



## Datos Generales:

**Nombre:** Tomás Alfredo Villaseca Constantinescu

**País:** Chile

**Fecha:** 14/09/2023

**Contacto:** [tomas.villaseca.c@gmail.com](mailto:tomas.villaseca.c@gmail.com)

En esta sesión de laboratorio, hará lo siguiente:

- Resumir la situación del cliente
- Crear una VPC, una puerta de enlace de Internet, una tabla de enrutamiento, un grupo de seguridad, una lista de acceso de redes y una instancia EC2 para generar una red enrutable dentro de la VPC.
- Familiarizarse con la consola
- Desarrollar una solución para el problema del cliente presentado en esta sesión de laboratorio

La sesión de laboratorio se completará una vez que pueda utilizar con éxito el comando ping por fuera de la VPC.

## Situación:

Su rol es el de un ingeniero de soporte en la nube en Amazon Web Services (AWS). Durante su turno, un cliente de una empresa emergente solicita asistencia con respecto a un problema de redes que tiene en su infraestructura de AWS.

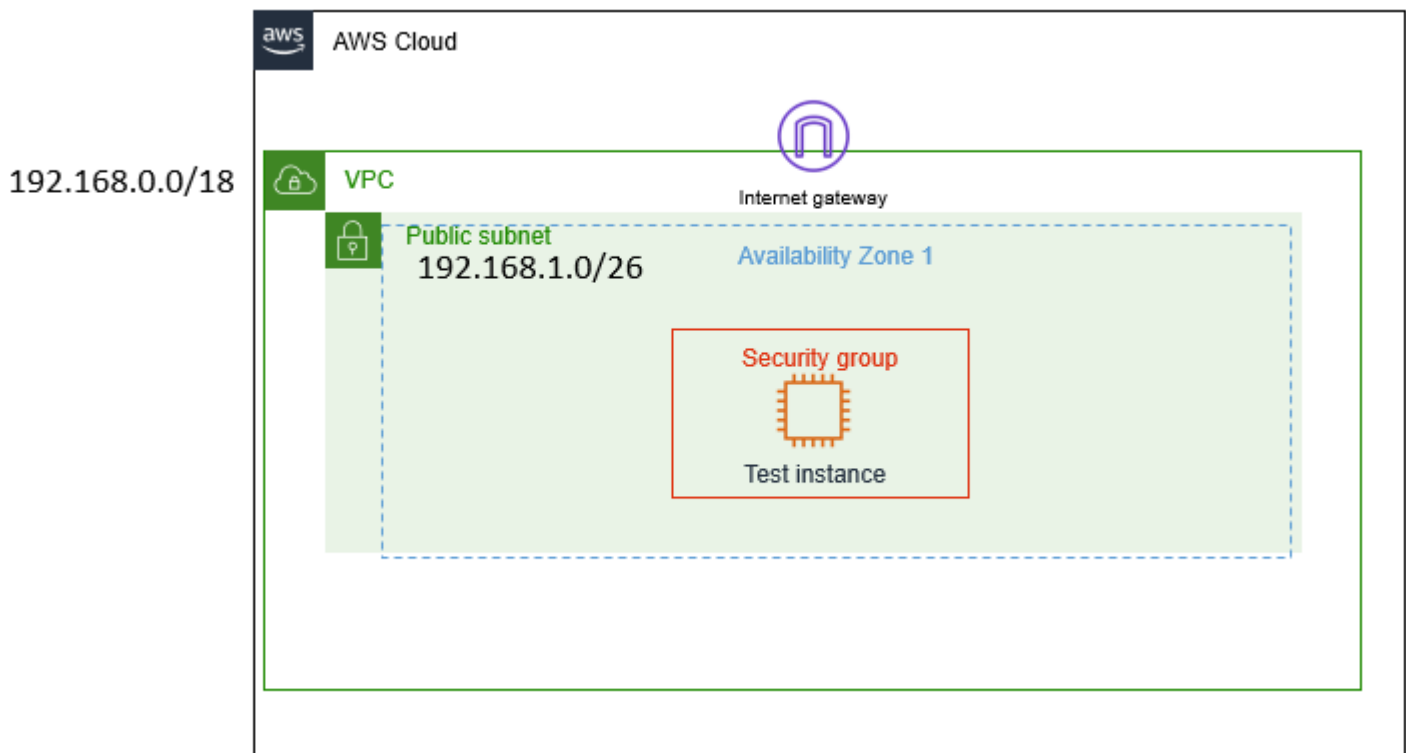
A continuación, se encuentran el correo electrónico y un archivo adjunto de su arquitectura:

### Correo electrónico del cliente

¡Hola, equipo de soporte en la nube!

