

## Práctica 10.1

### Crear una VPC y Subredes en AWS Services

#### 1. Objetivos

- 1.1. Conocer los servicios y conceptos principales del Cloud Computing
- 1.2. Crear redes de ordenadores en la Nube
- 1.3. Comprender los conceptos de funcionamiento y seguridad de las VPC.
- 1.4. Crear una VPC y crear subredes
- 1.5. Configurar un grupo de seguridad para asegurar los recursos

#### 2. Materiales

- 2.1. Guión de la práctica
- 2.2. Cuenta AWS Educate e AWS Services

#### 3. Recursos

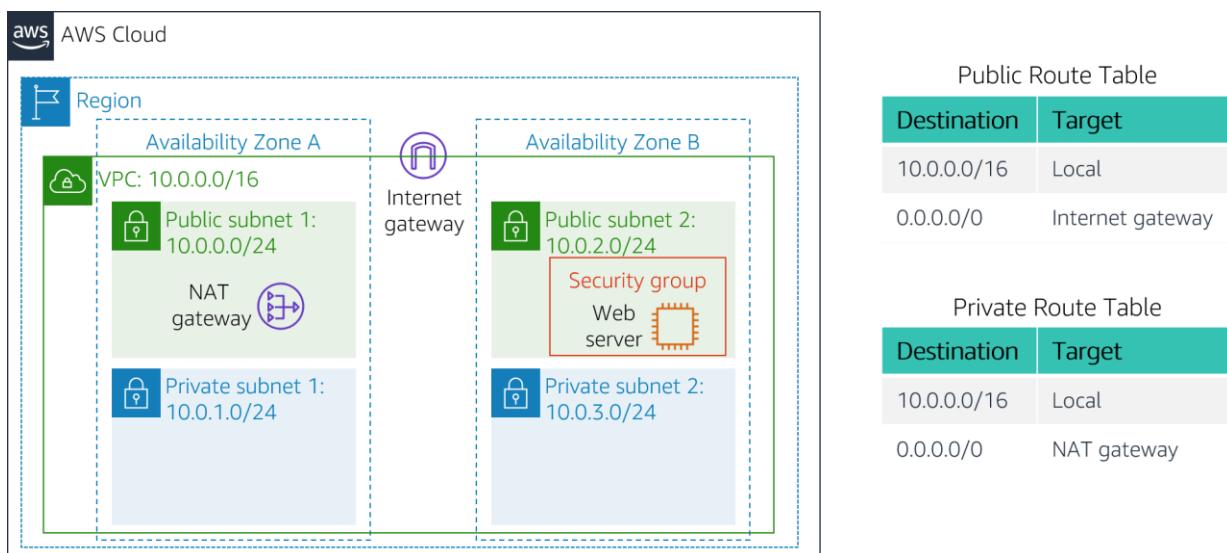
- 3.1. [AWS. Introducción al Cloud Computing](#)
- 3.2. [Video: Creación de VPC con 1 subred pública y 1 privada](#)
- 3.3. [Video: Salida a Internet con NAT Gateway para redes privadas](#)

En esta práctica, usaremos el servicio Amazon Virtual Private Cloud (VPC) para crear una Red Privada en la Nube (Virtual Private Cloud o VPC) y agregar componentes adicionales para producir una red personalizada. También crearemos grupos de seguridad para conocer el concepto de los mismos y cómo nos ayudan a proteger los recursos.

**Amazon Virtual Private Cloud (Amazon VPC)** permite iniciar recursos de Amazon Web Services (AWS) en una red virtual. Esta red virtual se asemeja mucho a una red tradicional que operaría en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS. Podemos crear un VPC que abarque varias zonas de disponibilidad.

## Escenario a construir

En este laboratorio se construye la siguiente infraestructura:



Vamos a crear una VPC (Red Privada) con 4 subredes, 2 públicas y 2 privadas, 2 de ellas en una zona de disponibilidad y otras 2 en otra zona de disponibilidad.

Una vez hecho esto crearemos un par de instancias de sistemas linux para probar la configuración creada y probar el acceso a las mismas desde el exterior y la salida a internet desde las propias instancias tanto en la subred privada como en la subred públicas.

### Tarea 1. Crear la VPC

En esta tarea, no vamos a utilizar el asistente, de esta forma nos permitirá comprender mejor los pasos a seguir.

Una **puerta de enlace a Internet (IGW)** es un componente VPC que permite la comunicación entre instancias de la VPC e Internet.

Un **NAT gateway** es un componente VPC que permite obtener acceso a internet desde redes privadas, como funcionalidad principal.

La idea es que la subred pública sea accesible desde internet y la privada no, lo que nos permitirá tener nuestras máquinas en una zona segura, fuera de los peligros de internet.

Después de crear un VPC, vamos a agregar **subredes**. Cada subred reside completamente dentro de una Zona de Disponibilidad y no puede abarcar zonas. Si el tráfico de una subred se enruta a una puerta de enlace de Internet, la subred se conoce como *subred pública*. Si una subred no tiene una ruta a la puerta de enlace de Internet, la subred se conoce como *subred privada*.

En la **consola de administración de AWS**, en el menú **Servicios**, haga clic en **VPC**.

1. Haga clic en el menú lateral en “Your VPCs”
2. En el panel de navegación izquierdo, haga clic en **VPC con subredes públicas y privadas** (la segunda opción).
3. Haga clic en **Seleccionar** y luego configure:
  - **Nombre VPC:** WSRV\_VPC
  - **IPv4 CIDR block:** 10.0.0.0/16
4. Damos a crear, y ya tenemos creada nueva VPC.
5. Ahora creamos 2 subredes, una privada y otra pública.
6. En el menú lateral nos vamos a opción “Subnets” y click en “Create Subnet”.
  - **VPC ID:** Seleccionamos la vpc que creamos en el paso anterior.
  - **Nombre:** pri\_subnet
  - **Zona de disponibilidad:** La primera que nos aparece
  - **IPv4 CIDR block:** 10.0.1.0/24
7. Para finalizar le damos al botón “Create”.
8. Ahora creamos la subnet pública, lo hacemos de la misma manera:
  - **VPC ID:** Seleccionamos la vpc que creamos en el paso anterior.
  - **Nombre:** pub\_subnet
  - **Zona de disponibilidad:** La primera que nos aparece
  - **IPv4 CIDR block:** 10.0.2.0/24
9. Y la creamos, pulsando el botón “Create”.
10. Ya tenemos creada la VPC y 2 subredes dentro de esta VPC.
11. Ahora vamos a configurar para que la subred pública tenga salida a internet, para ello necesitamos crear un Internet Gateway, además de indicar a la subred que podamos auto-asignar IPs públicas, es decir, que se le pueda asignar una IP pública a esta subred.
12. Para ello, en Subnets (menú), selecciono la subred pública “pub\_subnet1” y en el clic en la opción “Modfy auto-assign IP settings” dentro del menú desplegable situado en el botón “Actions.”

En la pantalla siguiente, simplemente activo el check “Enable auto-assign public IPv4 address”
13. Ahora vamos a crear un Internet Gateway, para que la subred pública tenga salida a internet.

Desde el menú lateral, opción “Internet Gateways” y en la pantalla de configuración, le asigno el nombre “IGW-1”.

Este componente vemos que en el estado aparece “detached” indicando que no está adjunto o agregado a ninguna VPC. Para que funcione es necesario asignarlo a nuestra VPC.

Para hacerlo, en el menú “Actions” elegimos la opción “Attach to VPC”.

Ahora el VPC puede utilizar el Internet Gateway, pero aún ninguna subred lo utiliza, por lo que seguimos sin tener acceso a internet de forma real.

14. Ahora debemos crear las **tablas de enrutamiento**, que permitan enrutar el tráfico hacia y desde la opción “Route tables” desde el menú lateral.

En la ventana de configuración habrá una tabla por defecto que le daremos el nombre de “rtbl-default” para distinguirla de las que vamos a crear.

Ahora vamos a crear las tablas de enrutamiento que tendrán las rutas, que redirigen el tráfico en nuestra VPC entre nuestras subredes e internet.

Para ello, clic en botón “Create Route Table” y le damos el nombre “rtbl-internet” y la asociamos a nueva VPC.

Una vez creada, en la lista de tablas de ruta, ya la tendremos disponible.

Existe la tabla por defecto, que enruta todo el tráfico hacia nuestra VPC y sus subredes, pero vemos como no tenemos una entrada predeterminada, es decir, una “0.0.0.0/0” que permita enrutar todo el tráfico que vaya fuera de la subred hacia internet.

La idea es que la “rtbl\_default” permita enrutar hacia la subredes privadas. Para ello necesitamos asociar a esta tabla de rutas una subred. Para realizar esto seleccionamos la “rtbl-default” y en la pestaña inferior “Subnet Associations”, click en Edit y seleccionamos la “pri\_subnet1” y clic en Save. De esta forma, el rtbl\_default sirve como tabla de enrutamiento para redes internas.

15. Ahora tenemos que permitir el acceso a internet.

Seleccionamos el “rtbl-internet” y en pestaña routes, agregamos una nueva ruta, con la siguiente configuración:

- **Destination:** 0.0.0.0/0
- **Target:** igw.xxxxxx (el componente internet gateway que configuramos antes)

Clic en Save, ya tenemos configurada nuestra tabla de rutas para salida a internet.

