

AWS EVALUATION

1. AWS Academy Cloud Foundations (Theory)

• Módulo 1 - Información general sobre los conceptos de la nube	Completa todos los ítems ✓
• Módulo 2 - Facturación y economía de la nube	Completa todos los ítems ✓
• Módulo 3 - Información general sobre la infraestructura global de AWS	Completa todos los ítems ✓
• Módulo 4 - Seguridad en la nube	Completa todos los ítems ✓
• Módulo 5 - Redes y entrega de contenido	Completa todos los ítems ✓
• Módulo 6 - Informática	Completa todos los ítems ✓
• Módulo 7 - Almacenamiento	Completa todos los ítems ✓
• Módulo 8 - Bases de datos	Completa todos los ítems ✓
• Módulo 9 - Arquitectura en la nube	Completa todos los ítems ✓
• Módulo 10 - Monitoreo y escalado automático	Completa todos los ítems ✓

2.a. Creación de una VPC donde instalar las instancias que vamos a usar.

Crear una VPC con las siguientes condiciones:

- Se trata de montar una infraestructura para una empresa que va a tener dos subredes, una pública y otra privada. Cada una de las subredes estará dispersa en dos zonas de disponibilidad de la región para más disponibilidad y seguridad.
- La zona pública deberá tener salida a Internet a través de un gateway propio creado para la VPC.
- El rango de direcciones de la VPC será el CIDR 10.0.0.0/16 y cada una de las dos subredes tendrá los CIDR 10.0.1.0/24 y 10.0.2.0/24 respectivamente.
- La subred pública se llamará "vpc_publica_test" y la privada "vpc_privada_test".
- Se creará una tabla de enrutamiento que permita salida a Internet a la subred pública, pero no a la privada.

Ficha técnica:

- Nombre VPC: vpc_< tus iniciales >
- Subred pública: vpc_publica_test
- Subred privada: vpc_privada_test
- CIDR VPC: 10.0.0.0/16
- CIDR público: 10.0.1.0/24
- CIDR privado: 10.0.2.0/24

Salida a Internet (subred pública):



Lo primero es iniciar el Learner Lab del entorno de AWS.

The screenshot shows the AWS Learner Lab interface. The main area displays a large blue 'V' logo. On the right side, there is a sidebar with the following sections:

- Learner Lab**
 - [Environment Overview](#)
 - [Environment Navigation](#)
 - [Access the AWS Management Console](#)
 - [Region restrictions](#)
 - [Service usage and other restrictions](#)
 - [Using the terminal in the browser](#)
 - [Running AWS CLI commands](#)
 - [Using the AWS SDK for Python](#)
 - [Preserving your budget](#)
 - [Accessing EC2 instances](#)
 - [SSH Access to EC2 instances](#)
 - [SSH Access from Windows](#)
 - [SSH Access from a Mac](#)
- Environment Overview**

This Learner Lab provides a sandbox environment for ad-hoc exploration of AWS services.

This environment is long-lived. When the session timer runs to 0:00, the session will end, but any data and resources that you created in the AWS account will be retained. If you later launch a new session (for example, the next day), you will find that your work is still in the lab environment.

Running EC2 instances will be stopped and then automatically restarted the next time you start a session. SageMaker notebook instances will be stopped, but not restarted the next time you start a session.

IMPORTANT: Monitor your lab budget in the lab interface above. Whenever you have an active lab session, the latest known remaining budget information will display at the top of this screen. This data comes from AWS Budgets which typically updates every 8 to 12 hours. Therefore the remaining budget that you see may not reflect your most recent account activity. **If you exceed your lab budget your lab account will be disabled and all progress and resources will be lost.** Therefore, it is important for you to manage your spending. Read about [how to preserve your budget](#).
- Environment Navigation**

Una vez dentro del panel de control, buscamos "vpc" en la barra de búsqueda y clicamos en la opción que nos llevará al menú principal para poder trabajar con las VPC.



Entre las opciones que ofrece este panel de control, debemos elegir primero la de crear una nueva VPC.



Nos encontramos con una serie de ajustes que podemos cambiar o dejar de forma predeterminada. Para empezar, marcamos la opción "VPC only" de la izquierda, ya que por ahora solo queremos crear una VPC básica.

Se le asigna un nombre ("vpc_< tusiniciales >"). Se establece el CIDR que nos pide el ejercicio y, por último, añadimos una etiqueta "AWSEvaluation" con valor "1daw" (esto es solo un ejemplo, la etiqueta puede ser cualquiera, simplemente debe ser identificable).

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*
Creates a tag with a key of 'Name' and a value that you specify.

vpc_cms

IPv4 CIDR block [Info](#)
☒ IPv4 CIDR manual input ☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
10.0.0.0/16

Esto último lo haremos siempre que se presente la opción de añadir una nueva etiqueta para poder encontrar los elementos de forma más sencilla en caso de ser necesario.

Tags

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 or track your AWS costs.

Key	Value - optional	
Name	vpc_cms	Remove
AWSEvaluation	1daw	Remove

[Add new tag](#)
You can add 48 more tags.

Hacemos clic en el botón "Create VPC" y podemos ver cómo la VPC se ha creado correctamente con los ajustes definidos.

You successfully created vpc-09555c98614ee63ff / vpc_cms

VPC > Your VPCs > vpc-09555c98614ee63ff

vpc-09555c98614ee63ff / vpc_cms

Details		Info	
VPC ID	vpc-09555c98614ee63ff	State	Available
Tenancy	Default	DHCP option set	dopt-080c8b9907a7f43ac
Default VPC	No	IPv4 CIDR	10.0.0.0/16
Network Address Usage metrics	Disabled	Route 53 Resolver DNS Firewall rule groups	Failed to load rule groups
DNS hostnames	Disabled	Main route table	rtb-06b16fec18bd21985
DNS resolution	Enabled	IPv6 pool	-
Main network ACL	acl-0160feb37706714c3	Owner ID	808925875888
IPv6 CIDR (Network border group)	-		

El siguiente paso es dirigirse al panel lateral de la izquierda para entrar en el apartado "Subnets".