Hace unos días, me puse en contacto con ustedes para solicitar ayuda a fin de configurar mi VPC. Pensé que sabía adjuntar todos los recursos para establecer una conexión a Internet, pero ni siquiera puedo hacer ping por fuera de la VPC. ¡Todo lo que necesito es hacer ping! ¿Me pueden ayudar a configurar mi VPC donde tenga conectividad de red y pueda hacer ping? A continuación, se encuentra la arquitectura. ¡Gracias!

Brock, propietario de la empresa emergente



# Tarea 1: Investigar el entorno del cliente

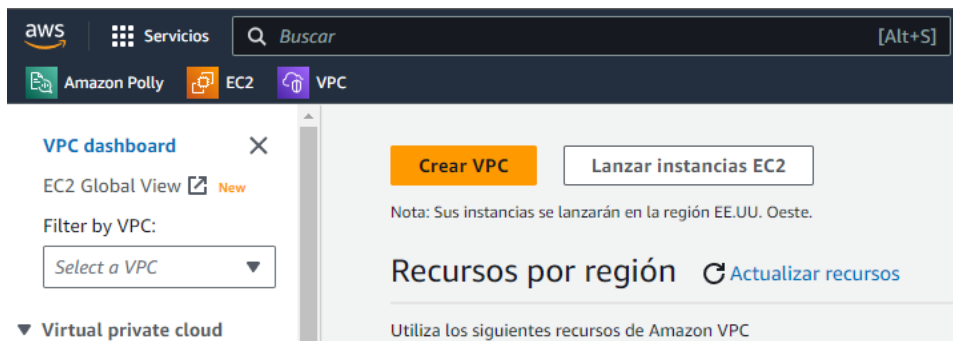
Resumen situación cliente:

- Asistencia para crear y configurar una VPC que tenga conectividad a internet
- Necesita poder hacer *ping* por fuera de la VPC

Componentes de una VPC para que sea compatible con la red:

- **Virtual Private Cloud (VPC)** = Es como un centro de datos, pero en la nube. Está aislada de forma lógica de otras redes virtuales desde las que puede activar y lanzar los recursos de AWS en cuestión de minutos.
- **Direcciones IP privadas** = Son la forma en que se comunican entre sí los recursos dentro de la VPC. Una instancia necesita una dirección IP pública para comunicarse por fuera de la VPC. La VPC necesita recursos de red, como una puerta de enlace de Internet (IGW) y una tabla de enrutamiento, para que la instancia llegue a Internet.
- **Internet Gateway (IGW)** = Es lo que hace posible que la VPC tenga conectividad a Internet. Tiene dos funciones: (1) Hacer la Network Address translation (NAT), (2) Ser el objetivo para dirigir el tráfico a Internet para la VPC. La ruta de una IGW en una tabla de enrutamiento siempre es 0.0.0.0/0.
- **Subnet** = Es un rango de direcciones IP que se encuentra dentro de la VPC.
- **Route Table** = Contiene rutas para la subred y dirige el tráfico mediante las reglas definidas dentro de la tabla de enrutamiento. Asocie la tabla de enrutamiento a una subred. Si una IGW estuviera en una tabla de enrutamiento, el destino sería 0.0.0.0/0 y, el objetivo, IGW.
- **Security Group** = Stateful Firewall dentro de la VPC, lo que significa que bloquean todo de forma predeterminada. Funciona al nivel de la instancia.
- **Network Access Control List (NACL)** = Stateless Firewall dentro de la VPC, lo que significa que no bloquean nada de forma predeterminada. Funcionan al nivel de la subred.

**Paso 1:** Crear una VPC en AWS Management Console → Iniciar asistente de VPC



## Paso 2: Configurar VPC y Crear

### Configuración de la VPC

#### Recursos que se van a crear [Información](#)

Cree únicamente el recurso de VPC o la VPC y otros recursos de red.