Pero aún, no tendremos acceso a internet, porque ninguna subred está asociada a esta tabla, por lo que necesitamos asociar la subred pública.

Para ello, igual que hicimos antes, desde la pestaña “Subnet associations”, clic en Edit y seleccionamos la subred pública (la única que debe aparecer).

**Importante:** Solo una subred puede estar asociada a una tabla de enrutamiento.

16. Con esto ya tendríamos configurado la VPC y las subredes.

### Tarea 3. Crear key pair. Claves públicas y privadas

Para poder acceder a las instancias creadas es necesario acceder a través del concepto de claves privadas y públicas. Este par de claves van de la mano, es decir, es como una cerradura con 2 llaves, para poder abrirla se necesitan las 2.

AWS utiliza este sistema para acreditar nuestra identidad al conectarnos a una instancia. AWS almacena la clave pública y nosotros debemos proveer la clave privada, que solo nosotros debemos conocer, por tanto, es de vital importancia almacenarla en un lugar seguro.

AWS por seguridad no almacena una copia de los pares de claves generados, por tanto, es fundamental guardarla, ya que solo existirá una oportunidad de obtenerla y guardarla en local, solo estará disponible en el momento de crearla.

1. Desde AWS Console, accedemos al servicio EC2.
2. En el panel de navegación izquierdo, hacemos clic en **Network & Security** y clic en **Key Pairs**.
3. Hacemos clic en **Crear par de claves** y luego configure:
  - **Nombre de la clave:** mykey
  - **Formato:** pem
  - **Tag:** Name = mykeypairs
4. Ahora clic en **Create Key Pair**
5. Acto seguido vemos como un fichero (mykey.pem) es descargado.
6. Este fichero lo debemos guardar porque lo vamos a necesitar en las siguientes prácticas.

### Tarea 4. Crear instancias de EC2

En esta tarea, vamos a probar el funcionamiento de la VPC y las subredes.

Para ello necesitamos crear 2 máquinas virtuales (llamadas instancias en AWS), una en la subred privada y otra en la subred pública.

1. Desde AWS Console, en la barra de búsqueda ponemos “EC2”, y accedemos al servicio.
2. Accedemos a la opción “Dashboard”, en el menú lateral, en la parte superior.
3. El Dashboard es el panel de control de EC2, y en general, cualquier servicio ofrece esta vista.
4. En la parte inferior, clic sobre el botón “Launch instance”.

5. Vamos a crear 2 instancias de tipo linux, un Debian 9, como ya hicimos en las prácticas del tema anterior.
6. En la barra de búsqueda, ponemos “debian”, la primera que nos aparece “Debian 10 (HVM), SSD Volume Type” (elegible dentro de la Free-layer). Dejamos por defecto, 64-bit (x86) y clic en botón “Select”.
7. Ahora tenemos que elegir la configuración de la instancia, a nivel de CPU, Ram, Tipo de red, ... dejamos la opción por defecto, como aparece en la siguiente imagen.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes

Seguimos hacia delante en el asistente, y clic [Next:Configure instance details](#).

8. En esta pantalla debemos indicar:
  - a. VPC: WSRV\_VPC
  - b. Network: pub\_subnet1
  - c. Auto-assign Public IP: Le indicamos default (enable) o enable.
  - d. El resto de opciones lo dejamos por defecto.

Seguimos hacia delante en el asistente, y clic [Next: Add Storage](#)

9. El almacenamiento lo dejamos por defecto. Clic en [Next: Add Tags](#)
10. En pantalla etiqueta, le asignamos la etiqueta “Name = Debian1-Pruebas”. Clic en [Next: Configure Security Group](#)
11. En la pantalla de configuración de los Security Group.

Vamos a configurar el acceso por SSH y por ICMP (ping). Damos el nombre de sgdefault.

Configuramos como aparece en la imagen.

Type	Protocol	Port Range	Source
SSH	TCP	22	Custom 0.0.0.0/0
All ICMP - IPv4	ICMP	0 - 65535	Anywhere 0.0.0.0/0, ::/0

Ahora clic en Review y Launch, para revisar la configuración realizada antes de iniciar la máquina.

12. En la parte inferior de la pantalla clic en “Launch”, y nos pregunta para que ingresemos o creamos la key-pairs.

En nuestro caso seleccionamos la clave que creamos en la tarea anterior.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

Select a key pair

mykey

I acknowledge that I have access to the selected private key file (mykey.pem), and that without this file, I won't be able to log into my instance.

Cancel      Launch Instances

Para terminar clic en Launch Image.

13. Si todo va bien, la instancia comenzará a inciarse. Esto llevará varios minutos, con lo que aprovechamos para configurar la otra máquina, la que asignaremos a nuestra subred privada.
14. Ahora nos vamos a la lista de instancias, y a la instancia creada le ponemos el nombre “Debian1-Pruebas”
15. Para crear la nueva instancia, repetimos los pasos realizados para la instancia 1<sup>a</sup>, asignando a la pri-subnet1.

En Auto-assign Public IP le ponemos disabled, porque a esta red no queremos que se le asigne una IP pública.

En tags, le ponemos el nombre “pri-debian”.

Para el Security Group, reutilizamos el que creamos para 1<sup>a</sup> instancia, sgdefault.

Y por último, asignamos la clave “mykey” que creamos en otra tarea.

Y ya lanzamos la instancia.

16. Ahora toca esperar hasta que las 2 instancias estén creadas.
17. Una vez completado el inicio de las 2 instancias, podemos comprobar en su ficha, como AWS le ha asignado a la pub-debian una ip pública y una ip privada (esta siempre se la asigna).

Sin embargo, para la instancia pri-debian solamente tiene una ip privada.

#### Tarea 4. Crear un grupo de seguridad VPC

En esta tarea, creará un grupo de seguridad VPC, que actúa como un firewall virtual. Un grupo de seguridad lo utilizaremos en las siguientes prácticas, enlazado a las máquinas virtuales (instancias) que creemos. Uno o más grupos de seguridad se pueden asociar a una o varias instancias, y estos controlan el acceso desde la red a los recursos de las mismas.

Un grupo de seguridad permite agregar que controlar (permiten o deniegan) el tráfico hacia o desde las instancias asociadas.

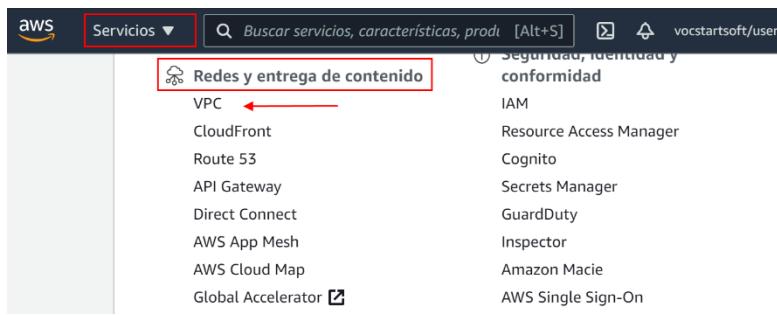
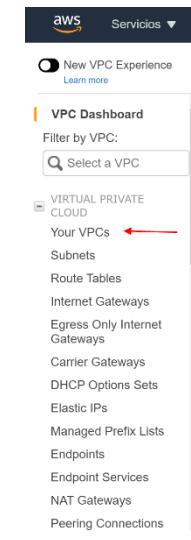
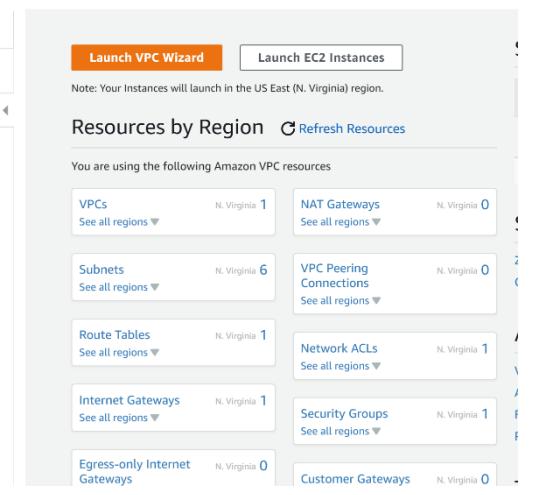
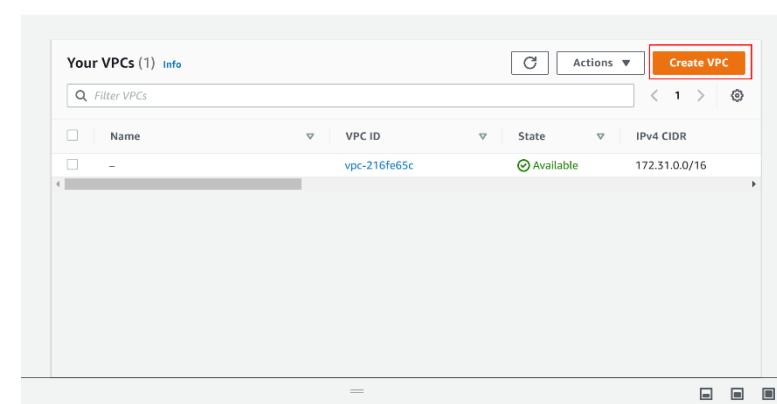
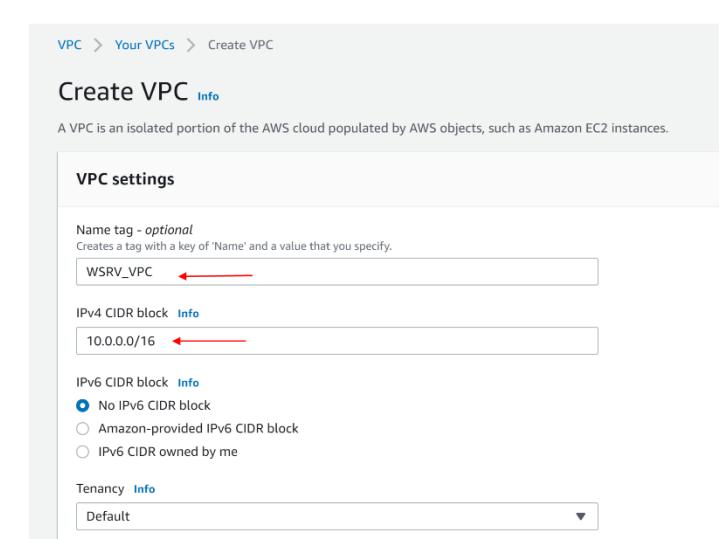
1. En el panel de navegación izquierdo, haga clic en **Grupos de seguridad**.
2. Haga clic en **Crear grupo de seguridad** y luego configure:
  - **Nombre del grupo de seguridad:** Web Security Group
  - **Descripción:** Enable HTTP access
  - **VPC:** VPC de laboratorio
3. En el panel **Reglas entrantes**, elija **Agregar regla**
4. Configure los siguientes ajustes:
  - **Tipo:** HTTP
  - **Fuente:** En cualquier lugar
  - **Descripción:** Permit web requests
5. Desplácese hasta la parte inferior de la página y elija **Crear grupo de seguridad**

