

AWS VPC EX1

Preguntas que hemos de saber responder:

Dada la IPv4 172.31.15.6/20...

- ¿A qué red pertenece? ¿Cuál es su máscara?
 - ¿Cuál es el nº de hosts que puede soportar?
 - ¿Cuál es la primera IP asignable?
 - ¿Cuál es la dirección de broadcast?
 - ¿Cuál sería la última IP asignable?
-

3. Vamos a crear un 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 una gateway propio creado ad-hoc para el VPC.

El rango de direcciones del VPC será el CIDR 10.0.0.0/16 y cada una de las dos subredes pública y privada tendrán los CIDR 10.0.1.0/24 y 10.0.2.0/24 respectivamente.

Las subredes públicas se llamarán "publica_vpc" y "privada_vpc".

Se creará una tabla de enrutamiento que permita salida a Internet a la subred pública, pero no a la privada.

En la barra de búsqueda de AWS, buscamos "VPC" y entramos al panel de control de dicha herramienta. Aquí se nos presenta la posibilidad de crear un nuevo VPC:

[Create VPC](#) [Launch EC2 Instances](#)

Note: Your Instances will launch in the US East region.

Resources by Region [Refresh Resources](#)

You are using the following Amazon VPC resources

VPCs See all regions	US East 1	NAT Gateways See all regions	US East 0
Subnets See all regions	US East 6	VPC Peering Connections See all regions	US East 0
Route Tables See all regions	US East 1	Network ACLs See all regions	US East 1
Internet Gateways See all regions	US East 1	Security Groups See all regions	US East 3
Egress-only Internet Gateways See all regions	US East 0	Customer Gateways See all regions	US East 0
DHCP option sets See all regions	US East 1	Virtual Private Gateways See all regions	US East 0
Elastic IPs See all regions	US East 0	Site-to-Site VPN Connections See all regions	US East 0
Endpoints See all regions	US East 0	Running Instances See all regions	US East 2
Endpoint Services See all regions	US East 0		

Elegimos la opción "VPC only", ya que por ahora solo queremos crear una VPC básica. Le asignamos un nombre reconocible (en mi caso, "vpc_mis-iniciales"), establecemos el CIDR que nos pide el ejercicio y añadimos una etiqueta "Ejercicio" con valor "1daw" (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).

VPC > Your VPCs > Create VPC

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

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

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input

☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

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](#)