☒ Solo la VPC

☐ VPC y más

#### Etiqueta de nombre - *opcional*

Crea una etiqueta con una clave de "Nombre" y el valor que usted especifique.

Test VPC

#### Bloque de CIDR IPv4 [Información](#)

☒ Entrada manual de CIDR IPv4

☐ Bloque de CIDR IPv4 asignado por IPAM

#### CIDR IPv4

192.168.0.0/18

#### Bloque de CIDR IPv6 [Información](#)

☒ Sin bloque de CIDR IPv6

☐ Bloque de CIDR IPv6 asignado por IPAM

☐ Bloque de CIDR IPv6 proporcionado por Amazon

☐ CIDR IPv6 de mi propiedad

#### Tenencia [Información](#)

Predeterminado ▼

Paso 3: Crear Subred pública

▼ Virtual private cloud

Your VPCs [New](#)

Subnets

Acciones ▼

Crear subred

< 1 > ⚙

Crear subred [Información](#)

VPC

ID de la VPC

Cree subredes en esta VPC.

vpc-0709e776d0ec423e6 (Test VPC) ▼

CIDR de VPC asociados

CIDR IPv4

192.168.0.0/18

Configuración de la subred

Especifique los bloques de CIDR y la zona de disponibilidad de la subred.

Subred 1 de 1

Nombre de la subred

Cree una etiqueta con una clave de "Nombre" y el valor que especifique.

Public Subnet

El nombre puede tener un máximo de 256 caracteres.

Zona de disponibilidad [Información](#)

Elija la zona en la que residirá la subred o deje que Amazon elija una por usted.

Sin preferencia ▼

Bloque de CIDR IPv4 [Información](#)

🔍 192.168.1.0/26 ✕

## Paso 4: Crear Route Table (Tabla de enrutamiento)

### ▼ Virtual private cloud

Your VPCs [New](#)

Subnets

**Route tables**

Acciones ▼

Crear tabla de enrutamiento

< 1 > ⚙

## Crear tabla de enrutamiento [Información](#)

Una tabla de enrutamiento especifica cómo se envían los paquetes entre las subredes de la VPC, Internet y la conexión de la VPN.

### Configuración de la tabla de enrutamiento

Nombre - *opcional*

Cree una etiqueta con una clave de "Nombre" y el valor que especifique.

VPC

La VPC que se debe usar para esta tabla de enrutamiento.

## Paso 5: Crear Internet Gateway (IGW)

### ▼ Virtual private cloud

Your VPCs [New](#)

Subnets

Route tables

**Internet gateways**

Acciones ▼

Crear gateway de Internet

< 1 > ⚙

## Crear gateway de Internet [Información](#)

Una gateway de Internet es un router virtual que conecta una VPC a Internet. Para crear una nueva gateway de Internet, especifique el nombre de la gateway a continuación.

### Configuración de gateway de Internet

Etiqueta de nombre

Crea una etiqueta con una clave de "Nombre" y el valor que usted especifique.

**Paso 6:** Asociar la IGW con la VPC → Acciones → Conectar a la VPC

	Name ▾	ID de gateway de Internet ▾	Estado ▾
<input type="checkbox"/>	–	igw-04ae247d03420724c	Attached
<input checked="" type="checkbox"/>	IGW Test VPC	igw-07ce240a6ce557df0	Detached

Acciones ▾

Conectar a la VPC (igw-07ce240a6ce557df0) [Información](#)

VPC

Conecte una gateway de Internet a la VPC para habilitar la comunicación con Internet. Especifique la VPC que desea asociar a continuación.

VPC disponibles

Conecte la gateway de Internet a esta VPC.

vpc-0709e776d0ec423e6

► Comando de la interfaz de línea de comandos de AWS

Cancelar

Conectar gateway de Internet

## Paso 7: Agregar ruta de enrutamiento

- Route Table → Seleccionar la Route table creada → Seleccionar la pestaña “Rutas” → Seleccionar “Editar rutas”
- Destination → 0.0.0.0/0
- Target → IGW Test VPC
- Se le está indicando a la tabla de enrutamiento que cualquier tráfico que necesite conectarse a Internet usará 0.0.0.0/0 para llegar a la IGW y a Internet