Una vez dentro, localizamos la opción "Create subnet", en la esquina superior derecha del menú. Hacemos clic en ella.

Se nos presenta un menú de creación similar al anterior para crear la subred nueva.

En el desplegable que aparece en el primer cuadro se debe seleccionar la VPC que creamos anteriormente:



De esta forma hemos vinculado la nueva subred que vamos a crear a la VPC con la que trabajaremos en este ejercicio.

En el siguiente cuadro aparecen nuevos ajustes. Debemos establecer un nombre para la nueva subred (tendremos que crear dos subredes, por lo que esta primera se llamará "vpc_publica_test").

Es importante que la zona de disponibilidad sea "US East (N. Virginia) / ...", ya que es donde se localiza la versión de AWS que tenemos disponible con nuestro correo corporativo.

Adicionalmente, se le asigna un rango CIDR a la subred (el cual lo da el enunciado del ejercicio) y una etiqueta nueva para tener la posibilidad de localizar este elemento de forma fácil y rápida si es necesario.

El rango CIDR para la subred pública es 10.0.1.0/24. Se pone la misma etiqueta en todos los elementos.

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

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
vpc_publica_test
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](#)
10.0.1.0/24

Tags - optional

Key	Value - optional	
Name	vpc_publica_test	Remove
AWSEvaluation	1daw	Remove

Terminamos de crear la nueva subred y esto nos lleva al panel de control de las subredes, donde podemos ver que la subred se ha creado con éxito.

You have successfully created 1 subnet: subnet-01549b01ed8c7782c

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone	Availability Zone ID	Name tags
vpc_publica_test	subnet-01549b01ed8c7782c	Available	vpc-09555c98614ee63ff	10.0.1.0/24		251	us-east-1a	us-east-1a	vpc_publica_test

Ahora es necesario realizar el mismo proceso para la subred privada, pero cambiando los valores pertinentes.

Se vuelve a seleccionar la VPC que creamos anteriormente en el desplegable del primer cuadro y se establece el nombre correspondiente a esta segunda subred, su rango CIDR (en este caso, 10.0.2.0/24) y su zona de disponibilidad, la cual es distinta de la anterior subred (esta zona de disponibilidad es la que termina en "us-east-1b").

VPC

VPC ID
Create subnets in this VPC.

vpc-09555c98614ee63ff (vpc_cms)

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

vpc_privada_test

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](#)

10.0.2.0/24

▼ Tags - optional

Key	Value - optional	
Name	vpc_privada_test	Remove
AWSEvaluation	1daw	Remove

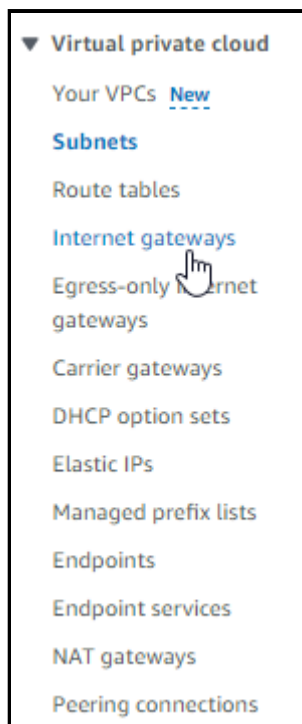
[Add new tag](#)

You can add 48 more tags.

[Remove](#)

[Add new subnet](#)

Una vez creadas las dos subredes, volvemos al menú lateral izquierdo para entrar en el menú "Internet gateways". La subred pública debe poder salir a Internet si es necesario, para ello hace falta una puerta de enlace.



Seguimos el mismo proceso inicial que en los demás paneles de control y hacemos clic en el botón "Create internet gateway" en la esquina superior derecha.

Establecemos un nombre para la nueva puerta de enlace y la asignamos la misma etiqueta de siempre. El nombre puede seguir el patrón "gw_vpc_< tusiniciales >", por ejemplo, aunque se le puede poner cualquier nombre (preferiblemente reconocible).

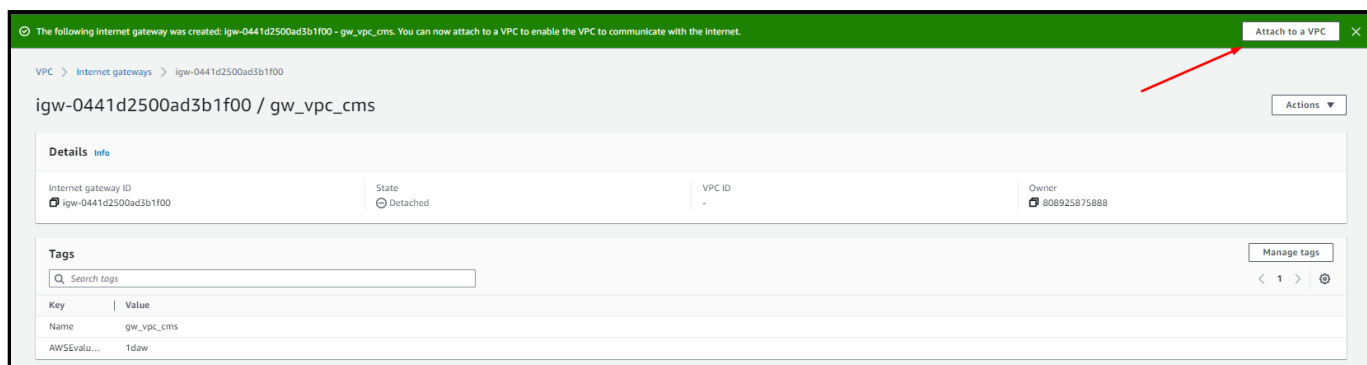
A screenshot of the 'Internet gateway settings' form in the AWS console. The 'Name tag' section has a text input field containing 'gw_vpc_cms'. Below this is the 'Tags - optional' section, which includes a description: 'A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search your resources or track your AWS costs.' There are two rows of tag inputs. The first row has a 'Key' of 'Name' and a 'Value - optional' of 'gw_vpc_cms'. The second row has a 'Key' of 'AWSEvaluation' and a 'Value - optional' of '1daw'. Each row has a 'Remove' button to its right.