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

X

Value - optional

X

Remove

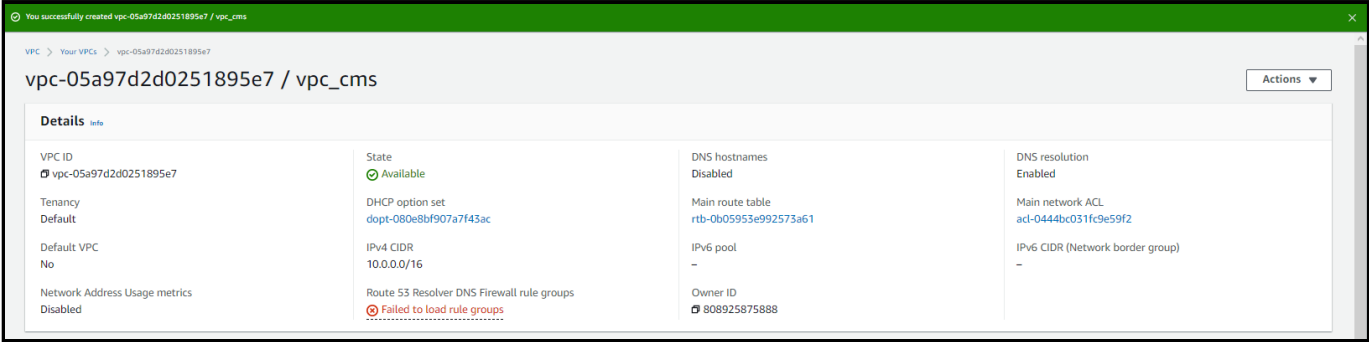
X

X

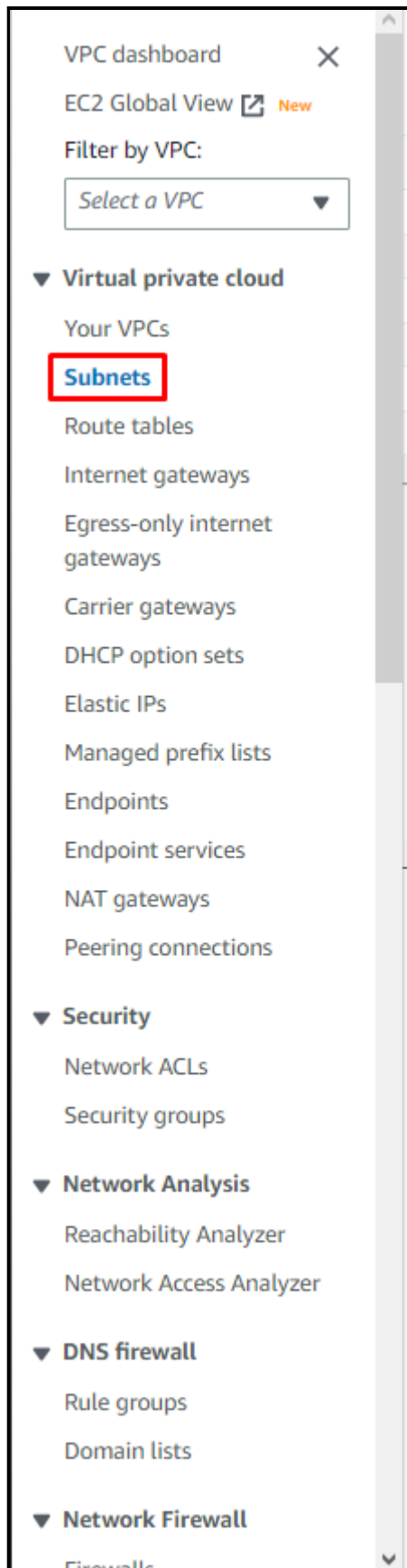
Remove

Add new tag

Ya se ha creado el nuevo VPC.



Ahora nos dirigimos al menú lateral a la izquierda de la página y entramos en la opción "Subnets/Subredes".



Elegimos la opción para crear una nueva subred que aparece en el panel de control de las subredes. Elegimos el VPC al que se le va a crear una subred en el desplegable que aparece.

Create subnet

Info

VPC

VPC ID

Create subnets in this VPC.

vpc-05a97d2d0251895e7 (vpc_cms)

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Además de esto, le asignamos un nombre reconocible a la subred ("vpc_publica", en este caso), la zona de disponibilidad y el rango de IP de la misma.

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

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

Remove

Ejercicio

1daw

Remove

Add new tag

You can add 48 more tags.

Remove

Add new subnet

Subred creada con éxito.

You have successfully created 1 subnet: subnet-03a9940486f385dc6

Subnets (1)

Info

Filter subnets

Subnet ID: subnet-03a9940486f385dc6

Clear filters

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	
<input type="checkbox"/>	vpc_publica	subnet-03a9940486f385dc6	Available	vpc-05a97d2d0251895e7 vpc_cms	10.0.1.0/24	-	251	ut

Hacemos lo mismo para la subred privada que también tenemos que crear y le asignamos el rango de IP correspondiente, distinto de la anterior subred.

VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID

Create subnets in this VPC.

vpc-05a97d2d0251895e7 (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

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

10.0.2.0/24

Tags - optional

Key

Value - optional

Name

vpc_privada

Remove

Ejercicio

1daw

Remove

Add new tag

You can add 48 more tags.

Remove

Add new subnet

Aquí se pueden identificar sin problemas las dos subredes recién creadas:

You have successfully created 1 subnet: subnet-0a94b53b3e050b1f6

Subnets (8) Info

Filter subnets

Actions

Create subnet

	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	
<input type="checkbox"/>	-	subnet-076b10a48df77bbd	Available	vpc-0319a0fe077aa36dc	172.31.16.0/20	-	4091	ut
<input type="checkbox"/>	-	subnet-0c7bc6351c1c9572e	Available	vpc-0319a0fe077aa36dc	172.31.80.0/20	-	4091	ut
<input type="checkbox"/>	-	subnet-03aa635a632f4d2f6	Available	vpc-0319a0fe077aa36dc	172.31.0.0/20	-	4090	ut
<input type="checkbox"/>	vpc_publica	subnet-03a9940486f385dc6	Available	vpc-05a97d2d0251895e7 vpc_cms	10.0.1.0/24	-	251	ut
<input type="checkbox"/>	-	subnet-0d0daac0ef80688fc	Available	vpc-0319a0fe077aa36dc	172.31.64.0/20	-	4091	ut
<input type="checkbox"/>	-	subnet-07d623df8aa616d95	Available	vpc-0319a0fe077aa36dc	172.31.48.0/20	-	4090	ut
<input type="checkbox"/>	-	subnet-02bcf3133916a23d7	Available	vpc-0319a0fe077aa36dc	172.31.32.0/20	-	4091	ut
<input type="checkbox"/>	vpc_privada	subnet-0a94b53b3e050b1f6	Available	vpc-05a97d2d0251895e7 vpc_cms	10.0.2.0/24	-	251	ut

Volvemos al menú lateral izquierdo, esta vez para entrar en "Internet gateways/Puertas de enlace a Internet".