Virtual private cloud	Name	ID de tabla de enrutam...
Your VPCs <a href="#">New</a>	–	rtb-0d0db67bad0df1fb1
Subnets	–	rtb-09255ae668117a8d8
<b>Route tables</b>	<input checked="" type="checkbox"/> Public Route Table	rtb-057ad6b5a67fb53e7

**rtb-057ad6b5a67fb53e7 / Public Route Table**

DetallesRutasAsociaciones de subredes

Rutas (1)

Editar rutas

## Editar rutas

Destino	Destino	Estado
192.168.0.0/18	local	✓ Activo
0.0.0.0/0	igw- igw-07ce240a6ce557df0 (IGW Test VPC)	–

Agregar ruta



**Paso 8:** Asociar Subred a la Route Table

- Route Table → Seleccionar la route table creada → Seleccionar la pestaña “Asociaciones de subredes” → Seleccionar “Editar asociaciones de subredes” → Asociar Subred con Route Table.

▼ Virtual private cloud		Name	▼	ID de tabla de enrutam...	▼
Your VPCs <a href="#">New</a>	<input type="checkbox"/>	–		<a href="#">rtb-0d0db67bad0df1fb1</a>	
Subnets	<input type="checkbox"/>	–		<a href="#">rtb-09255ae668117a8d8</a>	
Route tables	<input checked="" type="checkbox"/>	Public Route Table		<a href="#">rtb-057ad6b5a67fb53e7</a>	

rtb-057ad6b5a67fb53e7 / Public Route Table

Detalles

Rutas

Asociaciones de subredes

Editar asociaciones de subredes

Editar asociaciones de subredes

Cambiar las subredes que están asociadas a esta tabla de enrutamiento.

Subredes disponibles (1/1)

Filtrar asociaciones de subredes

<input checked="" type="checkbox"/>	Nombre	▼	ID de subred	▼	CIDR IPv4
<input checked="" type="checkbox"/>	Public Subnet		<a href="#">subnet-0f44d7225565329c5</a>		192.168.1.0/26

Subredes seleccionadas

subnet-0f44d7225565329c5 / Public Subnet

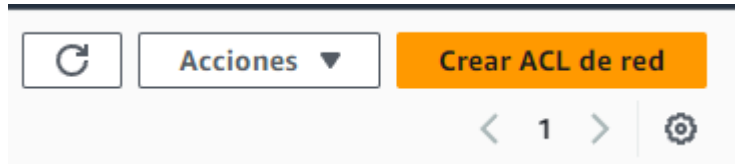
## Paso 9: Crear NACL (Network Access Control List)

- Network ACL → Crear ACL de red

### ▼ Security

Network ACLs

Security groups



Crear la ACL en la VPC creada.

## Crear ACL de red

[Información](#)

Una ACL de red es una capa de seguridad opcional que funciona como un firewall para controlar el tráfico entrante y saliente de una subred.

### Configuración de ACL de red

#### Nombre - *opcional*

Crea una etiqueta con una clave de "Nombre" y el valor que usted especifique.

Test ACL

#### VPC

La VPC que se debe usar para esta ACL de red.

vpc-0709e776d0ec423e6 (Test VPC)

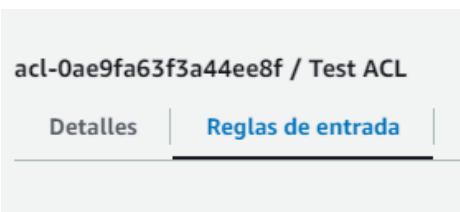
## ACL de red (1/3)

[Información](#)

Find resources by attribute or tag

	Name	ID de ACL de red	Asociada a
<input type="checkbox"/>	–	acl-041fe67bfccf22310	4 Subredes
<input type="checkbox"/>	–	acl-073e1a3432a56cfd9	subnet-0f44d7225565329c5 / Public Subnet
<input checked="" type="checkbox"/>	Test ACL	acl-0ae9fa63f3a44ee8f	–

Ir a la pestaña "Reglas de entrada" para revisar las reglas de entrada de la ACL.



Número de regla 100 = establece que todo el tráfico, todos los protocolos y todos los rangos de puerto desde cualquier fuente (0.0.0.0/0) pueden ingresar (entrar) a la subred.