Clicamos en el botón de creación para terminar de crear el gateway.

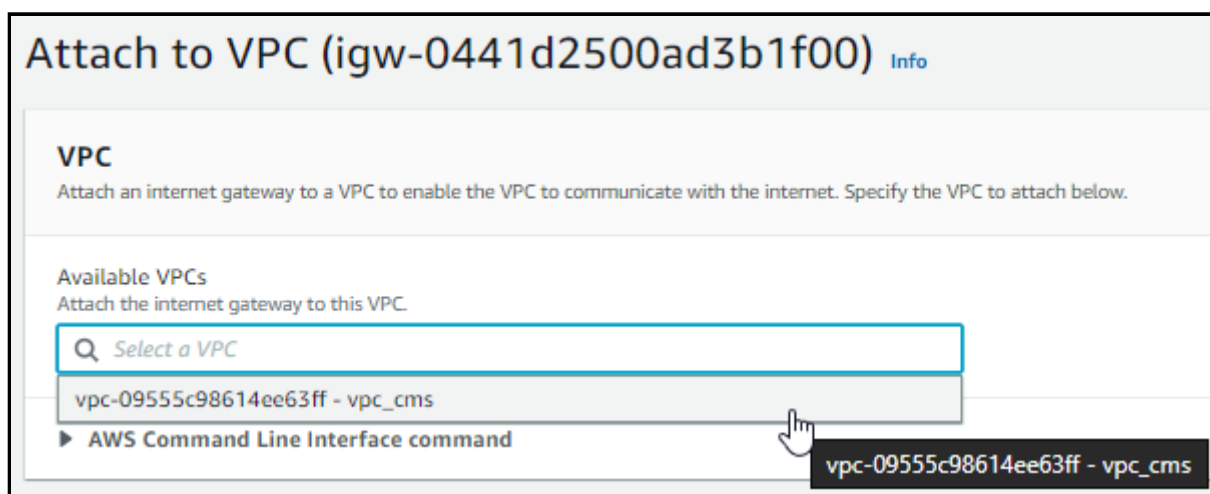
Al crearse, salimos automáticamente al panel de control, y más concretamente al apartado del propio gateway que se acaba de crear.

Ahora es necesario vincular esta puerta de enlace recién creada con la VPC que creamos anteriormente. Para ello debemos hacer clic en el botón "Attach to a VPC" que aparece en la esquina superior derecha justo

después de terminar de crear el gateway.



Una vez dentro, simplemente seleccionamos nuestro VPC en el desplegable que aparece en el cuadro de ajustes.



Clicamos en el botón de confirmación y se vincula la puerta de enlace con la VPC.

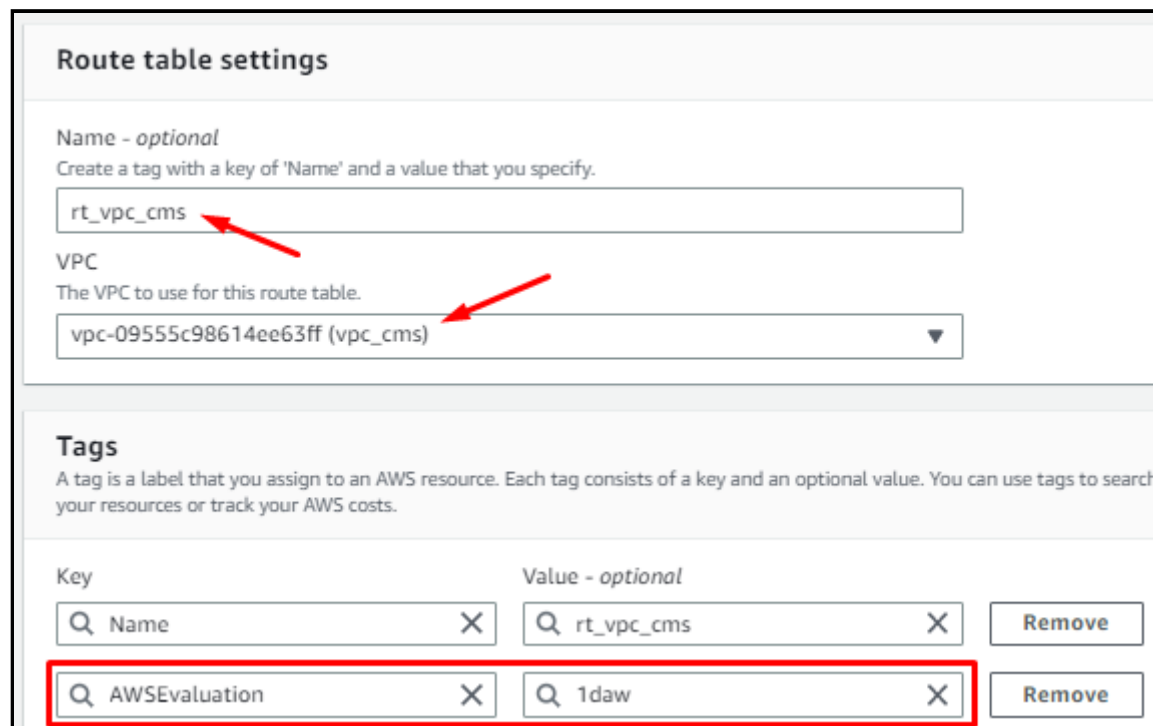
Una vez más, vamos al menú lateral izquierdo, esta vez a la opción "Route tables".



Como venimos haciendo en cada menú, hacemos clic en el botón "Create route table" en la esquina superior derecha.

Para el nombre de la nueva tabla de enrutamiento podemos seguir el mismo patrón que utilizamos anteriormente, el cual es "rt_vpc_< tus iniciales >".