7 / 19



Debemos crear una puerta de enlace nueva para poder salir a Internet, no solo tener conexión interna entre equipos.

The screenshot shows the 'Create internet gateway' page in the AWS Management Console. The breadcrumb navigation is 'VPC > Internet gateways > Create internet gateway'. The page title is 'Create internet gateway' with an 'Info' link. A description states: '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.'

Internet gateway settings

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

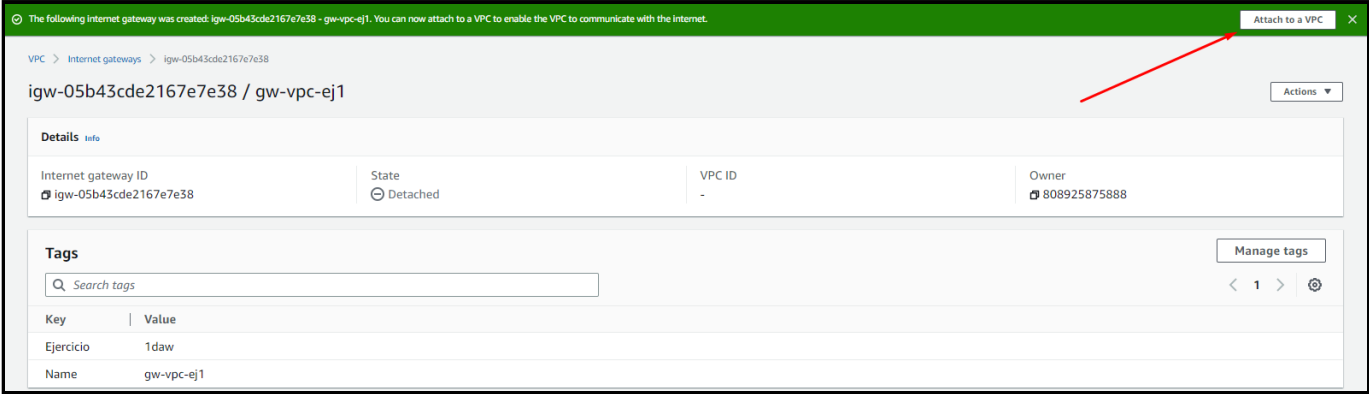
Input field: gw-vpc-ej1

Tags - optional
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	
Q Name	Q gw-vpc-ej1	Remove
Q Ejercicio	Q 1daw	Remove

Add new tag
You can add 48 more tags.

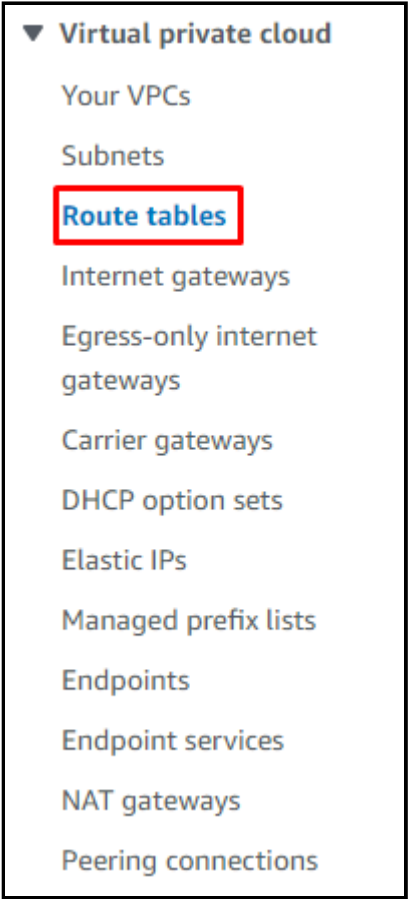
Una vez creada, hacemos clic en la opción superior derecha para agregar este gateway a nuestro VPC.



Simplemente seleccionamos el VPC creado anteriormente en el desplegable.