Número de regla asterisco (\*) = indica que se rechaza todo lo que no coincida con esta regla.

Reglas de entrada (2)		
<input type="text" value="Filter inbound rules"/>		
Número de regla	Tipo	Protocolo
100	Todo el tráfico	Todo
*	Todo el tráfico	Todo

Editar reglas de entrada

< 1 > ⚙

Rango de puertos	Origen	Permitir/denegar
Todo	0.0.0.0/0	✓ Allow
Todo	0.0.0.0/0	✗ Deny

## Paso 10: Crear Security Group (Grupo de seguridad)

- Security Group → Crear Security Group → Configurar Security Group → Detalles Básicos → Reglas de Entrada → Reglas de Salida.

▼ Security

Network ACLs

Security groups

Crear grupo de seguridad

< 1 > ⚙

Crear grupo de seguridad Información

Un grupo de seguridad actúa como un firewall virtual para que la instancia controle el tráfico de entrada.

Detalles básicos

Nombre del grupo de seguridad Información

Public Security Group

El nombre no se puede editar después de su creación.

Descripción Información

Crear grupo de seguridad

URL de consola

11

Para las reglas de entrada (inbound rules), se está permitiendo los tipos de tráfico SSH, HTTP y HTTPS. La fuente desde la que este tráfico llega a la instancia EC2 se puede originar desde cualquier lugar (anywhere).

**Reglas de entrada** [Información](#)

Tipo <a href="#">Información</a>	Protocolo <a href="#">Información</a>	Intervalo de puertos <a href="#">Información</a>	Origen <a href="#">Información</a>
SSH ▼	TCP	22	Anywhere-... ▼ <div>0.0.0.0/0 ✕</div>
HTTP ▼	TCP	80	Anywhere-... ▼ <div>0.0.0.0/0 ✕</div>
HTTPS ▼	TCP	443	Anywhere-... ▼ <div>0.0.0.0/0 ✕</div>

Para las reglas de salida (outbound rules), se está permitiendo todo el tráfico hacia afuera de la instancia EC2.

**Reglas de salida** [Información](#)

Tipo <a href="#">Información</a>	Protocolo <a href="#">Información</a>	Intervalo de puertos <a href="#">Información</a>	Destino <a href="#">Información</a>
Todo el tráfico ▼	Todo	Todo	Personaliz... ▼ <div>0.0.0.0/0 ✕</div>

Todos los pasos anteriores permiten tener una VPC funcional

# Tarea 2: lanzar la instancia EC2 y establecer una conexión SSH con la instancia

## Paso 1: Nombrar la instancia EC2

**Lanzar la instancia**  
Para comenzar, lance una instancia en la consola de la nube.

**Nombre y etiquetas** [Información](#)

**Nombre**

**Lanzar la instancia** ▼

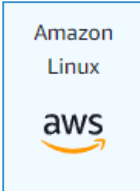
Test Instance

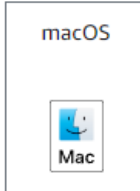
## Paso 2: Elegir una AMI


**▼ Imágenes de aplicaciones y sistemas operativos (Amazon Machine Image)** [Información](#)

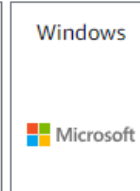
Una AMI es una plantilla que contiene la configuración de software (sistema operativo, servidor de aplicaciones y aplicaciones) necesaria para lanzar la instancia. Busque o examine las AMI si no ve lo que busca a continuación.


**Inicio rápido**


**Amazon Linux**


**macOS**

**Ubuntu**

**Windows**

**Red Hat**

**SUSE Linux**

  
**Buscar más AMI**  
Inclusión de AMI de AWS, Marketplace y la comunidad

**Amazon Machine Image (AMI)**

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type  
ami-0be50262c078dfea9 (64 bits (x86)) / ami-042eeed13706023b (64 bits (Arm))  
Virtualización: hvm    Habilitado para ENA: true    Tipo de dispositivo raíz: ebs