Seleccionamos de nuevo la VPC a la que se añade esta nueva tabla de enrutamiento en el desplegable, y por último, añadimos la etiqueta que utilizamos en todos los elementos.



Route table settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

rt_vpc_cms

VPC
The VPC to use for this route table.

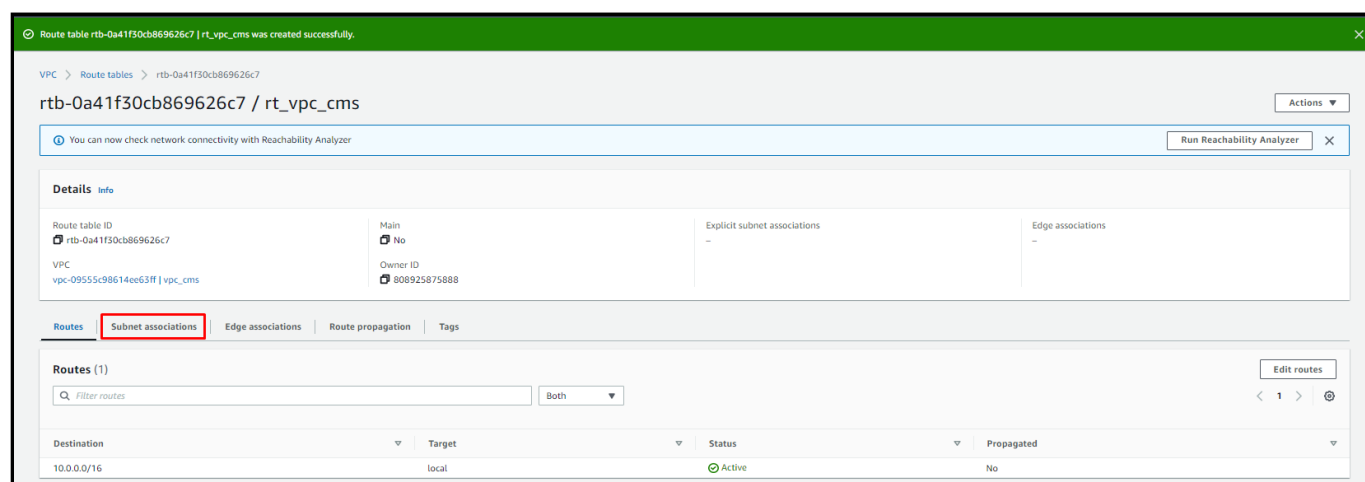
vpc-09555c98614ee63ff (vpc_cms)

Tags
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 your resources or track your AWS costs.

Key	Value - optional	
Name	rt_vpc_cms	Remove
AWSEvaluation	1daw	Remove

Una vez hacemos clic en el botón de confirmación, aparece un menú similar al de siempre que se crea un nuevo elemento.

En este nuevo menú, vemos una pestaña llamada "Subnet associations". Entramos en dicha pestaña.



Route table rtb-0a41f30cb869626c7 | rt_vpc_cms was created successfully.

VPC > Route tables > rtb-0a41f30cb869626c7

rtb-0a41f30cb869626c7 / rt_vpc_cms

You can now check network connectivity with Reachability Analyzer. [Run Reachability Analyzer](#)

Details

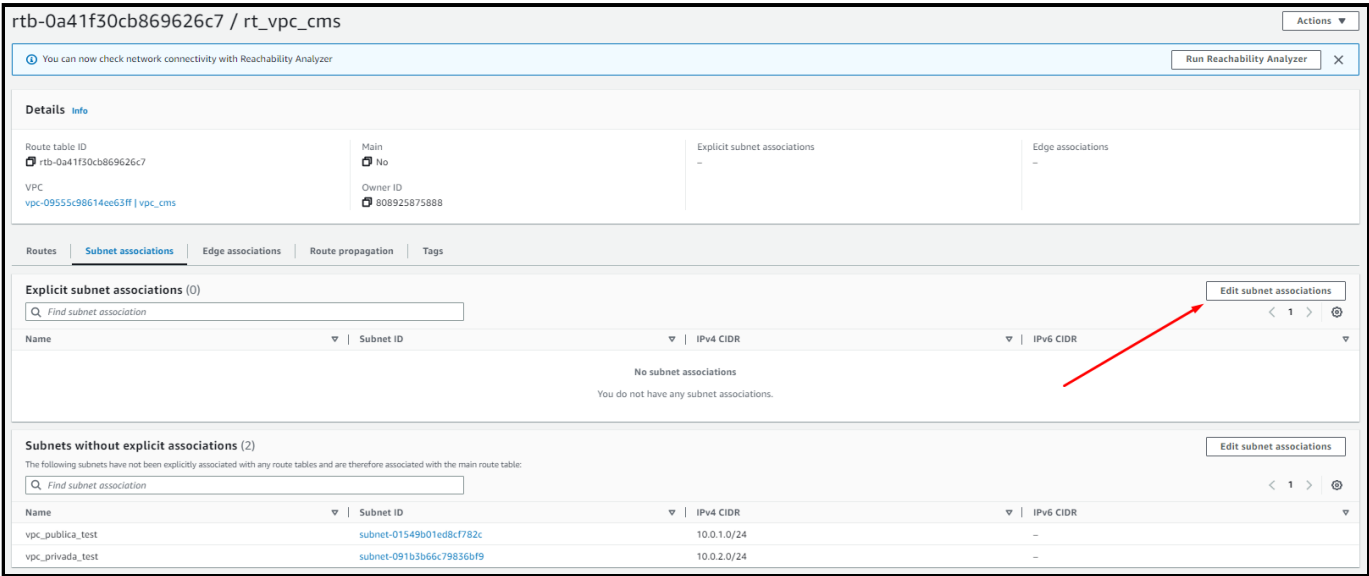
Route table ID rtb-0a41f30cb869626c7	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-09555c98614ee63ff vpc_cms	Owner ID 808925875888		