De nuevo vamos al menú de la izquierda, a la opción "Route tables/Tablas de enrutamiento".



Creamos una nueva tabla de enrutamiento:

Route tables (2) Info

Actions

Create route table

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC	Owner ID
<input type="checkbox"/>	-	rtb-0cd03a7a8d4632994	-	-	Yes	vpc-0319a0fe077aa36dc	808925875888
<input type="checkbox"/>	-	rtb-0b05953e992573a61	-	-	Yes	vpc-05a97d2d0251895e7 vpc_cms	808925875888

Le asignamos un nombre y un VPC donde se va a usar.

VPC > Route tables > Create route table

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional

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

rt-vpc-publica

VPC

The VPC to use for this route table.

vpc-05a97d2d0251895e7 (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 and filter your resources or track your AWS costs.

Key

Value - optional

Q Name

X

Q rt-vpc-publica

X

Remove

Q Ejercicio

X

Q 1daw

X

Remove

Add new tag

You can add 48 more tags.

Una vez creada, vamos al submenú "Subnet associations/Asociaciones de subredes".

Route table rtb-034ae07f00bc9028f / rt-vpc-publica was created successfully.

VPC > Route tables > rtb-034ae07f00bc9028f

rtb-034ae07f00bc9028f / rt-vpc-publica

Actions

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Details

Route table ID

rtb-034ae07f00bc9028f

Main

No

Explicit subnet associations

-

Edge associations

-

VPC

vpc-05a97d2d0251895e7 | vpc_cms

Owner ID

808925875888

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (1)

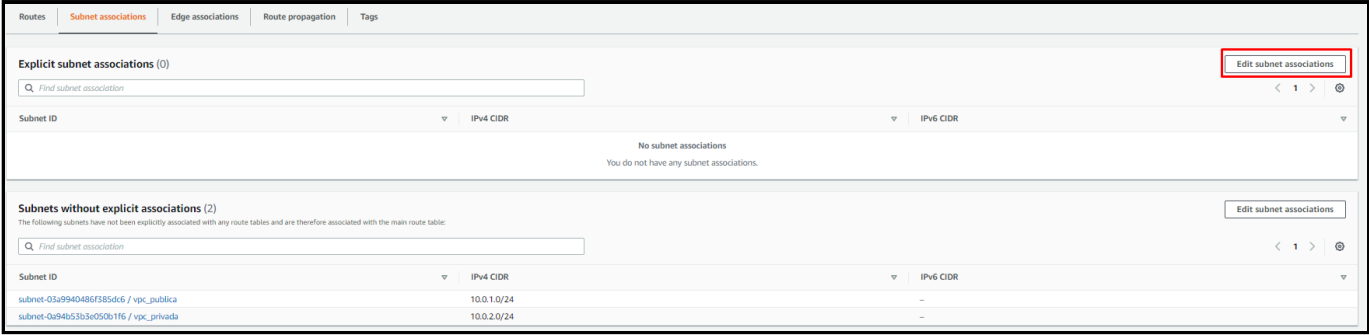
Filter routes

Both

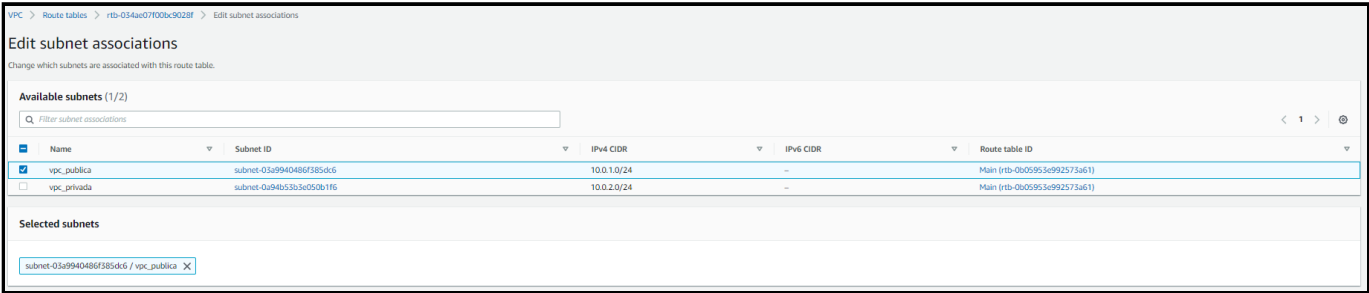
Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