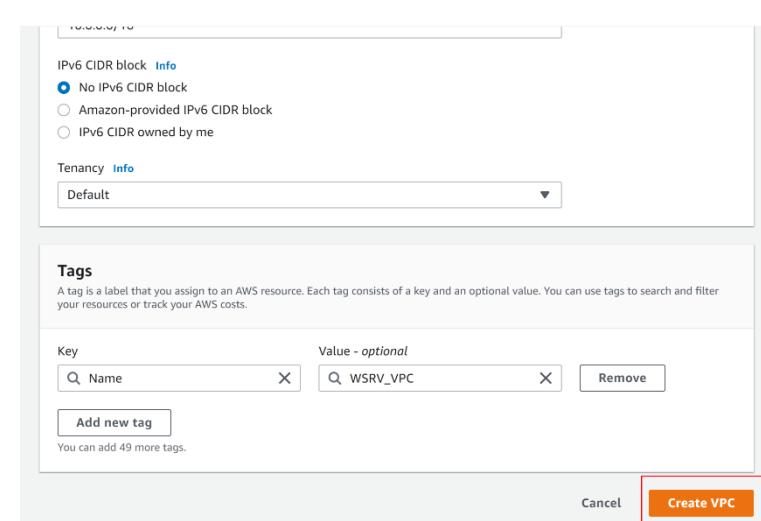
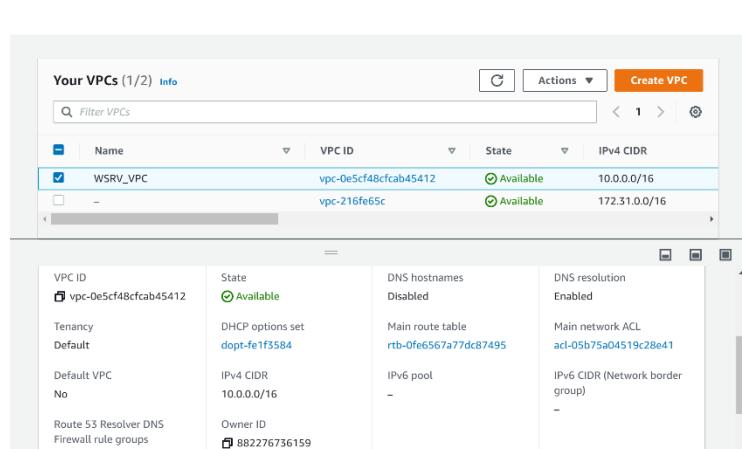
#### ENTREGA:

**DOCUMENTACIÓN:** Entregar un documento con las imágenes que demuestren la realización de la práctica.

**Instrumento de Evaluación:** prueba/evaluación en clase 100%.

## Crear una VPC

## Crear subnet (publica y privada)

New VPC Experience [Learn more](#)

VIRTUAL PRIVATE CLOUD

**Your VPCs**

- Subnets ←
- Route Tables
- Internet Gateways
- Egress Only Internet Gateways
- Carrier Gateways
- DHCP Options Sets
- Elastic IPs
- Managed Prefix Lists
- Endpoints
- Endpoint Services
- NAT Gateways
- Peering Connections

**Your VPCs (2) Info**

**Select a VPC above**

### Create subnet Info

**VPC**

**VPC ID**  
Create subnets in this VPC.  
 ←

**Associated VPC CIDRs**

IPv4 CIDRs  
10.0.0.0/16

**Subnets (6) Info**

Name	Subnet ID	State	VPC
—	subnet-c99818f8	Available	vpc-216fe65c
—	subnet-9264529c	Available	vpc-216fe65c
—	subnet-d3a2dc8c	Available	vpc-216fe65c
—	subnet-3d9fe25b	Available	vpc-216fe65c
—	subnet-c06219e1	Available	vpc-216fe65c
—	subnet-dfe7ea92	Available	vpc-216fe65c

**Select a subnet**

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

**IPv4 CIDR block** Info  
 ←

**Tags - optional**

Key	Value - optional
<input style="width: 150px; border: 1px solid #ccc; border-radius: 4px; padding: 2px 10px;" type="text" value="Name"/> <span style="color: red;">←</span>	<input style="width: 150px; border: 1px solid #ccc; border-radius: 4px; padding: 2px 10px;" type="text" value="pub-subnet1"/> <span style="color: red;">←</span>

**Add new tag**  
You can add 49 more tags.

**Add new subnet** ←

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

**IPv4 CIDR block** Info  
 ←

**Tags - optional**

Key	Value - optional
<input style="width: 150px; border: 1px solid #ccc; border-radius: 4px; padding: 2px 10px;" type="text" value="Name"/> <span style="color: red;">←</span>	<input style="width: 150px; border: 1px solid #ccc; border-radius: 4px; padding: 2px 10px;" type="text" value="pub-subnet1"/> <span style="color: red;">←</span>

**Add new tag**  
You can add 49 more tags.

**Add new subnet**

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.

**IPv4 CIDR block** Info

**Tags - optional**

Key	Value - optional
<input style="width: 150px; border: 1px solid #ccc; border-radius: 4px; padding: 2px 10px;" type="text" value="Name"/> <span style="color: red;">←</span>	<input style="width: 150px; border: 1px solid #ccc; border-radius: 4px; padding: 2px 10px;" type="text" value="pub-subnet1"/> <span style="color: red;">←</span>

**Add new tag**  
You can add 49 more tags.

**Add new subnet**

**Create subnet** ←

You have successfully created 1 subnet: subnet-0f58ca758e288ba5e

Subnets (1) <a href="#">Info</a>				
<a href="#">Actions</a> <a href="#">Create subnet</a>				
<a href="#">Filter subnets</a>				
<a href="#">Subnet ID: subnet-0f58ca758e288ba5e X</a>	<a href="#">Clear filters</a>	<a href="#">Name</a>	<a href="#">Subnet ID</a>	<a href="#">State</a>
pub-subnet1	subnet-0f58ca758e288ba5e	<a href="#">Available</a>	vpc-0e5cf48cfcab45412   WSR...	

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.  
[No preference](#)

**IPv4 CIDR block** [Info](#)  
 [X](#)

**Tags - optional**

Key	Value - optional
<a href="#">Name</a>	<a href="#">pri_subnet1</a>

[Add new tag](#)  
You can add 49 more tags.

[Remove](#)

[Add new subnet](#)

[Cancel](#) [Create subnet](#)

### Create subnet [Info](#)

**VPC**

VPC ID  
Create subnets in this VPC.  
[vpc-0e5cf48cfcab45412 \(WSRV\\_VPC\)](#)

**Associated VPC CIDs**

IPv4 CIDs  
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.  
[pri\\_subnet1](#)

The name can be up to 256 characters long.