Subnet associations | Routes | Edge associations | Route propagation | Tags

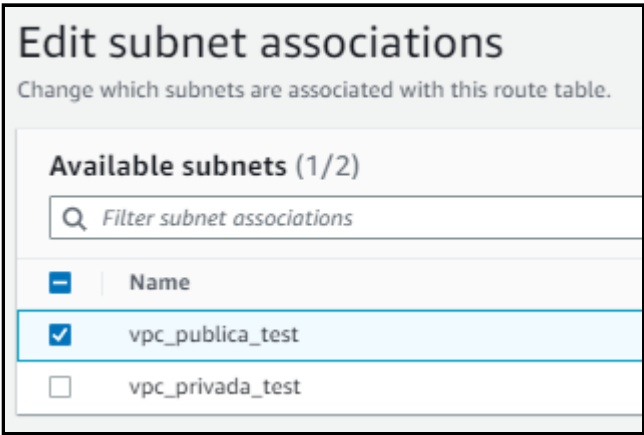
Routes (1)

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

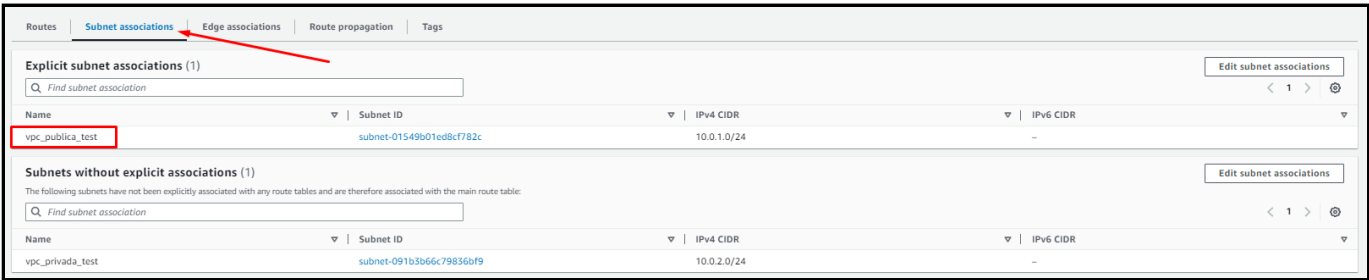
Vemos 2 cuadros llamados "Explicit subnet associations" (arriba) y "Subnets without explicit associations" (abajo). En el cuadro de arriba, clicamos en el botón "Edit subnet associations", para poder asociar la subred pública que creamos anteriormente a esta nueva tabla de enrutamiento.



Nos aparece una lista de las subredes que tenemos creadas. Simplemente seleccionamos la subred pública y hacemos clic en el botón de confirmación.

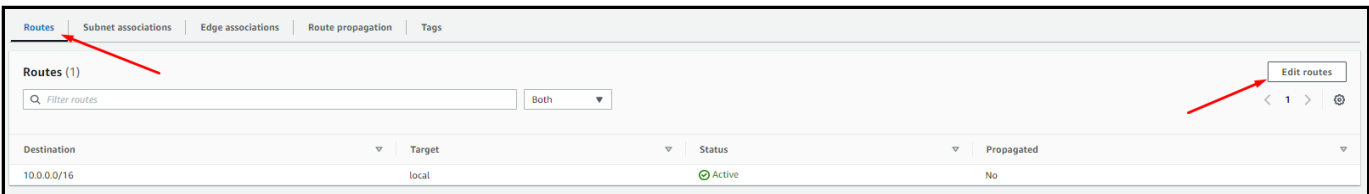


Una vez hecho, si volvemos a la pestaña "Subnet associations", podemos ver que en el cuadro de arriba ya aparece la subred que acabamos de asociar a esta tabla de enrutamiento.



Ahora cambiamos de pestaña a la principal, llamada "Routes".

En ella podemos ver otro cuadro con un botón en su esquina superior derecha que dice "Edit routes". Clicamos en él.



Lo que tenemos que hacer en este menú de ajustes es añadir una ruta nueva conocida como es la 0.0.0.0/0.

Esta ruta se encarga de que, en caso de que la dirección con la que se quiere establecer conexión no se encuentre entre el rango de IPs locales establecidas en la ruta justo encima (es decir, la comunicación no se va a establecer con un equipo local, sino con uno fuera de la red interna, un equipo de Internet), se establecerá comunicación con una IP cualquiera, que no pertenece a la red local.

Por lo tanto, en el primer recuadro, se establece el rango 0.0.0.0/0 y, en el segundo recuadro (el cual es un desplegable), debemos seleccionar la opción "Internet Gateway", la cual mostrará los gateways disponibles, entre los que estará el gateway que creamos anteriormente.

The image shows two screenshots from the AWS VPC console. The top screenshot shows the 'Target' dropdown menu with 'Internet Gateway' selected. The bottom screenshot shows the 'Destination' and 'Target' fields with '0.0.0.0/0' and 'igw-0441d250ad3b1f00' respectively.

Target

Q local X

Q

- Carrier Gateway
- Core Network
- Egress Only Internet Gateway
- Gateway Load Balancer Endpoint
- Instance
- Internet Gateway**
- local
- NAT Gateway
- Network Interface
- Outpost Local Gateway
- Peering Connection
- Transit Gateway
- Virtual Private Gateway

Destination

10.0.0.0/16

Q 0.0.0.0/0 X

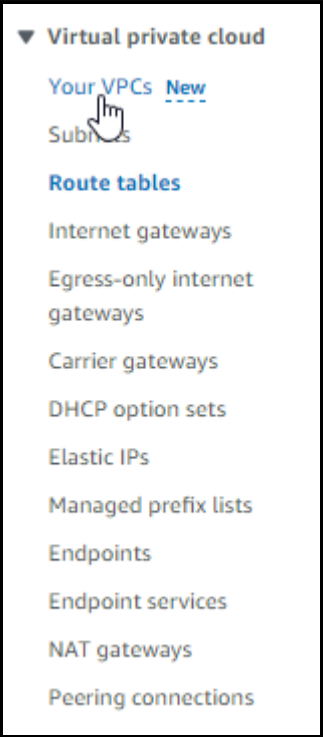
Target

Q local X

Q igw-0441d250ad3b1f00 X

Guardamos los cambios.