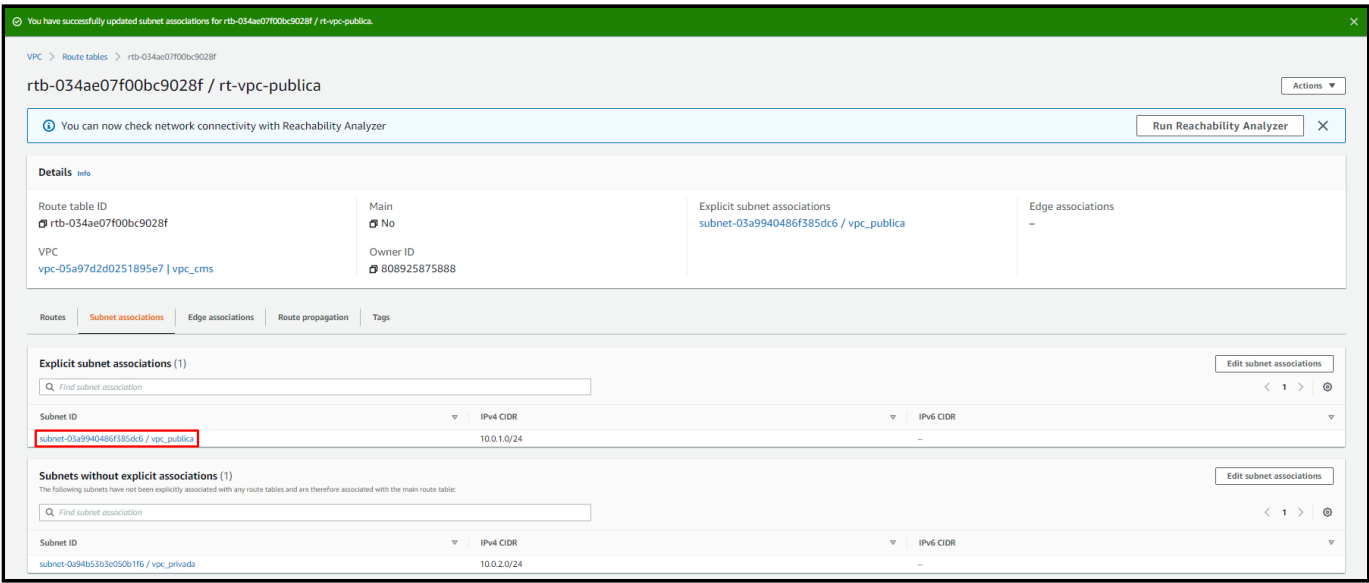
Editamos las asociaciones...



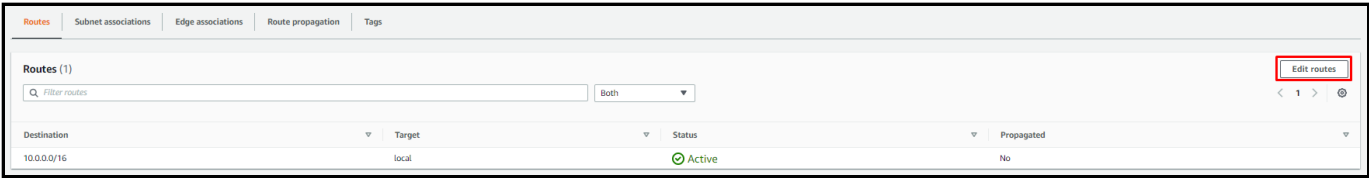
Seleccionamos la subred que debe tener acceso a dicha tabla de enrutamiento.



Y podemos ver que se ha añadido correctamente dicha subred:



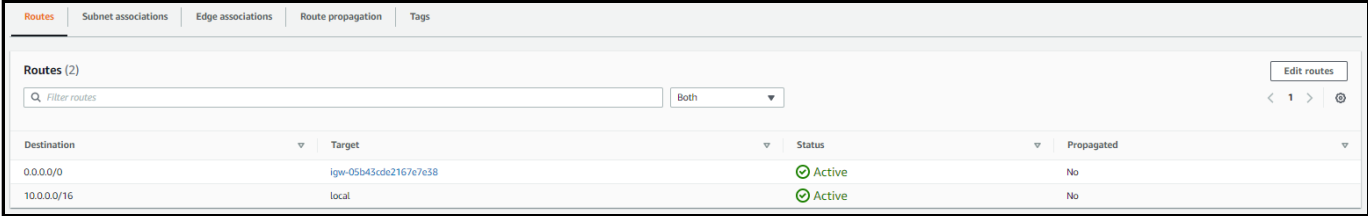
Entramos en el submenú "Routes/Rutas".