You have successfully created 1 subnet: subnet-03a3acd4f92b67b68

Subnets (8) <a href="#">Info</a>				
<a href="#">Actions</a> <a href="#">Create subnet</a>				
<a href="#">Filter subnets</a>				
<a href="#">Name</a>	<a href="#">Subnet ID</a>	<a href="#">State</a>	<a href="#">VPC</a>	
pub-subnet1	subnet-0f58ca758e288ba5e	<a href="#">Available</a>	vpc-0e5cf48cfcab45412   WSR...	
-	subnet-c99818f8	<a href="#">Available</a>	vpc-216fe65c	
pri_subnet1	subnet-03a3acd4f92b67b68	<a href="#">Available</a>	vpc-0e5cf48cfcab45412   WSR...	
-	subnet-9264529c	<a href="#">Available</a>	vpc-216fe65c	
-	subnet-d3a2dc8c	<a href="#">Available</a>	vpc-216fe65c	
-	subnet-3d9fe25b	<a href="#">Available</a>	vpc-216fe65c	

Select a subnet

You have successfully created 1 subnet: subnet-03a3acd4f92b67b68

Subnets (1/8) <a href="#">Info</a>				
<a href="#">Actions</a> <a href="#">Create subnet</a>				
<a href="#">View details</a>				
<a href="#">Name</a>	<a href="#">Subnet ID</a>	<a href="#">State</a>	<a href="#">Actions</a>	
<input checked="" type="checkbox"/> pub-subnet1	subnet-0f58ca758e288ba5e	<a href="#">Available</a>	<a href="#">View details</a> <a href="#">Modify auto-assign IP settings</a> <a href="#">Edit IPv6 CIDs</a> <a href="#">Edit network ACL association</a> <a href="#">Edit route table association</a> <a href="#">Share subnet</a> <a href="#">Manage tags</a> <a href="#">Delete subnet</a>	
-	subnet-c99818f8	<a href="#">Available</a>		
pri_subnet1	subnet-03a3acd4f92b67b68	<a href="#">Available</a>		
-	subnet-9264529c	<a href="#">Available</a>		
-	subnet-d3a2dc8c	<a href="#">Available</a>		
-	subnet-3d9fe25b	<a href="#">Available</a>		

subnet-0f58ca758e288ba5e / pub-subnet1

[VPC](#) > [Subnets](#) > [subnet-0f58ca758e288ba5e](#) > [Modify auto-assign IP settings](#)

### Modify auto-assign IP settings [Info](#)

Enable the auto-assign IP address setting to automatically request a public IPv4 or IPv6 address for a new network interface in this subnet.

**Settings**

Subnet ID  
[subnet-0f58ca758e288ba5e](#)

Auto-assign IPv4 [Info](#)  
 Enable auto-assign public IPv4 address

Auto-assign customer-owned IPv4 address [Info](#)  
 Enable auto-assign customer-owned IPv4 address  
Option disabled because no customer owned pools found.

[Cancel](#) [Save](#)

## Crear el Internet Gateway

You have successfully modified auto-assign IP settings.  
• Public IPv4 address

**Subnets (1/8) Info**

**Routes (1)**

Destination	Target
10.0.0.0/16	local

Internet gateways (1/1) Info

Name	Internet gateway ID	State	VPC ID
-	igw-3bf00c41	Attached	vpc-216fe65c

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.

**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	X igw-1 X Remove

Add new tag  
You can add 49 more tags.

Cancel **Create internet gateway**

The following internet gateway was created: igw-07b5d59a526d8df0e. You can now attach to a VPC to enable the VPC to communicate with the internet.

Internet gateways (1/2) Info

Name	Internet gateway ID	State	VPC ID
igw-1	igw-07b5d59a526d8df0e	Attached	vpc-0e5cf48fcab45412
-	igw-3bf00c41	Attached	vpc-216fe65c

VPC > Internet gateways > Attach to VPC (igw-07b5d59a526d8df0e)

## Attach to VPC (igw-07b5d59a526d8df0e) Info

**VPC**  
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

**Available VPCs**  
Attach the internet gateway to this VPC.

AWS Command Line Interface command

Cancel **Attach internet gateway**

Internet gateways (2) Info

Name	Internet gateway ID	State	VPC ID
igw-1	igw-07b5d59a526d8df0e	Attached	vpc-0e5cf48fcab45412   WSR
-	igw-3bf00c41	Attached	vpc-216fe65c

## Crear una tabla de ruta

Route Tables

Name	Internet gateway ID
igw-1	igw-07b5d59a526d8df0e
-	igw-3bf00c41

Select an internet gateway above

Name	Route table ID	Main	VPC
<input checked="" type="checkbox"/> RTBL_DEFAULT	rtb-0fe6567a77dc87495	Yes	vpc-0e5cf48cfcab45412   WSR...
<input type="checkbox"/> -	rtb-413e2a3f	Yes	vpc-216fe65c

Name	Route table ID	Main	VPC
<input checked="" type="checkbox"/> RTBL_DEFAULT	rtb-0fe6567a77dc87495	Yes	vpc-0e5cf48cfcab45412
<input type="checkbox"/> -	rtb-413e2a3f	Yes	vpc-216fe65c

Name	Route table ID	Main	VPC
<input checked="" type="checkbox"/> RTBL_DEFAULT	rtb-0fe6567a77dc87495	Yes	vpc-0e5cf48cfcab45412
<input type="checkbox"/> -	rtb-413e2a3f	Yes	vpc-216fe65c
<input type="checkbox"/> RTBL-INTERNET	rtb-08c5af38f37cac2c7	No	vpc-0e5cf48cfcab45412

### Route table settings

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

RTBL-INTERNET

VPC  
The VPC to use for this route table.  
vpc-0e5cf48cfcab45412 (WSRV\_VPC)

### Tags

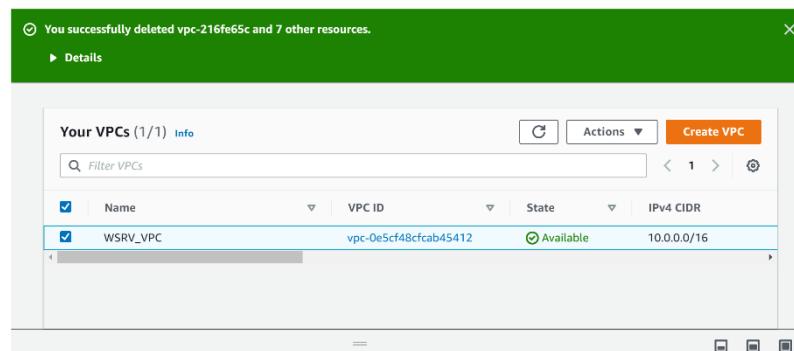
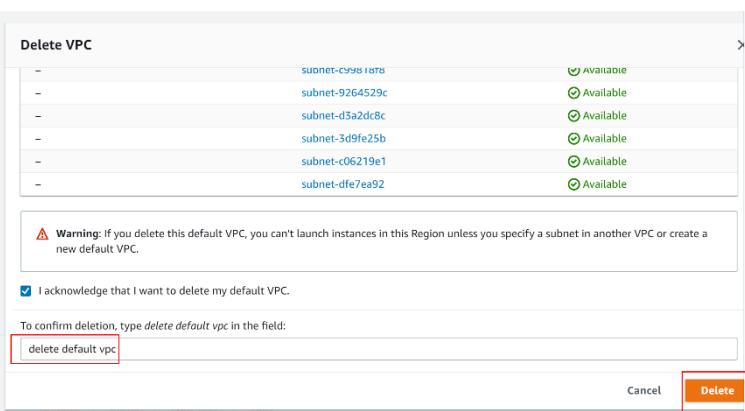
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
Q Name	Q RTBL-INTERNET

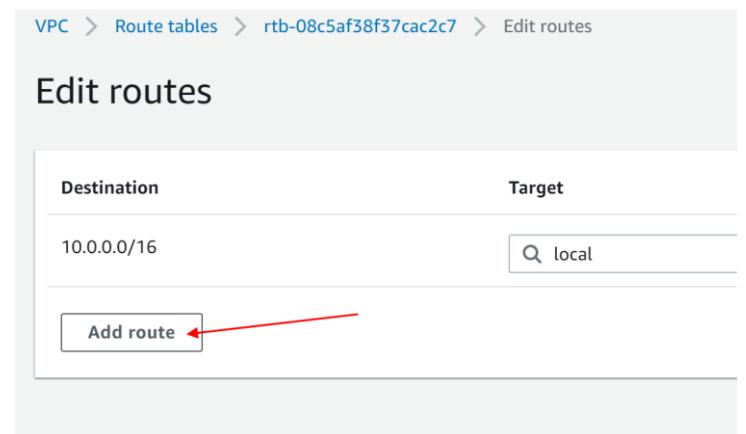
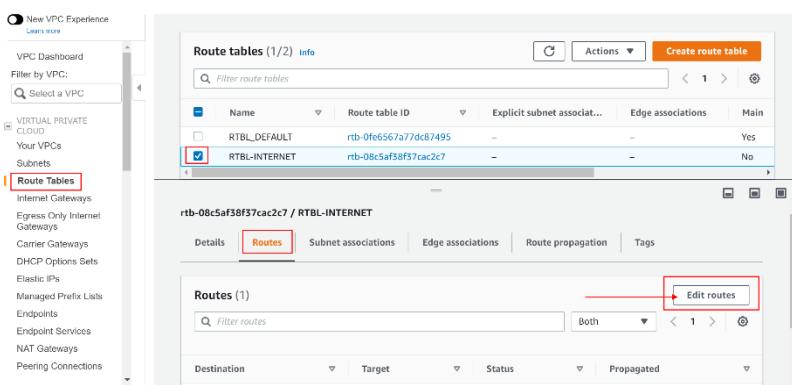
Add new tag  
You can add 49 more tags.