Para terminar con la creación de la VPC, volvemos al menú lateral izquierdo, a la opción llamada "Your VPCs".



Nos aparece una lista de las VPCs que tenemos disponibles. Hacemos clic en la que acabamos de terminar de crear.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table	Main network ACL	Tenancy	Default VPC
-	vpc-0319e0fe077aa36dc	Available	172.31.0.0/16	-	dopt-080e8bf907a7f4...	rtb-0cb03a7a8d4632994	acl-0dfb9ccfa64550851	Default	Yes
<input checked="" type="checkbox"/> vpc_cms	vpc-09555c98614ee63ff	Available	10.0.0.0/16	-	dopt-080e8bf907a7f4...	rtb-06b16fec18bd21985	acl-0160feb377067f4c3	Default	No

Dentro de ella podemos volver a ver el resumen de la VPC configurada al completo, donde ahora aparece la tabla de enrutamiento principal, entre otras cosas:

Details

VPC ID: vpc-09555c98614ee63ff

State: Available

DHCP option set: dopt-080e8bf907a7f43ac

IPv4 CIDR: 10.0.0.0/16

Main route table: rtb-06b16fec18bd21985

DNS hostnames: Disabled

DNS resolution: Enabled

Owner ID: 808925875888

Resource map

VPC: vpc_cms

Subnets (2): us-east-1a, vpc_publica_test, us-east-1b, vpc_privada_test

Route tables (2): rt_vpc_cms, rtb-06b16fec18bd21985

Network connections (1): gw_vpc_cms

2.b. Una vez creada la VPC, vamos a crear una instancia EC2 en la red pública.

Detalles de la instancia a crear:

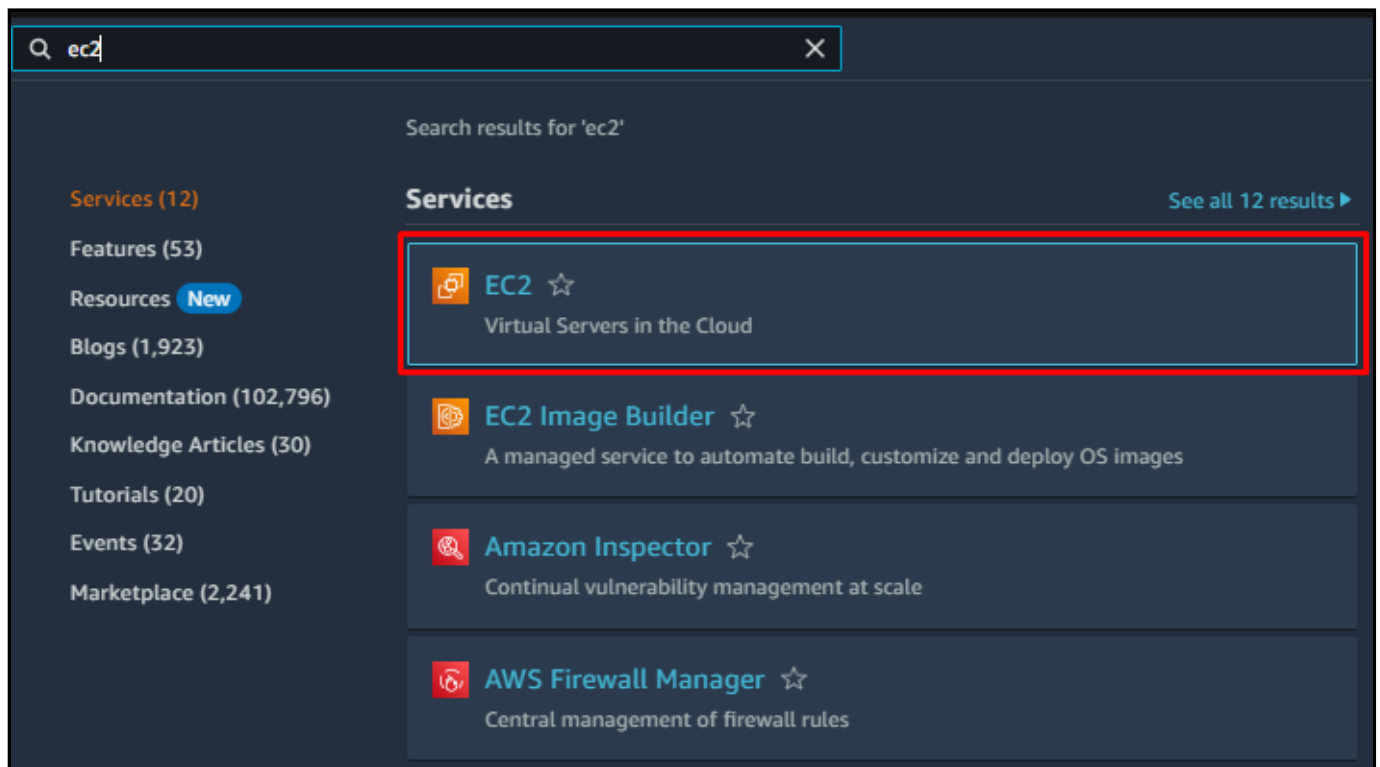
- Nombre: Ubuntu_WebServer

- **Capa gratuita:** instancia tipo "t2.micro", VPC: vpc_< tusiniciales >, subred: vpc_publica_test, IP local fija asignada: 10.0.1.10/24, grupo de seguridad: sg_ubuntu
- **Acceso mediante vockey con el usuario < tunombre >**