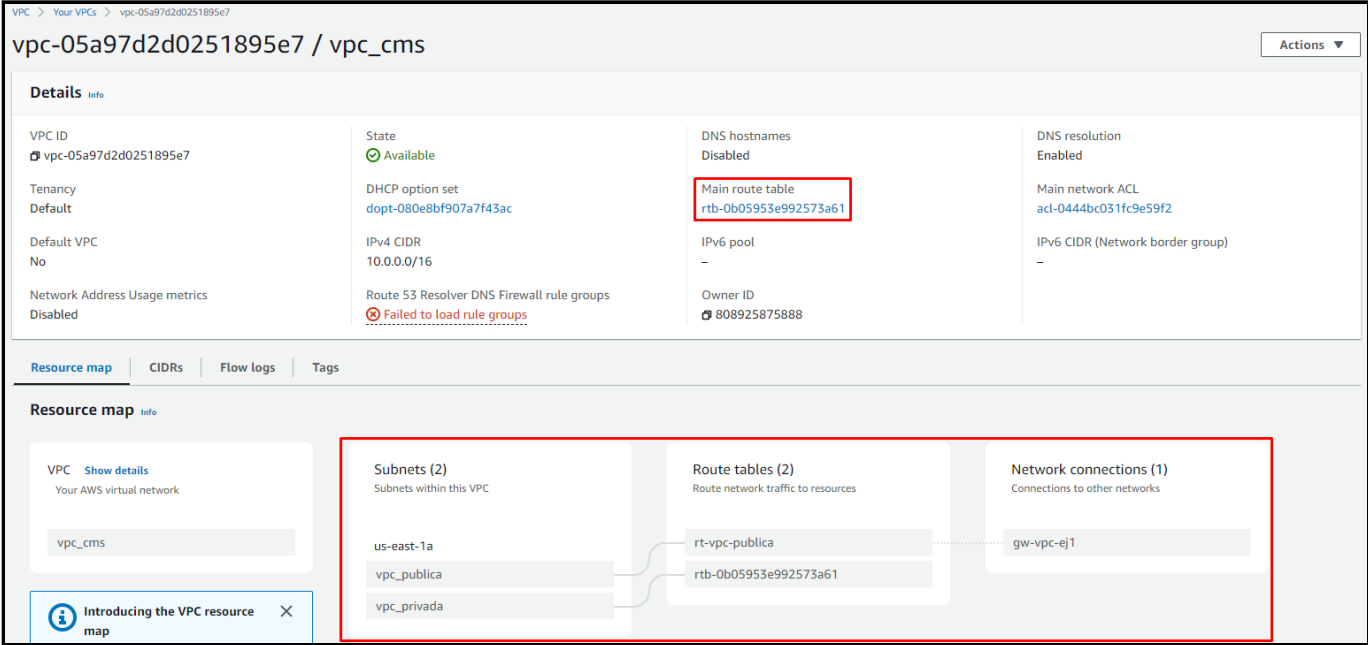
Establecemos una ruta conocida como es la "0.0.0.0/0", la cual se encarga de que, en caso de no encontrarse entre la lista de IPs locales establecida en la ruta justo encima (es decir, la comunicación no se va a establecer con un equipo local, sino con uno de fuera de la red interna, un equipo de Internet), se establecerá comunicación con una IP cualquiera, que no pertenece a la red local.



