

Datos Generales:

Nombre: Tomás Alfredo Villaseca Constantinescu

País: Chile

Fecha: 06/11/2023

Contacto: tomas.villaseca.c@gmail.com

Al final de este laboratorio, usted debe ser capaz de hacer lo siguiente:

- Crear una VPC con una subred privada y una pública, una puerta de enlace a Internet y una puerta de enlace NAT.
- Configurar tablas de rutas asociadas con subredes para tráfico local y de Internet mediante una puerta de enlace de Internet y una puerta de enlace NAT.
- Poner en marcha un servidor bastión en una subred pública.
- Utilice un servidor bastión para iniciar sesión en una instancia de una subred privada.

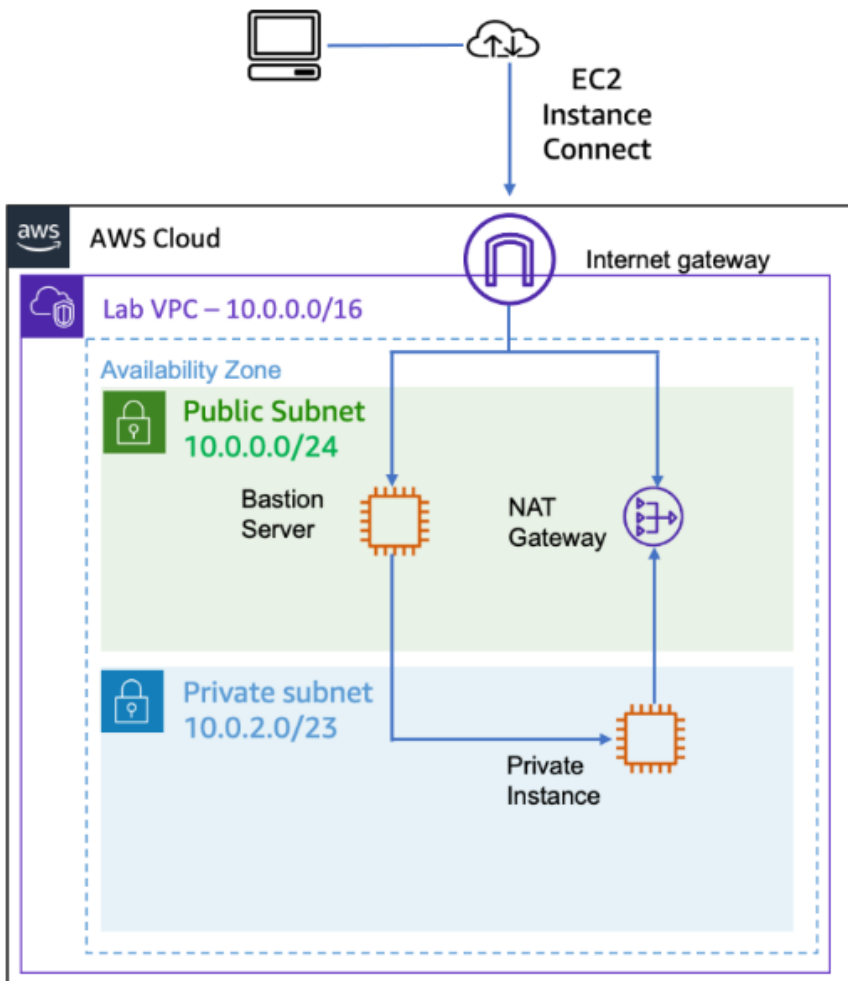
Resumen Laboratorio:

Amazon Virtual Private Cloud (VPC) ofrece la posibilidad de aprovisionar una sección lógicamente aislada de la nube de AWS en la que puede lanzar recursos de AWS en una red virtual definida por usted.

Usted tiene el control completo sobre su entorno de red virtual, incluyendo la selección de sus rangos de direcciones IP, la creación de subredes, y la configuración de tablas de rutas y puertas de enlace de red.

En este laboratorio, creará una (VPC) y otros componentes de red necesarios para implementar recursos, como una instancia de Amazon EC2.

Arquitectura Final:



Public Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Internet Gateway

Private Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	NAT Gateway

Tarea 1: Crear una VPC

Paso 1: VPC → Your VPCs

- Default VPC → En cada región, ya se ha creado una VPC predeterminada con un bloque CIDR de 172.31.0.0/16 para usted.

