

ENUNCIADO

Deberás crear la siguiente infraestructura en una región de AWS:

- 1 VPC
- Dos subredes en zonas de disponibilidad diferentes, una subred pública y otra subred privada configurando las tablas de enrutamiento necesarias para esta configuración.
- Una instancia EC2 en cada una de las subredes con sus correspondientes Security Groups.
- Para la instancia que está en la subred pública, el SG debe permitir SSH y HTTP desde cualquier IP de origen.
 - Para la instancia que está en la subred privada, el SG solo debe permitir SSH desde las direcciones IP de la subred pública y no debe permitir ningún tipo de tráfico desde cualquier otro rango de direcciones IP.
 - La creación de las subredes y los Security Groups puede hacerse desde la consola web, pero la creación de las máquinas debe ser desde AWS CLI.
- La instancia EC2 que está en la subred pública debe tener instalado el servicio web de Apache y la instalación debe ser mediante un script "user data".

Tarea 1 (50 puntos): Creación de la VPC y las subredes.

Tarea 2 (50 puntos): Creación de las instancias EC2 y los Security Groups.

Tal y como se pide en el enunciado lo primero que he hecho ha sido crear una VPC con la siguiente dirección de red: 10.0.0.0/16.

Create VPC info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create info
Create only the VPC resource or the VPC and other networking resources.
☒ VPC only ☐ VPC and more

Name tag - optional info
Creates a tag with a key of 'Name' and a value that you specify.
mruiz-vpc

IPv4 CIDR block info
☒ IPv4 CIDR manual input
☐ IPAM-allocated IPv4 CIDR block
10.0.0.0/16

IPv6 CIDR block info
☒ No IPv6 CIDR block
☐ IPAM-allocated IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block
☐ IPv6 CIDR owned by me

Tenancy info
Default

Tags info
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources to track your AWS costs.

Key **Value - optional**

You can add 49 more tags.

Después he creado una subred (mruiz-public) en la AZ us-east-1a.

Create subnet info

VPC

VPC ID info
Create subnets in this VPC.
vpc-0627226b07b18fbc7 (mruiz-vpc)

Associated VPC CIDRs info
IPv4 CIDRs
10.0.0.0/16

Subnet settings info
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name info
Create a tag with a key of 'Name' and a value that you specify.
mruiz-public
The name can be up to 256 characters long.

Availability Zone info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1a

IPv4 CIDR block info
10.0.1/24

Tags - optional info

Key **Value - optional**

You can add 49 more tags.

y otra subred (mruiz-private) en la AZ us-east-1b.

Create subnet info

VPC

VPC ID info
Create subnets in this VPC.
vpc-0627226b07b18fbc7 (mruiz-vpc)

Associated VPC CIDRs info
IPv4 CIDRs
10.0.0.0/16

Subnet settings info
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name info
Create a tag with a key of 'Name' and a value that you specify.
mruiz-private
The name can be up to 256 characters long.

Availability Zone info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1b

IPv4 CIDR block info
10.0.2/24

Tags - optional info

Key **Value - optional**

You can add 49 more tags.

Acto seguido he creado una Internet Gateway para asociarla a la subred pública y que ésta tenga acceso a internet.

The screenshot shows the 'Create internet gateway' page in the AWS Management Console. The page title is 'Create internet gateway'. Below the title, there is a brief description: 'An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.' The main section is 'Internet gateway settings'. It includes a 'Name tag' field with the value 'emula-ig'. Below this, there is a 'Tags - optional' section with a table for adding tags. The table has columns for 'Key' and 'Value - optional'. A single tag is added with the key 'Name' and the value 'emula-ig'. At the bottom of the page, there are 'Cancel' and 'Create internet gateway' buttons.

La asociamos a nuestra VPC.

The screenshot shows the 'Attach to VPC' page in the AWS Management Console. The page title is 'Attach to VPC (igw-02eb33287d1df05b4)'. Below the title, there is a brief description: 'Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.' The main section is 'VPC'. It includes a search bar for 'Available VPCs' and a list of VPCs. One VPC is listed: 'vpc-0627810e7b1e9b07'. Below the list, there is a section for 'AWS Command Line Interface command'. At the bottom of the page, there are 'Cancel' and 'Attach internet gateway' buttons.