Create route table

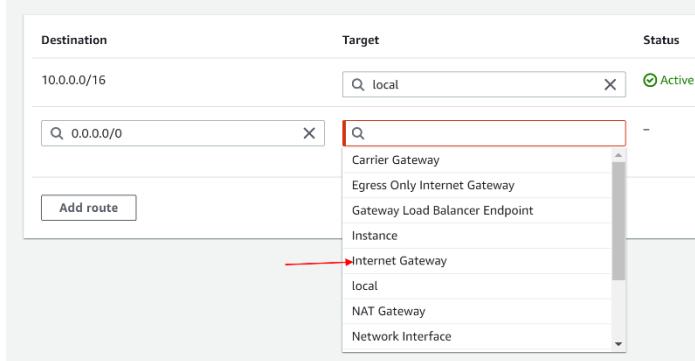
Name	Route table ID	Main	VPC
<input checked="" type="checkbox"/> RTBL_DEFAULT	rtb-0fe6567a77dc87495	Yes	vpc-0e5cf48cfcab45412
<input type="checkbox"/> -	rtb-413e2a3f	Yes	vpc-216fe65c
<input type="checkbox"/> RTBL-INTERNET	rtb-08c5af38f37cac2c7	No	vpc-0e5cf48cfcab45412



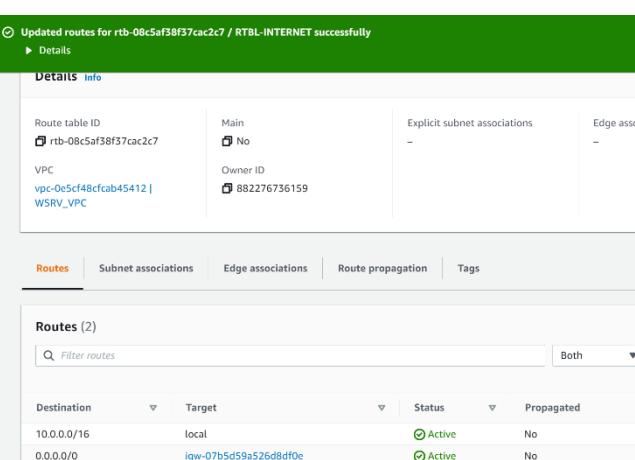
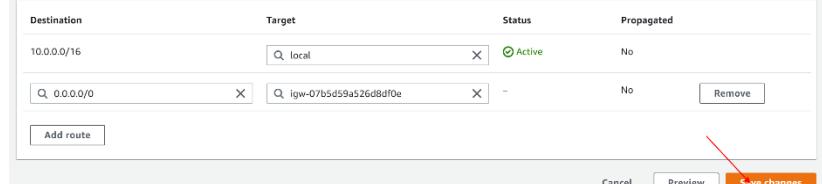
## Añadir una nueva ruta para el Internet Gateway



## Edit routes



## Edit routes



## Asignar tabla de ruta del Internet Gateway a la subnet publica

VPC Dashboard  
Filter by VPC:  
Select a VPC  
Virtual Private Cloud  
Your VPCs  
Subnets  
**Route Tables**  
Internet Gateways  
Egress Only Internet Gateways  
Carrier Gateways  
DHCP Options Sets  
Elastic IPs  
Managed Prefix Lists  
Endpoints  
Endpoint Services  
NAT Gateways  
Peering Connections  
Security  
Network ACLs  
Security Groups

Subnets (1/2) Info  
Filter subnets  
Name Sub... State VPC IPv4 Cl... IPv6... Avail... Available... Availability Zone  
pub\_subnet1 subnet-0f58ca758e288ba5e Available vpc-0e5cf48cfcab45412 | WSR... 10.0.0.0/24 - 251 us-east-1c us-east-1a26  
pri\_subnet1 subnet-03a3acd4f92b67b68 Available vpc-0e5cf48cfcab45412 | WSR... 10.0.1.0/24 - 251 us-east-1c us-east-1a26

subnet-0f58ca758e288ba5e / pub-subnet1  
Details Flow logs Route table Network ACL Sharing Tags  
Route table: rtb-0fe6567a77dc87495 / RTBL\_DEFAULT  
Routes (1)  
Destination Target  
10.0.0.0/16 local

VPC &gt; Subnets &gt; subnet-0f58ca758e288ba5e &gt; Edit route table association

## Edit route table association Info

## Subnet route table settings

Subnet ID  
subnet-0f58ca758e288ba5eRoute table ID  
rtb-0fe6567a77dc87495 (RTBL\_DEFAULT)rtb-0fe6567a77dc87495 (RTBL\_DEFAULT)  
Main route table  
rtb-08c5af38f37cac2c7 (RTBL-INTERNET)Destination Target  
10.0.0.0/16 local

Cancel Save

## Edit route table association Info

Subnet route table settings  
Subnet ID: subnet-0f58ca758e288ba5e  
Route table ID: rtb-08c5af38f37cac2c7 (RTBL-INTERNET)

Routes (2)  
Q Filter routes  
Destination Target  
10.0.0.0/16 local  
0.0.0.0/0 igw-07b5d59a526d8df0e

Cancel Save

Subnet (subnet-0f58ca758e288ba5e) has been successfully associated with route table (rtb-08c5af38f37cac2c7).

Subnets (1/2) Info  
Filter subnets  
pub\_subnet1 subnet-0f58ca758e288ba5e Available vpc-0e5cf48cfcab45412 | WSR... 10.0.0.0/24  
pri\_subnet1 subnet-03a3acd4f92b67b68 Available vpc-0e5cf48cfcab45412 | WSR... 10.0.1.0/24

subnet-0f58ca758e288ba5e / pri-subnet1  
Details Flow logs Route table Network ACL Sharing Tags  
Route table: rtb-08c5af38f37cac2c7 / RTBL-INTERNET  
Routes (2)  
Q Filter routes  
Destination Target  
10.0.0.0/16 local  
0.0.0.0/0 igw-07b5d59a526d8df0e

## Asignar Tabla de ruta Default a la subnet privada

Subnets (1/2) Info  
Filter subnets  
pub\_subnet1 subnet-0f58ca758e288ba5e Available vpc-0e5cf48cfcab45412 | WSR... 10.0.0.0/24  
pri\_subnet1 subnet-03a3acd4f92b67b68 Available vpc-0e5cf48cfcab45412 | WSR... 10.0.1.0/24

subnet-0f58ca758e288ba5e / pri-subnet1  
Details Flow logs Route table Network ACL Sharing Tags  
Route table: rtb-0fe6567a77dc87495 / RTBL\_DEFAULT  
Routes (1)  
Q Filter routes  
Destination Target  
10.0.0.0/16 local

## Edit route table association Info

## Subnet route table settings

Subnet ID  
subnet-03a3acd4f92b67b68Route table ID  
rtb-0fe6567a77dc87495 (RTBL\_DEFAULT)rtb-0fe6567a77dc87495 (RTBL\_DEFAULT)  
Main route table  
rtb-08c5af38f37cac2c7 (RTBL-INTERNET)Destination Target  
10.0.0.0/16 local

Cancel Save

## generar par de claves

Subnets (2) Info						
Name	Subnet ID	State	VPC	IPv4 CIDR	Actions	Create subnet
pub-subnet1	subnet-0f58ca758e288ba5e	Available	vpc-0e5cf48cfcab45412   WSR...	10.0.0.0/24		
pri_subnet1	subnet-03a5acd4f92b67b68	Available	vpc-0e5cf48cfcab45412   WSR...	10.0.1.0/24		

Favoritos

Agregue favoritos haciendo clic en la estrella situada junto al nombre del servicio.

Todos los servicios

Informática

- EC2
- Lightsail
- Lambda
- Batch
- Elastic Beanstalk
- Serverless Application Rep...
- AWS Outposts
- EC2 Image Builder

Pares de claves

Nombre Huella digital ID

No hay pares de claves para mostrar

Crear par de claves

Par de claves

Un par de claves, compuesto por una clave privada y una clave pública, es un conjunto de credenciales de seguridad que se utilizan para demostrar su identidad cuando se conecta a una instancia.

Nombre  
mykey

El nombre puede incluir hasta 255 caracteres ASCII. No puede incluir espacios al principio ni al final.

Formato de archivo

pem  
Para usar con OpenSSH

ppk  
Para usar con PuTTY

Etiquetas (opcional)

No hay etiquetas asociadas a este recurso.

Agregar etiqueta

Cancelar **Crear par de claves**

El par de claves se ha creado correctamente

Pares de claves (1)

Nombre Huella digital ID

mykey b2:8a:6af5:cf:9f:84:50:d7:d1:32:bd:07... key-021ff026337c14

Panel de EC2

Eventos

Etiquetas

Límites

Instancias

Instancias

Tipos de instancia

Plantillas de lanzamiento

Solicitudes de spot

Savings Plans

Instancias reservadas

Hosts dedicados

Instancias programadas

Reservas de capacidad

Imagenes

Comentarios

Español

mykey.pem

```
C:\Users\Sergio DC\Tools\cmders
λ cd C:\Users\Sergio DC\Desktop\Sistemas Informaticos\Tema 10 - AWS\UD10-Practica 10.1. Crear una VPC
C:\Users\Sergio DC\Desktop\Sistemas Informaticos\Tema 10 - AWS\UD10-Practica 10.1. Crear una VPC
λ chmod 600 mykey.pem
```

```
C:\Users\Sergio DC\Desktop\Sistemas Informaticos\Tema 10 - AWS\UD10-Practica 10.1. Crear una VPC
λ ls -la
total 1905
drwxr-xr-x 1 Sergio DC 197121 0 may. 12 13:29 ../
drwxr-xr-x 1 Sergio DC 197121 0 may. 11 16:58 ...
-rw-r--r-- 1 Sergio DC 197121 162 may. 12 12:52 '→$10. Practica 10.1. AWS. Crear una VPC_Subredes.docx'
drwxr-xr-x 1 Sergio DC 197121 0 may. 12 13:30 img/
-rw-r--r-- 1 Sergio DC 197121 3678 may. 12 13:27 mykey.pem
-rw-r--r-- 1 Sergio DC 197121 1928093 may. 11 17:19 'UD10. Practica 10.1. AWS. Crear una VPC_Subredes.docx'
```

Permiso lectura+escritura solo para el usuario

## Crear las instancias

**Paso 1: Elegir una imagen de Amazon Machine (AMI)**

Una AMI es una plantilla que contiene la configuración de software (sistema operativo, servicios de aplicaciones y aplicaciones) necesaria para lanzar la instancia. Puede seleccionar una AMI proporcionada por AWS, nuestra comunidad de usuarios o AWS Marketplace, o puede seleccionar una de sus propias AMI.