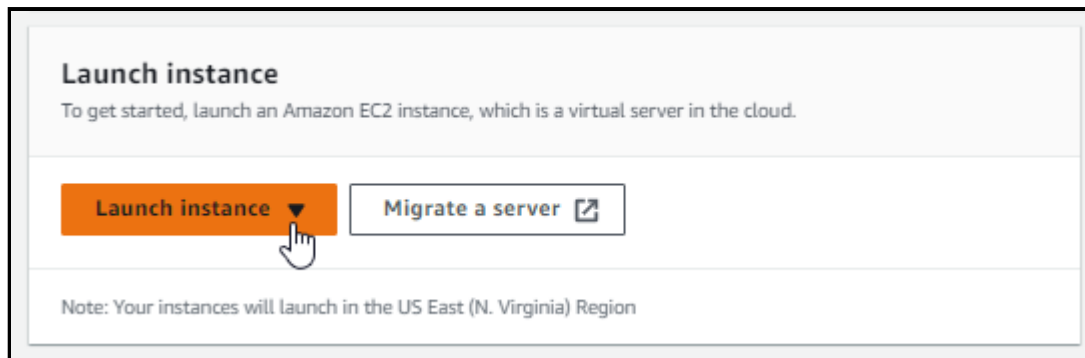
En este equipo se debe:

- **Crear una carpeta en el workdir (/home/user) con el nombre "miweb".**
- **Instalar Docker.** Añade al usuario < tunombre > en el grupo "docker" para poder lanzar comandos Docker.
- **Copiar el contenido de una página web estática que tengas creada usando el correspondiente comando scp desde tu equipo y usuario Ubuntu.**
- **Lanzar la instrucción "docker run", una vez tengamos el contenido web en "/home/user/miweb", para ejecutar un contenedor llamado "webserver" que ponga en contacto el directorio "/home/user/miweb" con el directorio de publicación por defecto de nginx. La imagen a usar será "nginx:1.23.3-alpine-slim". Comprueba que al visitar en un navegador "http://< ippublicaserver >" se visualiza el contenido de tu web.**
- **Demostrar que, si se modifica en el equipo local la página web y se vuelve a transferir con scp este contenido a "/home/user/miweb", al visitar en cualquier navegador la página web "http://< ippublicaserver >" se visualizan los cambios.**

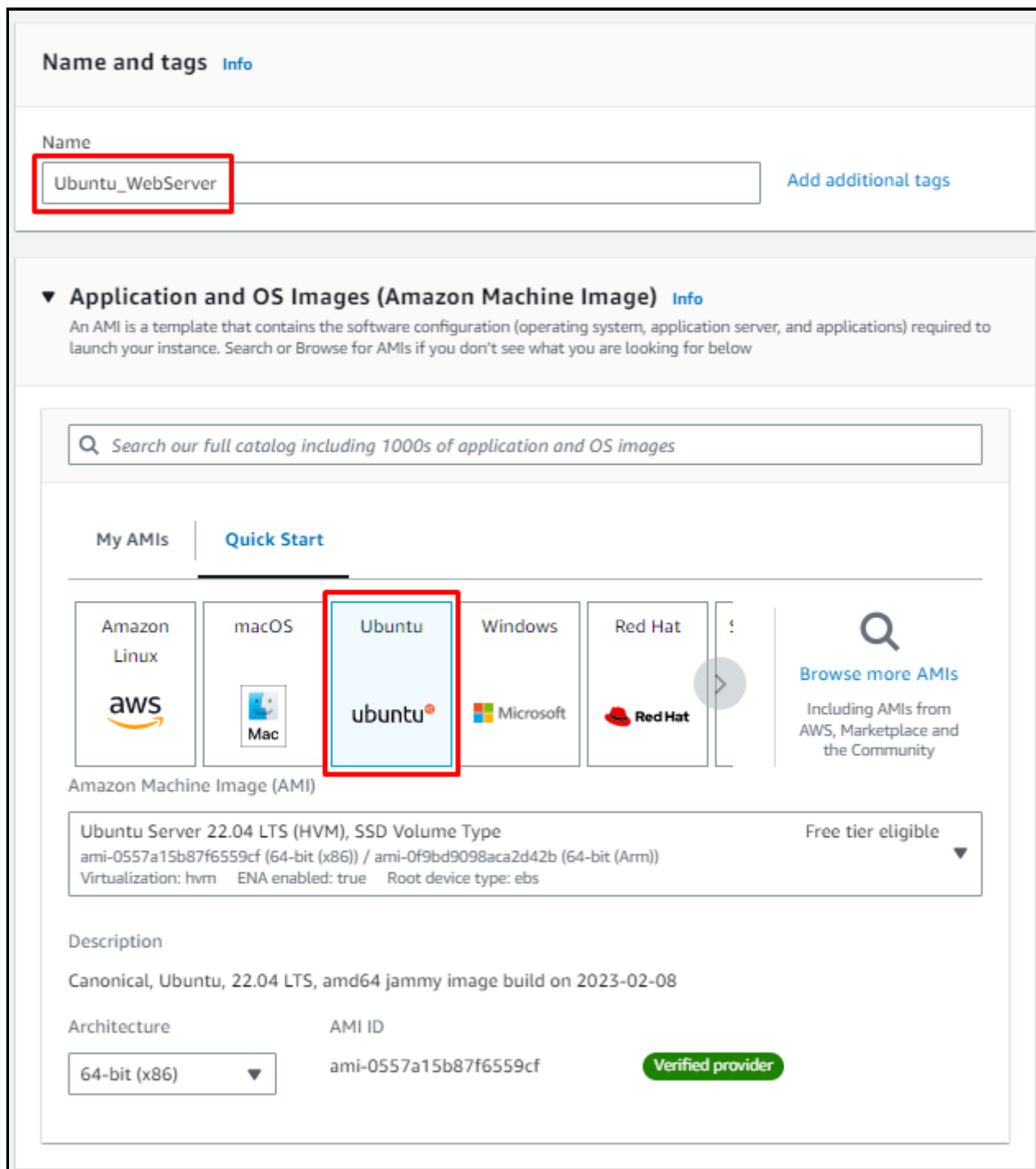
El comienzo es similar al ejercicio anterior: buscamos "ec2" en la barra de búsqueda del panel de control y hacemos clic en el menú.