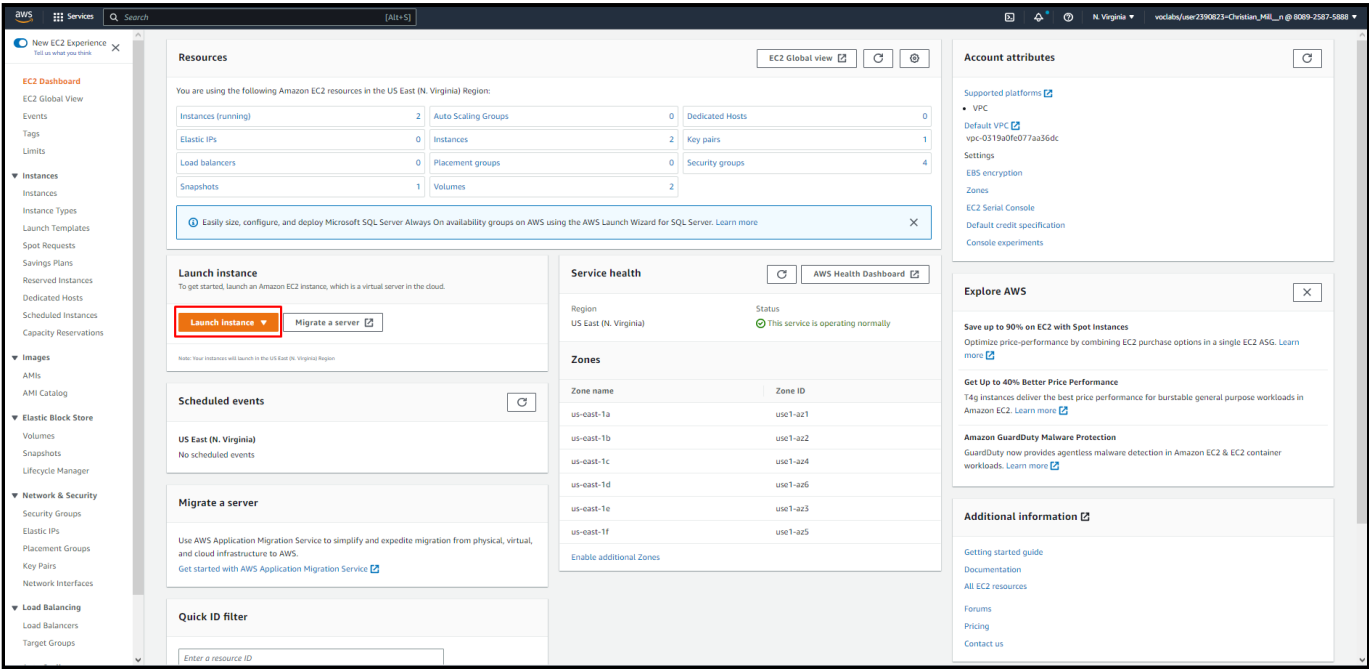
Podemos ver como se ha establecido la nueva ruta con éxito:



Viendo la vista general del VPC por ahora, se puede observar la nueva tabla de enrutamiento vinculada a este VPC:



Por último, solo queda crear una nueva instancia que utilice el VPC que acabamos de crear.



Le asignamos un nombre y un sistema operativo de Windows.

EC2 > Instances > Launch an instance

Launch an instance

Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Info

Name

windows-server

Add additional tags

▼ Application and OS Images (Amazon Machine Image)

Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Q Search our full catalog including 1000s of application and OS images

Recents

My AMIs

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

⋮

➤

Q

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Microsoft Windows Server 2022 Base

Free tier eligible

ami-0c2b0d3fb02824d92 (64-bit (x86))

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Microsoft Windows Server 2022 Full Locale English AMI provided by Amazon

Architecture

AMI ID

64-bit (x86)

ami-0c2b0d3fb02824d92

Verified provider

Le asignamos el par de claves "vockey" que ya hemos utilizado anteriormente con máquinas de Linux (sirve tanto para Linux como para Windows, como para otros S.O., ya que se vincula a la cuenta de AWS).

14 / 19

▼ Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*
 [Create new key pair](#)

For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.

Creamos un grupo de seguridad donde se asigna el VPC que hemos creado, la subred (en este caso la pública), se habilita la asignación de IPs públicas automática y se establece un nombre para el nuevo grupo de seguridad.

▼ Network settings Info

VPC - *required* Info

10.0.0.0/16 [Create new VPC](#)

Subnet Info

VPC: vpc-05a97d2d0251895e7 Owner: 808925875888
Availability Zone: us-east-1a IP addresses available: 251 CIDR: 10.0.1.0/24 [Create new subnet](#)

Auto-assign public IP Info

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*

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&{}!\$*

Description - *required* Info

También debemos crear unas reglas para el grupo de seguridad que permitan utilizar los puertos y protocolos necesarios para compartir ficheros, realizar pings, etc.