Apto para la capa gratuita ▼

**Descripción**

Amazon Linux 2 Kernel 5.10 AMI 2.0.20230906.0 x86\_64 HVM gp2

**Arquitectura**  
64 bits (x86) ▼

**ID de AMI**  
ami-0be50262c078dfea9

**Proveedor verificado**

### Paso 3: Elegir el tipo de instancia

▼ Tipo de instancia

Información

Tipo de instancia

t2.micro

Apto para la capa gratuita

Familia: t2 1 vCPU 1 GiB Memoria Generación actual: true

Bajo demanda Linux base precios: 0.0116 USD por hora

Bajo demanda SUSE base precios: 0.0116 USD por hora

Bajo demanda Windows base precios: 0.0162 USD por hora

Bajo demanda RHEL base precios: 0.0716 USD por hora

Additional costs apply for AMIs with pre-installed software

### Paso 4: Configurar un par de claves

▼ Par de claves (inicio de sesión)

Información

Puede utilizar un par de claves para conectarse de forma segura a la instancia. Asegúrese de claves seleccionado antes de lanzar la instancia.

Nombre del par de claves - obligatorio

vockey

### Paso 5: Configurar los ajustes de red

- Seleccionar Test VPC, Public Subnet y Public Security Group creados anteriormente

▼ Configuraciones de red

Información

VPC - obligatorio

vpc-0709e776d0ec423e6 (Test VPC)

192.168.0.0/18

Subred

subnet-0f44d7225565329c5

Public Subnet

VPC: vpc-0709e776d0ec423e6 Propietario: 948427900900

Zona de disponibilidad: us-west-2b Direcciones IP disponibles: 59

CIDR: 192.168.1.0/26

Asignar automáticamente la IP pública

Habilitar

Firewall (grupos de seguridad)

Información

Un grupo de seguridad es un conjunto de reglas de firewall que controlan el tráfico de la instancia. Agr tráfico específico llegue a la instancia.

☐ Crear grupo de seguridad

☒ Seleccionar un grupo de seguridad existente

Grupos de seguridad comunes

Seleccionar grupos de seguridad

Public Security Group sg-08e1c83a2202d4f34

VPC: vpc-0709e776d0ec423e6

Los grupos de seguridad que agrega o elimine aquí se agregarán a todas las interfaces de red o se elim

## Paso 6: Agregar Almacenamiento

**▼ Configurar almacenamiento** [Información](#)

1x

GiB

▼

Volumen raíz (Sin cifrar)