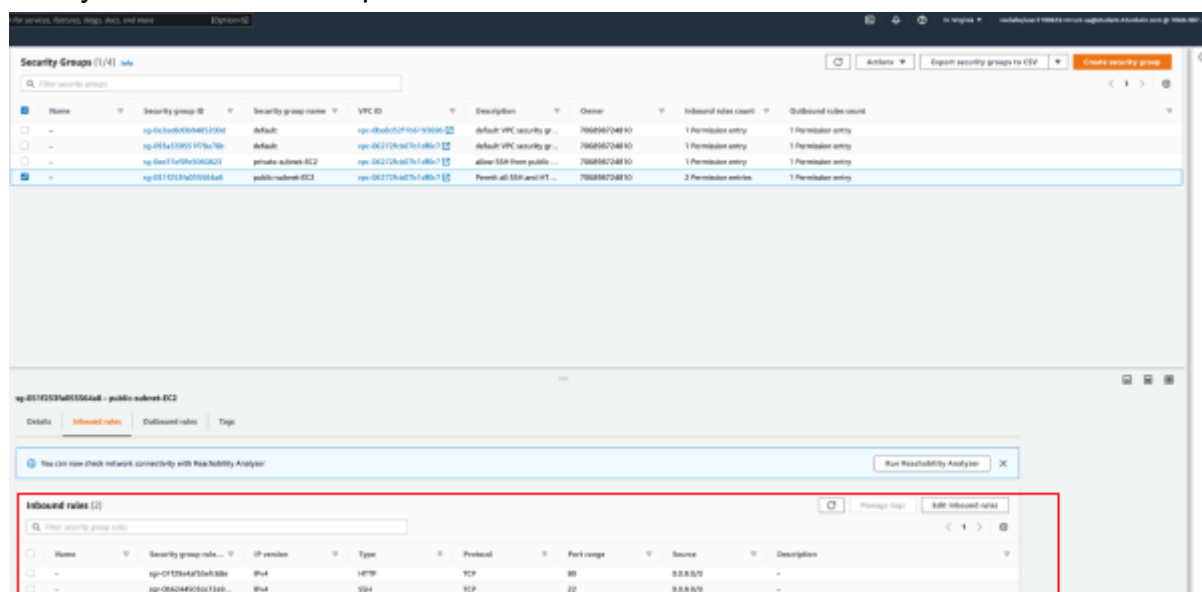
Y editamos la tabla de enrutamiento asociada a la subred pública para que todo el tráfico vaya a la internet gateway.

The screenshot shows the 'Edit routes' page in the AWS Management Console. The page title is 'Edit routes'. Below the title, there is a table with columns: 'Destination', 'Target', 'Status', and 'Propagated'. The table has two rows. The first row has '10.0.0.0/16' as the destination, 'local' as the target, 'Active' as the status, and 'No' as the propagated status. The second row has '0.0.0.0/0' as the destination, 'igw-02eb33287d1df05b4' as the target, '-' as the status, and 'No' as the propagated status. At the bottom of the page, there are 'Cancel', 'Preview', and 'Save changes' buttons.