Instancias

Tipos de instancia

Plantillas de almacenamiento

Solicitudes de spot

Savings Plans

Instancias

Información

Estado de la Instancia

Lanzar Instancias

No tiene ninguna instancia en esta región

**Paso 1: Elegir una imagen de Amazon Machine (AMI)**

Una AMI es una plantilla que contiene la configuración de software (sistema operativo, servicios de aplicaciones y aplicaciones) necesaria para lanzar la instancia. Puede seleccionar una AMI proporcionada por AWS, nuestra comunidad de usuarios o AWS Marketplace, o puede seleccionar una de sus propias AMI.

Para buscar una AMI, escriba un término de búsqueda; por ejemplo, "Windows"

Inicio rápido

Mis AMI

AWS Marketplace

AMI de la comunidad

Selección rápida

Amazon Linux 2 AMI (HVM, SSD Volume Type) - ami-0cfef0f6840b45e9 (64 bits x86) / ami-09d19e619c57453f6 (64 bits Arm)

Amazon Linux 2 incluye unos años de soporte. Proporciona el kernel de Linux 1.14 adaptado para un rendimiento óptimo en Amazon EC2, systemd 219, Docker 1.28, Grub 2.28, Binutils 2.28... y en los últimos paquetes de software a través de componentes.

macOS Big Sur 11.3.1 - ami-073c65a5a533d959a

The macOS Big Sur AMI is an F2SS-supported image. This AMI includes the AWS Command Line Interface, Command Line Tools for Xcode, Amazon SSM Agent, and Homebrew. The AWS Homebrew Tap includes the latest versions of multiple AWS packages included in the AMI.

macOS Catalina 10.15.7 - ami-0a0ca7240f7b

The macOS Catalina AMI is an ESXi-backed AWS-supported image. This AMI includes the AWS Command Line Interface, Command Line Tools for Xcode, Amazon SSM Agent, and Homebrew. The AWS Homebrew Tap includes the latest versions of multiple AWS packages included in the AMI.

**Paso 1: Elegir una imagen de Amazon Machine (AMI)**

Una AMI es una plantilla que contiene la configuración de software (sistema operativo, servicios de aplicaciones y aplicaciones) necesaria para lanzar la instancia. Puede seleccionar una AMI proporcionada por AWS, nuestra comunidad de usuarios o AWS Marketplace, o puede seleccionar una de sus propias AMI.

C: debian

Debian 10 (HVM, SSD Volume Type) - ami-0702ee1feeb0d996c (64 bits x86) / ami-08022930cd0deb2a (64 bits Arm)

Debian 10 (HVM, EBS General Purpose (SSD) Volume Type, Community developed free GNU/Linux distribution, https://www.debian.org/)

Tipo de dispositivo (x86): Tipo de virtualización: Intel

Habilitado para UMA: Si

Auto para la copia

Selecicionar

Mostrar por páginas de Systems Manager

1 a 1 de 1 AMI

Mis AMI (0)

AWS Marketplace (446)

AMI de la comunidad (16932)

So encontraron los siguientes resultados para "debian" en otros catálogos:

- 448 resultados en AWS Marketplace
- 448 resultados en AWS Marketplace
- 18952 resultados en AMI de la comunidad

Las AMI de la comunidad son AMI que ha compartido la comunidad general de AWS.

**Paso 2: Página Choose an Instance Type**

Amazon EC2 proporciona una amplia selección de tipos de instancias optimizados para adaptarse a diferentes casos de uso. Las instancias son servidores virtuales que pueden ejecutar aplicaciones. Tienen distintas combinaciones de CPU, memoria, almacenamiento y capacidad de red, lo que proporciona una gran flexibilidad para elegir la combinación de recursos adecuada para las aplicaciones. [Más información](#) acerca de los tipos de instancias y cómo pueden satisfacer sus necesidades de computación.

Filtrar por: Todas las familias de Instancias Generación actual Mostrar/ocultar columnas

Seleccionada actualmente: t2.micro - ECU, 1 vCPU, 2,6 GHz., 1, 0,5 memoria, EBS solo

Familia	Tipo	vCPU	Memoria (GiB)	Almacenamiento de la Instancia (GB)	Optimizado para EBS disponible	Desempeño de la red	Compatibilidad con IPv6
t2	t2.nano	1	0,5	EBS solo	-	De bajo a moderado	Si
t2	t2.micro	1	1	EBS solo	-	De bajo a moderado	Si
t2	t2.small	1	2	EBS solo	-	De bajo a moderado	Si
t2	t2.medium	2	4	EBS solo	-	De bajo a moderado	Si
t2	t2.large	2	8	EBS solo	-	De bajo a moderado	Si
t2	t2.xlarge	4	16	EBS solo	-	Moderada	Si
t2	t2.2xlarge	8	32	EBS solo	-	Moderada	Si

Cancelar Anterior Revisar y lanzar Siguiente: Página Configuración de los detalles de la instancia

**Paso 3: Página Configuración de los detalles de la instancia**

No se ha encontrado ninguna VPC predeterminada. Seleccione otra VPC o crear una nueva VPC predeterminada.

Configure la instancia adecuada a sus requisitos. Puede lanzar varias instancias desde la misma AMI, solicitar instancias de spot para aprovechar la instancia, entre otras operaciones.

Número de instancias: 1 Lanzar en grupo de Auto Scaling

Opción de compra: □ Solicitar instancias de spot

Red:  C Crear nueva VPC  
No se ha encontrado ninguna VPC predeterminada. [Crear una nueva VPC predeterminada.](#)

Subred:  C Crear nueva subred  
251 direcciones IP disponibles

Asignar automáticamente IP pública: □ Usar configuración de subred (habilitar)

Grupo de ubicación: □ Agregue la instancia a un grupo de ubicación.

Reserva de capacidad: □ Abrir C Crear nuevo directorio

Directorio de unión al dominio: □ Ningún directorio C Crear nuevo directorio

Cancelar

**Paso 3: Página Configuración de los detalles de la instancia**

Interfaces de red: □

Dispositivo	Interfaz de red	Subred	IP principal	Direcciones IP secundarias	Direcciones IP IPv6
eth0	Nueva interfaz de red	subred-0f58ca758e288ba5e	Asignación automática	Añadir IP	The selected subnet does not support IPv6 because it does not have an IPv6 CIDR.

Añadir dispositivo

Detalles avanzados

Enclave: □ Habilitar  
Metadatos accesibles: □ Habilitado  
Versión de metadatos: V1 y V2 (token opcional): 4  
Límite de saltos de respuesta de token de metadatos: 1 4  
Datos de usuario: □ Como texto □ Como archivo □ La entrada ya está codificada en base64  
(Opcional)

C Cancelar Anterior Revisar y lanzar Siguiente: Adición de almacenamiento

**Paso 6: Página Configure Security Group**

Un grupo de seguridad es un conjunto de reglas del firewall que controlan el tráfico de la instancia. En esta página, puede agregar reglas para permitir configurar un servidor web y permitir que el tráfico de Internet llegue a la instancia, agregue reglas que permitan el acceso sin restricción a los puertos existentes a continuación. [Más información](#) sobre los grupos de seguridad de Amazon EC2.

Asignar un grupo de seguridad:

- Crear un nuevo grupo de seguridad
- Seleccionar un grupo de seguridad existente

Nombre del grupo de seguridad: sgdefault

Descripción: sgdefault created 2021-05-12

Tipo	Protocolo	Rango de puertos	Origen
SSH	TCP	22	Personalizado: 0.0.0.0/0

Añadir regla →

**Paso 5: Agregar etiquetas**

Un grupo de seguridad es un conjunto de reglas del firewall que controlan el tráfico de la instancia. En esta página, puede agregar reglas para permitir que determinado tráfico llegue a la instancia. Por ejemplo, si desea configurar un servidor web y permitir que el tráfico de Internet llegue a la instancia, agregue reglas que permitan el acceso sin restricción a los puertos existentes a continuación. [Más información](#) sobre los grupos de seguridad de Amazon EC2.

Asignar un grupo de seguridad:

- Crear un nuevo grupo de seguridad
- Seleccionar un grupo de seguridad existente

Nombre del grupo de seguridad: sgdefault

Descripción: sgdefault created 2021-05-12

Tipo	Protocolo	Rango de puertos	Origen	Descripción
SSH	TCP	22	Personalizado: 0.0.0.0/0	por ejemplo SSH for Admin Desktop
Todos el ICMP	ICMP	0 - 65535	Cualquier: 0.0.0.0/0	por ejemplo ICMP for Admin Desktop

Añadir regla →

**Aviso**  
Las reglas con el origen 0.0.0.0 permiten que todas las direcciones IP tengan acceso a la instancia. Le recomendamos que configure las reglas del grupo de seguridad para permitir el acceso únicamente desde direcciones IP conocidas.