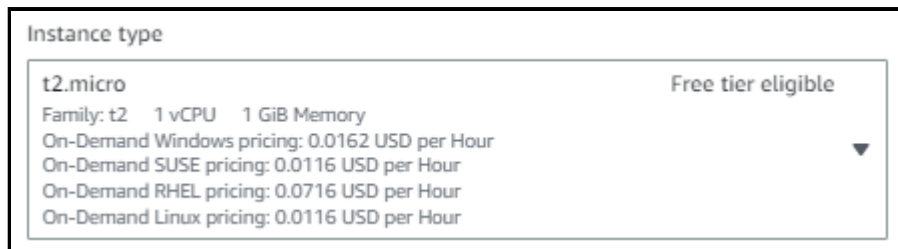
Creamos una nueva instancia:



Establecemos el nombre de la instancia y elegimos la imagen de sistema operativo que se instalará en ella.



El tipo de instancia lo dejamos con la opción predeterminada:



Instance type

t2.micro Free tier eligible

Family: t2 1 vCPU 1 GiB Memory

On-Demand Windows pricing: 0.0162 USD per Hour

On-Demand SUSE pricing: 0.0116 USD per Hour

On-Demand RHEL pricing: 0.0716 USD per Hour

On-Demand Linux pricing: 0.0116 USD per Hour

Seleccionamos la vockey en el siguiente desplegable, para indicar que el acceso a esta instancia se realizará mediante este método.

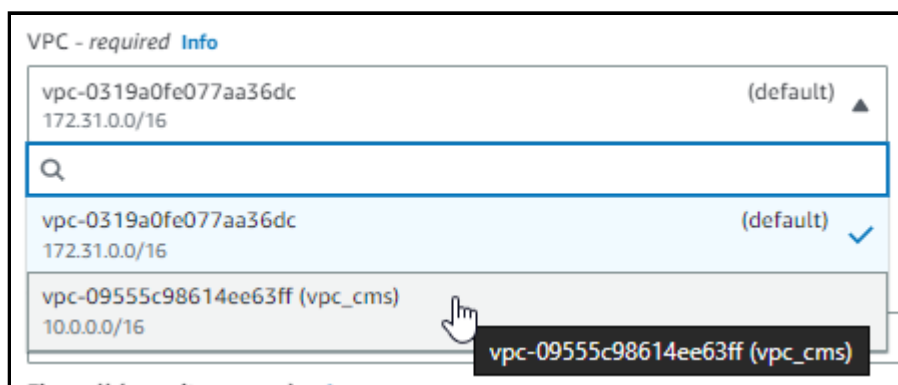


Key pair name - required

vockey

El siguiente cuadro se refiere a la configuración de la red de la nueva instancia. Debemos hacer clic en el botón de edición que aparece en la esquina superior derecha de este cuadro para cambiar algunos ajustes.

Lo primero es cambiar la VPC que utilizará en el primer desplegable que aparece:



VPC - required Info

vpc-0319a0fe077aa36dc (default)

172.31.0.0/16

Q

vpc-0319a0fe077aa36dc (default) ✓

172.31.0.0/16

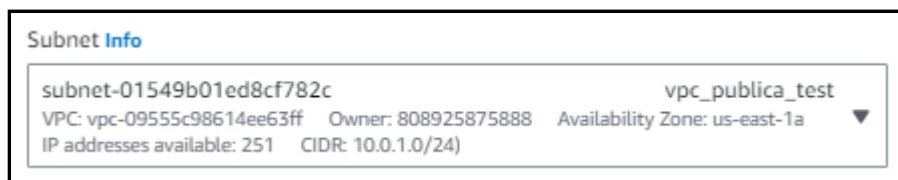
vpc-09555c98614ee63ff (vpc_cms)

10.0.0.0/16

vpc-09555c98614ee63ff (vpc_cms)

En el siguiente desplegable que aparece se selecciona la subred a la que se conecta la instancia (recordemos que tenemos una subred pública y otra privada).

Tenemos que asegurarnos de que la subred que está seleccionada en este desplegable es la pública, tal y como especifica el enunciado de este ejercicio.



Subnet Info

subnet-01549b01ed8cf782c vpc_publica_test

VPC: vpc-09555c98614ee63ff Owner: 808925875888 Availability Zone: us-east-1a

IP addresses available: 251 CIDR: 10.0.1.0/24

También hay que habilitar la siguiente opción, que permite que la máquina obtenga una IP pública:



Auto-assign public IP Info

Enable

El siguiente ajuste sirve para crear un grupo de seguridad que, como especifica el enunciado de este ejercicio, debe ser "sg_ubuntu".

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group

☐ Select existing security group

Security group name - *required*

sg_ubuntu

Justo después aparece la opción de crear reglas para el grupo de seguridad, las cuales se deben dejar tal cual vienen de forma predeterminada, ya que habilita el puerto para el protocolo ssh.

Por último en este cuadro de configuración de la red de la instancia, tendremos que abrir el último desplegable para cambiar un ajuste extra.

Inbound security groups rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Remove

Type [Info](#)

Protocol [Info](#)

Port range [Info](#)

ssh ▼

TCP

22

Source type [Info](#)

Source [Info](#)

Description - optional [Info](#)

Anywhere ▼

Q Add CIDR, prefix list or security

0.0.0.0/0 X

e.g. SSH for admin desktop

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

X

Add security group rule

▶ Advanced network configuration

Nada más abrirlo vemos que aparece una interfaz ya creada. El único ajuste que debemos tocar aquí es la IP primaria fija que se le asignará a la instancia, la cual es la 10.0.1.10, según especifica el enunciado de este ejercicio.

Network interface 1

Device index [Info](#)

Network interface [Info](#)

Description [Info](#)

0

New interface ▼

Subnet [Info](#)

Security groups [Info](#)

Primary IP [Info](#)

subnet-01549b01ed8cf782c

New security group

10.0.1.10

IP addresses available: 251