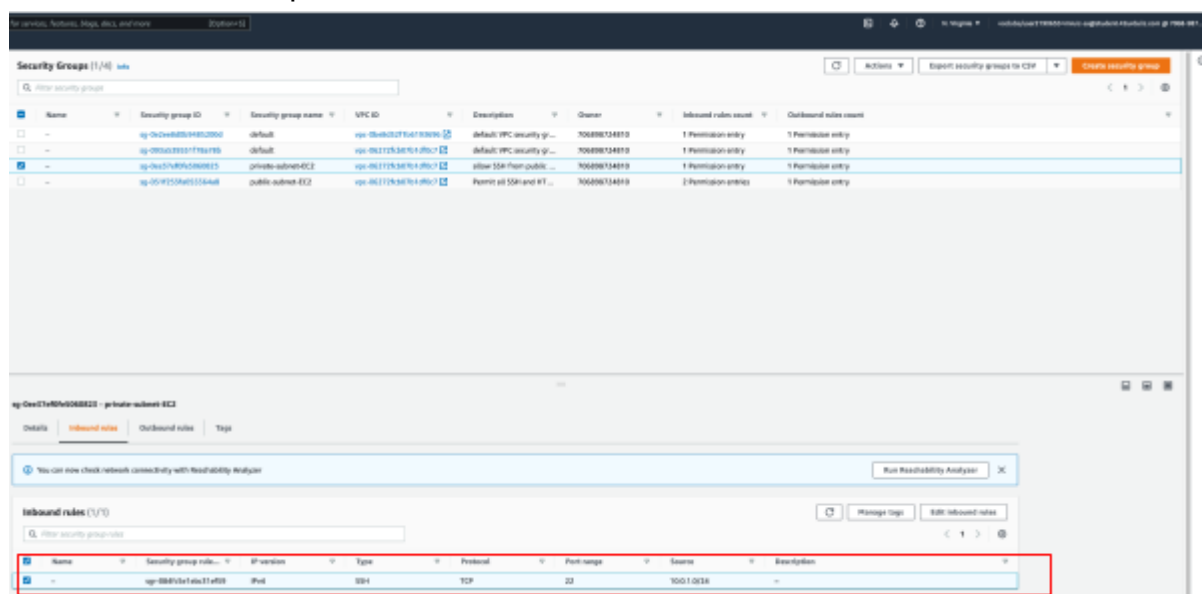
Después creamos una tabla de enrutamiento nueva para la subred privada solo con la regla que permita el tráfico entre subredes.

The screenshot shows the 'Route tables' page in the AWS Management Console. The page title is 'Route tables'. Below the title, there is a table with columns: 'Name', 'Route table ID', 'VPC', 'Status', and 'Propagated'. The table has three rows. The first row is 'main-route-table' with ID 'rtb-09f0e4f95c5f77e49', VPC 'vpc-0627810e7b1e9b07', and status 'Active'. The second row is 'private-route-table' with ID 'rtb-0627810e7b1e9b07', VPC 'vpc-0627810e7b1e9b07', and status 'Active'. The third row is 'public-route-table' with ID 'rtb-0627810e7b1e9b07', VPC 'vpc-0627810e7b1e9b07', and status 'Active'. Below the table, there is a section for 'Route table details' for the 'private-route-table'. It includes a 'Routes' tab with a table showing a single route with destination '10.0.0.0/16' and target 'local'. At the bottom of the page, there are 'Cancel', 'Preview', and 'Save changes' buttons.

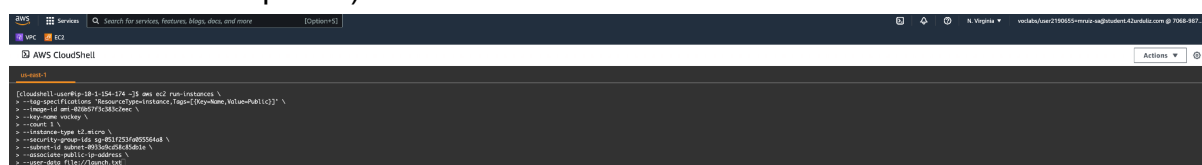
Creamos el security group de la instancia en la subred pública permitiendo el tráfico SSH y HTTP desde cualquier IP.



Y el SG de la instancia en la subred privada permitiendo el tráfico SSH de las IPs dentro de la subred pública.



Lanzamos la instancia de la subred pública con el comando `aws ec2 run-instances` y todas las especificaciones de la misma con las flags que se ven en la imagen. (en user data he metido el script que utilizamos en el Lab del módulo 5 para montar un Web Server con Apache).



La instancia de la subred privada la hemos lanzado de la misma manera, pero obviamente cambiando el ID del security group y el ID de la subred, y tampoco hemos lanzado el user data ni hemos asociado una IP pública.

Por último escribimos en el navegador la IP pública de la subred pública y vemos como nos ha conectado con el servidor web que hemos lanzado.