Cancelar Anterior Revisar y lanzar

**Paso 7: Página Review Instance Launch**

Detalles de la AMI

Debian 10 (HVM), SSD Volume Type: ami-07d02ee1eeb0c996c  
Debian 10 (HVM), EBS General Purpose (SSD) Volume Type. Community developed free GNU/Linux distribution. <https://www.debian.org/>

Auto para la capa

Tipo de dispositivo: /dev/sda  
Tipo de virtualización: hvm

Tipo de instancia ECU vCPU Memoria (GiB) Almacenamiento de la instancia (GB) Optimizado para EBS disponible Desempeño de la red

t2.micro - 1 1 EBS solo Low to Moderate

Editor tipo de instancia

Grupos de seguridad

Nombre del grupo de seguridad: sgdefault  
Descripción: sgdefault created 2021-05-12

Tipo	Protocolo	Rango de puertos	Origen	Descripción
SSH	TCP	22	0.0.0.0/0	
Todos el ICMP IPv4	Todo	N/D	0.0.0.0/0	
Todos el ICMP IPv4	Todo	N/D	0.0.0.0/0	

Cancelar Anterior Lanzar

**Seleccione un par de claves existente o cree un nuevo par de claves**

Un par de claves consta de una clave pública que AWS almacena y un archivo de claves privadas que usted almacena. Juntos, le permiten conectarse a su instancia de forma segura. Para las AMI de Windows, el archivo de claves privadas es necesario para obtener la contraseña usada para iniciar sesión en la instancia. Para las AMI de Linux, el archivo de claves privadas le permite realizar una conexión SSH segura con su instancia.

Nota: El par de claves seleccionado se añadirá al conjunto de claves autorizadas para esta instancia. Obtenga más información sobre [cómo eliminar pares de claves existentes de una AMI pública](#).

Elegir un par de claves existente  
Seleccionar un par de claves  
mykey  
Confirme que tengo acceso al archivo de claves privadas (mykey.pem) y que sin este archivo no podré iniciar sesión en mi instancia.

Cancelar Lanzar instancias

## Página Launch Status

Se está lanzando su instancia  
Se ha iniciado el siguiente lanzamiento de instancia: i-027d738841c96291a [Ver log de lanzamiento](#)

Recibir notificaciones de los cargos estimados  
Crear alertas de facturación para obtener una notificación por correo electrónico cuando los cargos estimados uso gratuita).

## Cómo conectarse a la instancia

Se está lanzando su instancia. Pueden transcurrir unos minutos hasta que tenga el estado **en ejecución**, momento en el inmediatamente y seguirán devengando gastos hasta que detenga o termine la instancia.

Haga clic en [Ver las instancias](#) para monitorizar el estado de su instancia. Cuando la instancia tenga el estado **en ejecución** instancia.

## Aquí tiene algunos recursos útiles que le ayudarán a comenzar

- [Cómo conectarse a la instancia Linux](#)
- [Amazon EC2: Guía del usuario](#)
- [Más información sobre la capa de uso gratuita de AWS](#)
- [Amazon EC2: Foro de debate](#)

NewEC2 Experience

Panel de EC2

Eventos

Etiquetas

Instancias

Instancias New

Típos de instancia

Plantillas de lanzamiento

Solicitudes de spot

Savings Plans

Instancias reservadas

Hosts dedicados

Instancias programadas

Reservas de capacidad

Imagenes

AMI

Damos la bienvenida a la nueva experiencia de Instancias

Instancias (1/1) Información

Instancia: i-027d738841c96291a (pub-debian)

Estado de la instancia: En ejecución

ID de la instancia: i-027d738841c96291a

Dirección IPv4 pública: 52.87.189.97 | dirección abierta

Direcciones IPv4 privadas: 10.0.0.245

DNS IPv4 privado: ip-10-0-0-245.cc2.internal

Estado de la instancia: En ejecución

## Acceder por ComandLine a la máquina Debian con ssh

The screenshot shows the AWS Management Console with the EC2 service selected. In the left sidebar, under 'Instancias', there is a red arrow pointing to the 'pub-debian' instance. The main content area displays a table with one row for the instance, showing details like Name (pub-debian), ID de la instancia (i-027d738841c96291a), Estado de la i... (En ejecución), Tipo de inst... (t2.micro), and Estado de la ... (2/2 comprobador). A red arrow points from the instance name in the table to the instance name in the 'Información' tab below.

This screenshot shows the 'Conectar a la instancia' (Connect to instance) page for the instance 'i-027d738841c96291a'. It includes sections for 'Conexión de la instancia EC2' (EC2 connection), 'Administrador de sesiones' (Session manager), and 'Cliente SSH' (SSH client). Under 'Conexión de la instancia EC2', there is a red box around the 'Nombre de usuario' (User name) field, which is set to 'admin'. A red arrow points from this field to the 'User name' field in the terminal window below.

The screenshot shows the AWS EC2 Instances page with the 'pub-debian' instance selected. A red arrow points from the instance name in the table to the 'Información' tab in the details panel. Another red arrow points from the 'Dirección IP4 pública' (Public IPv4 address) field in the details panel to the terminal window below.

This terminal window titled 'Cmder' shows an SSH session to the instance 'i-027d738841c96291a'. The session starts with the command 'ssh -i mykey.pem admin@52.87.189.97'. It then asks for authentication, and the user types 'yes'. The terminal then displays the Debian license and the prompt 'admin@ip-10-0-0-245:~\$'. A red arrow points from the terminal window back to the 'User name' field in the 'Conectar a la instancia' page above.

```
admin@ip-10-0-0-245:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default
    link/ether 0e:8:cc:f3:aa:19 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.245/24 brd 10.0.0.255 scope global dynamic eth0
        valid_lft 3018sec preferred_lft 3018sec
    inet6 fe80::c8:ccff:fef3:aa19/64 scope link
        valid_lft forever preferred_lft forever
admin@ip-10-0-0-245:~$
```

```
admin@ip-10-0-0-245:~$ sudo apt update
Get:1 http://security.debian.org/debian-security buster/updates InRelease [65.4 kB]
Get:2 http://cdn-aws.deb.debian.org/debian buster InRelease [121 kB]
Get:3 http://cdn-aws.deb.debian.org/debian buster-updates InRelease [51.9 kB]
Get:4 http://cdn-aws.deb.debian.org/debian buster-backports InRelease [46.7 kB]
Get:5 http://security.debian.org/debian-security buster/updates/main Sources [184 kB]
Get:6 http://security.debian.org/debian-security buster/updates/main amd64 Packages [286 kB]
Get:7 http://security.debian.org/debian-security buster/updates/main Translation-en [148 kB]
Get:8 http://cdn-aws.deb.debian.org/debian buster/main Sources [7841 kB]
Get:9 http://cdn-aws.deb.debian.org/debian buster/main amd64 Packages [7907 kB]
Get:10 http://cdn-aws.deb.debian.org/debian buster/main Translation-en [5969 kB]
Get:11 http://cdn-aws.deb.debian.org/debian buster-updates/main Sources [4868 B]
Get:12 http://cdn-aws.deb.debian.org/debian buster-updates/main amd64 Packages [10.9 kB]
Get:13 http://cdn-aws.deb.debian.org/debian buster-updates/main Translation-en [7807 B]
Get:14 http://cdn-aws.deb.debian.org/debian buster-backports/main Sources [455 kB]
Get:15 http://cdn-aws.deb.debian.org/debian buster-backports/main amd64 Packages [467 kB]
Get:16 http://cdn-aws.deb.debian.org/debian buster-backports/main Translation-en [394 kB]
Fetched 24.0 MB in 5s (5319 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
43 packages can be upgraded. Run 'apt list --upgradable' to see them.
admin@ip-10-0-0-245:~$
```

```
Cmder
C:\Users\Sergio DC\Desktop\Sistemas Informaticos\Tema 10
rear una VPC
λ ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=10ms TTL=114
Respuesta desde 8.8.8.8: bytes=32 tiempo=24ms TTL=114
Respuesta desde 8.8.8.8: bytes=32 tiempo=10ms TTL=114
Respuesta desde 8.8.8.8: bytes=32 tiempo=10ms TTL=114

Estadísticas de ping para 8.8.8.8:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
  Tiempos aproximados de ida y vuelta en milisegundos:
    Minimo = 10ms, Máximo = 24ms, Media = 13ms
```

```
Cmder
admin@ip-10-0-0-245:~$ sudo apt install dnutils
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package dnutils
admin@ip-10-0-0-245:~$
```

## Crear la instancia de la Debian privada

**Paso 1: Página Choose an Instance Type**

Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación ...	Estado de la ...	Zona de dispon...
pub-debian	i-027d738841c96291a	En ejecución	t2.micro	2/2 comprobador	1 alarme	us-east-1c

**Paso 2: Página Choose an Instance Type**

Familia	Tipo	vCPU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Optimizado para EBS disponible	Desempeño de la
i2	i2.nano	1	0.5	EBS solo	-	De bajo a mod
i2	i2.micro	1	1	EBS solo	-	De bajo a mod
i2	i2.small	1	2	EBS solo	-	De bajo a mod
i2	i2.medium	2	4	EBS solo	-	De bajo a mod
i2	i2.large	2	8	EBS solo	-	De bajo a mod
i2	i2.xlarge	4	16	EBS solo	-	Moderada
i2	i2.2xlarge	8	32	EBS solo	-	Moderada

**Paso 3: Página Configuration of the details of the instance**

**Paso 4: Adición de almacenamiento**

**Paso 5: Agregar etiquetas**

Paso 6: Página Configure Security Group

Un grupo de seguridad es un conjunto de reglas del firewall que controlan el tráfico de la instancia. En esta página, puede agregar reglas para permitir que determinado tráfico llegue a la instancia. Por ejemplo, si desea configurar un servicio web y permitir que el tráfico de Internet llegue a la instancia, agregue reglas que permitan el acceso sin restricción a los puertos HTTP y HTTPS. Puede crear un nuevo grupo de seguridad o seleccionar uno existente a continuación. [Más información](#) sobre los grupos de seguridad de Amazon EC2.