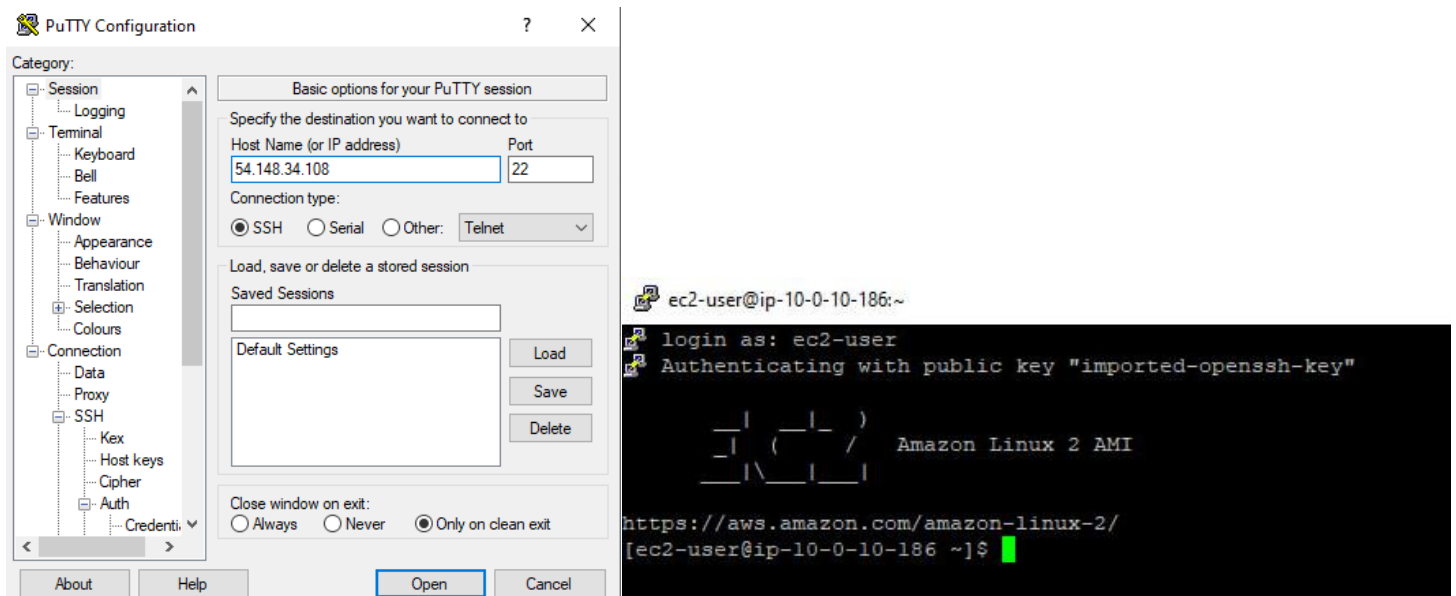
## Paso 7: Lanzar instancia EC2

<input checked="" type="checkbox"/>	Test Instance	i-0a9cf6839a8ada5eb	<input checked="" type="checkbox"/> En ejecución 🔍	t2.micro
-------------------------------------	---------------	---------------------	--	----------

## Paso 2: Elegir una AMI

Para establecer una conexión SSH con la instancia EC2:

1. Abrir Putty.exe: Se ingresa dirección IPv4 de la instancia EC2 en la sección Session.
2. En la sección Connection → SSH → Auth → Credentials se ingresa el archivo PPK descargado anteriormente.
3. En la sección Connection se establece **Seconds between keepalive en 30** (el valor predeterminado es 0).
4. Se hace click en “Open” para validar y conectarse al Host.



## Tarea 3: Usar el ping para probar la conectividad a Internet

ping = herramienta de diagnóstico de red que se utiliza para comprobar la conectividad entre dos dispositivos. Envía paquetes de datos a un dispositivo remoto y mide el tiempo que tardan en regresar.

- Funciona enviando un paquete de datos ICMP (Internet Control Message Protocol) al dispositivo remoto. El paquete ICMP contiene una solicitud de echo. El dispositivo remoto responde con un paquete de datos ICMP que contiene una respuesta de echo.
- También se puede utilizar para comprobar si un dispositivo remoto está disponible.

 ec2-user@ip-192-168-1-46:~

```
[ec2-user@ip-192-168-1-46 ~]$ ping google.com
PING google.com (142.250.69.206) 56(84) bytes of data.
64 bytes from sea30s08-in-fl4.1e100.net (142.250.69.206): icmp_seq=1 ttl=37 time=6.54 ms
64 bytes from sea30s08-in-fl4.1e100.net (142.250.69.206): icmp_seq=2 ttl=37 time=6.59 ms
64 bytes from sea30s08-in-fl4.1e100.net (142.250.69.206): icmp_seq=3 ttl=37 time=6.63 ms
64 bytes from sea30s08-in-fl4.1e100.net (142.250.69.206): icmp_seq=4 ttl=37 time=6.61 ms
64 bytes from sea30s08-in-fl4.1e100.net (142.250.69.206): icmp_seq=5 ttl=37 time=6.68 ms
64 bytes from sea30s08-in-fl4.1e100.net (142.250.69.206): icmp_seq=6 ttl=37 time=6.80 ms
64 bytes from sea30s08-in-fl4.1e100.net (142.250.69.206): icmp_seq=7 ttl=37 time=6.74 ms
64 bytes from sea30s08-in-fl4.1e100.net (142.250.69.206): icmp_seq=8 ttl=37 time=6.60 ms
64 bytes from sea30s08-in-fl4.1e100.net (142.250.69.206): icmp_seq=9 ttl=37 time=6.63 ms
64 bytes from sea30s08-in-fl4.1e100.net (142.250.69.206): icmp_seq=10 ttl=37 time=6.60 ms
64 bytes from sea30s08-in-fl4.1e100.net (142.250.69.206): icmp_seq=11 ttl=37 time=6.87 ms
^C
--- google.com ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10017ms
rtt min/avg/max/mdev = 6.546/6.666/6.872/0.141 ms
[ec2-user@ip-192-168-1-46 ~]$
```

Se verifica que la instancia EC2 creada dentro de la VPC de prueba está conectada al internet utilizando como prueba el comando ping que cliente solicitaba tener funcional.

## Laboratorio Completado