Inbound security groups rules

▼ Security group rule 1 (TCP, 3389, 0.0.0.0/0)

Remove

Type [Info](#)

Protocol [Info](#)

Port range [Info](#)

rdp

TCP

3389

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

▼ Security group rule 2 (ICMP, All, 0.0.0.0/0)

Remove

Type [Info](#)

Protocol [Info](#)

Port range [Info](#)

All ICMP - IPv4

ICMP

All

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

▼ Security group rule 3 (TCP, 445, 0.0.0.0/0)

Remove

Type [Info](#)

Protocol [Info](#)

Port range [Info](#)

SMB

TCP

445

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

▼ Advanced network configuration

Network interface 1

Device index [Info](#)

Network interface [Info](#)

Description [Info](#)

0

New interface

Subnet [Info](#)

Security groups [Info](#)

Primary IP [Info](#)

subnet-03a9940486f385dc6

New security group

10.0.1.10

IP addresses available: 251

Secondary IP [Info](#)

IPv6 IPs [Info](#)

IPv4 Prefixes [Info](#)

Select

Select

Select

The selected instance type does not support IPv4 prefixes.

IPv6 Prefixes [Info](#)

Delete on termination [Info](#)

Elastic Fabric Adapter [Info](#)

Select

Select

☐ Enable

EFA is only compatible with certain instance types.

The selected instance type does not support IPv6 prefixes.

Network card index [Info](#)

Select

▼

The selected instance type does not support multiple network cards.

Una vez se inicializa la máquina...

EC2 > Instances > Launch an instance

✓ Success

Successfully initiated launch of instance (i-0a06fcaedbf6d935b)

▼ Launch log

Initializing requests

Succeeded

Creating security groups

Succeeded

Creating security group rules

Succeeded

Launch initiation

Succeeded

... vemos como la IP fija que se le ha establecido en la configuración de la instancia se ha realizado con éxito:

EC2 > Instances > i-0a06fcaedbf6d935b

Instance summary for i-0a06fcaedbf6d935b (windows-server) [Info](#)

🔄

Connect

Instance state ▼

Actions ▼

Instance ID

i-0a06fcaedbf6d935b (windows-server)

IPv6 address

—

Hostname type

IP name: ip-10-0-1-10.ec2.internal

Answer private resource DNS name

IPv4 (A)

Auto-assigned IP address

52.3.231.34 (Public IP)

IAM Role

—

Public IPv4 address

52.3.231.34 | [open address](#)

Instance state

Running

Private IP DNS name (IPv4 only)

ip-10-0-1-10.ec2.internal

Instance type

t2.micro

VPC ID

vpc-05a97d2d0251895c7 (vpc_cms) | [🔗](#)

Subnet ID

subnet-03a9940486f385dc6 (vpc_public) | [🔗](#)

Private IPv4 addresses

10.0.1.10

Public IPv4 DNS

—

Elastic IP addresses

—

AWS Compute Optimizer finding

[Opt-in to AWS Compute Optimizer for recommendations. | Learn more](#)

Auto Scaling Group name

—

Utilizamos la opción "Connect/Conectar" que aparece en la barra de menú superior de la instancia.

EC2 > Instances > i-0a06fcaedbf6d935b

Instance summary for i-0a06fcaedbf6d935b (windows-server) [Info](#)

🔄

Connect

Instance state ▼

Actions ▼

Abajo, en el apartado "Password/Contraseña", debemos seleccionar el archivo "vockey.pem/labuser.pem" que debemos tener descargado debido a que lo hemos utilizado anteriormente con máquinas de Linux en AWS. Este es el fichero que genera la clave para la conexión por Escritorio Remoto hacia la máquina nueva. Copiamos la contraseña/el token que este archivo genera.

EC2 > Instances > i-0a06fcaedbf6d935b > Connect to instance


Connect to instance [Info](#)

Connect to your instance i-0a06fcaedbf6d935b (windows-server) using any of these options

Session Manager


RDP client

EC2 serial console


Instance ID
 **i-0a06fcaedbf6d935b** (windows-server)

Connection Type




☒ **Connect using RDP client**
Download a file to use with your RDP client and retrieve your password.


☐ **Connect using Fleet Manager**
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#) 

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

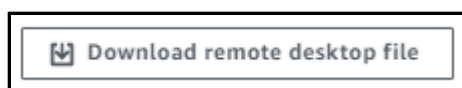
 **Download remote desktop file**

When prompted, connect to your instance using the following details:

Public IP	User name
 52.3.231.34	 Administrator
Password	
 Qb=)lOr3SV%LtYSQzEUHN?juPx EJcywy	

 If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

Por último, seleccionamos la opción de descarga del archivo que permite la conexión a esta nueva instancia utilizando esta contraseña.



Introducimos las credenciales (la contraseña/el token que acabamos de copiar).



Y ya tenemos conexión directa por Escritorio Remoto hacia esta nueva instancia que pertenece a una red que acabamos de crear.