**Asignar un grupo de seguridad:**

- Generar un nuevo grupo de seguridad
- Seleccionar un grupo de seguridad existente

ID de grupo de seguridad	Nombre	Descripción	Acciones
sg-023c63188778deed	default	default VPC security group sg/default created 2021-05-12	Copiar en uno nuevo Copiar en uno nuevo

Reglas de entrada para sg-023c63188778deed (Grupos de seguridad seleccionados: sg-023c63188778deed)

Tipo	Protocolo	Rango de puertos	Origen	Descripción
SSH	TCP	22	0.0.0.0/0	
Todos el ICMP IPv4	Todo	N/D	0.0.0.0/0	
Todos el ICMP IPv4	Todo	N/D	0.0.0.0/0	

**Cancelar** **Anterior** **Review later** **Lanzar**

Paso 7: Página Review Instance Launch

Revise los detalles de lanzamiento de su instancia. Haga clic en **Lanzar** para asignar un par de claves a la instancia y completar el proceso de lanzamiento.

**Mejore la seguridad de su instancia. Su grupo de seguridad, sgdefault, está abierto a todo el mundo.**

Su instancia puede estar accesible desde cualquier dirección IP. Le recomendamos que actualice las reglas de su grupo de seguridad para permitir el acceso únicamente desde direcciones IP conocidas. También puede abrir puertos adicionales en su grupo de seguridad para facilitar el acceso a la aplicación o el servicio que esté ejecutando, por ejemplo, HTTP (80) para los servicios web. [Editar grupos de seguridad](#)

**Detalles de la AMI**

Debian 10 (HVM), SSD Volume Type - ami-07d02e1eb0c996c

Auto-pausa: Deshabilitada | Auto-encendido: Deshabilitado | EBS: No | Tipo de visualización: Linux

**Tipo de instancia**

Tipo de instancia	ECU	vCPU	Memoria (GiB)	Almacenamiento de la instancia (GB)	Optimizado para EBS disponible	Desempeño de la red
t2.micro	1	1	EBS solo	-	-	Low to Moderate

**Grupos de seguridad**

**Cancelar** **Anterior** **Lanzar**

Seleccione un par de claves existente o cree un nuevo par de claves

Un par de claves consta de una **clave pública** que AWS almacena y un **archivo de claves privadas** que usted almacena. Juntos, le permiten conectarse a su instancia de forma segura. Para las AMI de Windows, el archivo de claves privadas es necesario para obtener la contraseña usada para iniciar sesión en la instancia. Para las AMI de Linux, el archivo de claves privadas le permite realizar una conexión SSH segura con su instancia.

Nota: El par de claves seleccionado se añadirá al conjunto de claves autorizadas para esta instancia. Obtenga más información sobre [cómo eliminar pares de claves existentes de una AMI pública](#).

**Elegir un par de claves existente**

**Seleccionar un par de claves**

mykey

Confirme que tengo acceso al archivo de claves privadas (mykey.pem) y que sin este archivo no podré iniciar sesión en mi instancia.

**Cancelar** **Lanzar instancias**

## Página Launch Status

### ✓ Se está lanzando su instancia

Se ha iniciado el siguiente lanzamiento de instancia: i-040e4e22132c1dc96 [Ver log de lanzamiento](#)

### ℹ Recibir notificaciones de los cargos estimados

[Crear alertas de facturación](#) para obtener una notificación por correo electrónico cuando los cargos estimados uso gratuita).

## Cómo conectarse a la instancia

Se está lanzado su instancia. Pueden transcurrir unos minutos hasta que tenga el estado **en ejecución**, momento en el cual inmediatamente y seguirán devengando gastos hasta que detenga o termine la instancia.

Haga clic en [Ver las instancias](#) para monitorizar el estado de su instancia. Cuando la instancia tenga el estado **en ejecución**, haga clic en [Conectar](#) para conectarse a la instancia.

## ▼ Aquí tiene algunos recursos útiles que le ayudarán a comenzar

- [Cómo conectarse a la instancia Linux](#)
- [Más información sobre la capa de uso gratuita de AWS](#)
- [Amazon EC2: Guía del usuario](#)
- [Amazon EC2: Foro de debate](#)

**BWS Servicios**

**Instancias** **now**

Tipos de instancia

Plantillas de lanzamiento

Solicitudes de spot

Savings Plans

Instancias reservadas

Hosts dedicados

Instancias programadas

Reservas de capacidad

Imágenes

AMI

Elastic Block Store

Volumenes

Instantáneas

Administrador del ciclo de vida

Red y seguridad

Security Groups

**Instancias**

**Instancias (1/2) Información**

**Instancia: i-040e4e22132c1dc96 (pri-debian)**

**Detalles** **Seguridad** **Redes** **Almacenamiento** **Comprobaciones de estado** **Monitoreo** **Etiquetas**

Resumen de instancia: i-040e4e22132c1dc96 (pri-debian)

ID de la instancia: i-040e4e22132c1dc96 (pri-debian)

Estado de la instancia: En ejecución

Dirección IPv4 pública: 10.0.1.212

Direcciones IPv4 privadas: ip-10-0-1-212.ec2.internal

DNS IPv4 privado: ip-10-0-1-212.ec2.internal

```
admin@ip-10-0-0-245:~$ ping 10.0.1.212
PING 10.0.1.212 (10.0.1.212) 56(84) bytes of data.
64 bytes from 10.0.1.212: icmp_seq=1 ttl=64 time=0.437 ms
64 bytes from 10.0.1.212: icmp_seq=2 ttl=64 time=0.443 ms
64 bytes from 10.0.1.212: icmp_seq=3 ttl=64 time=0.374 ms
64 bytes from 10.0.1.212: icmp_seq=4 ttl=64 time=0.395 ms
64 bytes from 10.0.1.212: icmp_seq=5 ttl=64 time=0.524 ms
64 bytes from 10.0.1.212: icmp_seq=6 ttl=64 time=0.545 ms
64 bytes from 10.0.1.212: icmp_seq=7 ttl=64 time=0.375 ms
64 bytes from 10.0.1.212: icmp_seq=8 ttl=64 time=0.430 ms
64 bytes from 10.0.1.212: icmp_seq=9 ttl=64 time=0.638 ms
64 bytes from 10.0.1.212: icmp_seq=10 ttl=64 time=0.553 ms
^C
--- 10.0.1.212 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 217ms
rtt min/avg/max/mdev = 0.374/0.471/0.638/0.086 ms
admin@ip-10-0-0-245:~$
```

Pasar la clave mykey.key hacia la debian publica

```
C:\Users\Sergio DC\Desktop\Sistemas Informaticos\Tema 10 - AWS\UD10-Practica 10.1. Crear una VPC
λ scp -i mykey.pem mykey.pem admin@52.87.189.97:~
mykey.pem                                     100% 1678     15.8KB/s   00:00
```

```
admin@ip-10-0-0-245:~$ ls
mykey.pem
```

Acceder a la debian privada a través de la pública con ssh

```
admin@ip-10-0-0-245:~$ sudo ssh -i mykey.pem admin@10.0.1.212
The authenticity of host '10.0.1.212 (10.0.1.212)' can't be established.
ECDSA key fingerprint is SHA256:kp0Te8+7C9S0v1BAj3T/Ukf8qPs5heLNVL19mIZDfiY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.212' (ECDSA) to the list of known hosts.
Linux ip-10-0-1-212 4.19.0-14-cloud-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
admin@ip-10-0-1-212:~$
```

```
admin@ip-10-0-1-212:~$ exit
logout
Connection to 10.0.1.212 closed.
admin@ip-10-0-0-245:~$ exit
logout
Connection to 52.87.189.97 closed.
```

Detener las instancias

	Name	ID de la instancia	Estado de la i...
<input checked="" type="checkbox"/>	pub-debian	i-027d738841c96291a	En ejecución
<input checked="" type="checkbox"/>	pri-debian	i-040e4e22132c1dc96	En ejecución

¿Detener Instancias?

Los ID de la instancia

- i-027d738841c96291a (pub-debian)
- i-040e4e22132c1dc96 (pri-debian)

Para confirmar que desea detener la Instancia, seleccione el botón Detener debajo.

Cancelar Detener

	Name	ID de la instancia	Estado de la i...
<input type="checkbox"/>	pub-debian	i-027d738841c96291a	Detenida
<input type="checkbox"/>	pri-debian	i-040e4e22132c1dc96	Detenida