si hiciéramos horizontal scaling tendríamos que añadir) haremos directamente al security group del EC2 sggrp-compute

6. Hacemos pruebas de conexión:

- De equipo local ('anywhere') a RDS
 - como RDS está en la privada (y SG solo deja al SG de la EC2) esperamos que esto falle:

1. no ha llegado (trying pero no acaba nunca):

```
valentinamunoz@MB2 Downloads % telnet rds-team-43.c7p8hbeig0f6.us-east-1.rds.amazonaws.com 3306
Trying 172.16.150.58...
```

- 2.
- 3.

- de equipo local ('anywhere') a EC2:
 - como EC2 está en la pública y SG de EC2 a anywhere esperamos que se conecte:

4. se ha conectado:

```

valentinamunoz@MB2 Downloads % valentinamunoz@MB2 Downloads % telnet rds-team-43.c7p8hbeig0f6.us-east-1.rds.amazonaws.com 3306
Trying 172.16.150.58...
^C
valentinamunoz@MB2 Downloads % ssh -i team43.pem ec2-user@3.84.29.121
hostkeys_find_by_key_hostfile: hostkeys_foreach failed for /Users/valentinamunoz/.ssh/known_hosts: Permission denied
The authenticity of host '3.84.29.121 (3.84.29.121)' can't be established.
ED25519 key fingerprint is SHA256:Ngl3czu0eRmXis06vvT5fqss3XJQkv89pJaXaXM5zns.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Failed to add the host to the list of known hosts (/Users/valentinamunoz/.ssh/known_hosts).
client_input_hostkeys: hostkeys_foreach failed for /Users/valentinamunoz/.ssh/known_hosts: Permission denied

#####
#####\
#####|
\#/\
V- ' ->
/
/m/ '
Last login: Sun Apr 6 17:47:26 2025 from 31.4.247.19
[ec2-user@ip-172-16-0-64 ~]$ telnet rds-team-43.c7p8hbeig0f6.us-east-1.rds.amazonaws.com 3306
Trying 172.16.150.58...
Connected to rds-team-43.c7p8hbeig0f6.us-east-1.rds.amazonaws.com.
Escape character is '^['.
J
0.0.40I
Nx-NX?EjDjUmynsl_native_password2#08501Got timeout reading communication packetsConnection closed by foreign host.
[ec2-user@ip-172-16-0-64 ~]$

```

- ahora de la EC2 nos conectamos a RDS:
 - formato para conectar con mysql:
 - `mysql -h (endpoint de RDS) -P (puerto RDS) -u (admin name) -p`
 - ahora no nos deja aún porque hay que instalar el `mySQL`
 - instalamos el cliente (`mySQL` o `mariadb105`)
 - volvemos con el commando
 - ponemos la password anterior
 - y hemos llegado!

```
mariadb105-common-3:10.5.25-1.amzn2023.0.1.x86_64 perl-Sys-Hostname-1.23-477.amzn2023.0.6.x86_64
Complete!
[ec2-user@ip-172-16-0-64 ~]$ mysql -h rds-team-43.c7p8hbeig0f6.us-east-1.rds.amazonaws.com -P 3306 -u admin43 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 34
Server version: 8.0.40 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```