<input checked="" type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR
<input checked="" type="checkbox"/>	-	vpc-029a475d6b2924bfe	Available	172.31.0.0/16

Paso 2: VPC → Your VPCs → Create VPC

- Resources to create → VPC only

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

☒ VPC only

☐ VPC and more

- Name tag = Lab VPC

Name tag - *optional*

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

Lab VPC

- IPv4 CIDR block → IPv4 CIDR manual input
- IPv4 CIDR → 10.0.0.0/16
- IPv6 CIDR block → No IPv6 CIDR block
- Tenancy → Default

IPv4 CIDR block [Info](#)

- ☒ IPv4 CIDR manual input
☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

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

Tenancy [Info](#)

Default

	Name	VPC ID	State	IPv4 CIDR
<input checked="" type="checkbox"/>	Lab VPC	vpc-0fe72ff8017dc8aeb	Available	10.0.0.0/16

Paso 3: VPC → Lab VPC → Actions → Edit VPC Settings

- DNS settings → Enable DNS hostnames

Actions ▲

Create flow log

Edit VPC settings

DNS settings

☒ Enable DNS resolution [Info](#)

☒ Enable DNS hostnames [Info](#)

Las instancias EC2 lanzadas en la VPC ahora reciben automáticamente un nombre de host público IPv4 DNS.



En esta tarea, se creará una subred pública y una subred privada.

Tarea 2.1 – Crear una subred pública

Paso 1: VPC → Subnets → Create subnet

- VPC ID → Lab VPC

VPC ID

Create subnets in this VPC.

- Subnet name = Public 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 → us-west-2a

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.


US West (Oregon) / us-west-2a

- IPv4 CIDR block → 10.0.0.0/24

IPv4 subnet CIDR block


10.0.0.0/24

256 IPs

<input checked="" type="checkbox"/>	Name	Subnet ID	State
<input checked="" type="checkbox"/>	Public Subnet	subnet-0ab2963360895931e	 Available

Paso 2: VPC → Subnets → Public Subnet → Actions → Edit subnet settings

- Auto-assign IP settings → Enable auto-assign public IPv4 address.



Actions ▲

Create subnet

View details

Create flow log

Edit subnet settings

Auto-assign IP settings [Info](#)

Enable the auto-assign IP settings to automatically request

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

Tarea 2.2 – Crear una subred privada

Paso 1: VPC → Subnets → Create subnet

- VPC ID → Lab VPC

VPC ID

Create subnets in this VPC.

vpc-0fe72ff8017dc8aeb (Lab VPC)

- Subnet name = Private Subnet

Subnet name

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

Private Subnet

The name can be up to 256 characters long.

- Availability Zone → us-west-2a

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US West (Oregon) / us-west-2a

- IPv4 CIDR block → 10.0.2.0/24

IPv4 subnet CIDR block

10.0.2.0/24

256 IPs

<input checked="" type="checkbox"/>	Name	Subnet ID	State
<input checked="" type="checkbox"/>	Private Subnet	subnet-0ffc3edc0b3e79ea6	Available

Tarea 3: Crear una puerta de enlace de Internet

En esta tarea, creará una puerta de enlace a Internet para su VPC. Necesita una puerta de enlace a Internet para establecer conectividad externa con instancias EC2 en su VPC.

Paso 1: VPC → Internet Gateways → Create internet gateway

- Name = Lab IGW

Name tag

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

Lab IGW

Paso 2: VPC → Internet Gateways → Lab IGW → Actions → Attach to a VPC

- VPC → Lab VPC
-

Available VPCs

Attach the internet gateway to this VPC.

Select a VPC

vpc-0fe72ff8017dc8aeb - Lab VPC

<input checked="" type="checkbox"/>	Name	Internet gateway ID	State
<input checked="" type="checkbox"/>	Lab IGW	igw-0e2cb2abe3458660c	Attached

Tarea 4: Configurar tablas de enrutamiento

En esta tarea realizará lo siguiente:

- Crear una tabla de rutas pública para el tráfico que se dirige a Internet.
- Añadir una ruta a la tabla de rutas para dirigir el tráfico de Internet a la puerta de enlace de Internet.
- Asociar la subred pública con la nueva tabla de rutas.

Paso 1: VPC → Route tables

- Seleccionar la Route table que tiene Lab VPC en la columna VPC

Route table ID	Explicit subnet associati...	Edge associations	Main	VPC
rtb-06f1528c874ae24db	–	–	Yes	vpc-0fe72ff8017dc8aeb Lab VPC

Paso 2: VPC → Route tables → Route table → Name → Edit name

- Name = Private Route Table

	Name	Route table ID
<input checked="" type="checkbox"/>	Private Route Table	rtb-06f1528c874ae24db

Paso 3: VPC → Route tables → Private Route Table → Routes

- Actualmente sólo hay una ruta. Muestra que todo el tráfico destinado a 10.0.0.0/16 (que es el rango de la VPC de Laboratorio) será enrutado localmente. Esta opción permite que todas las subredes de una VPC se comuniquen entre sí.

Routes	Subnet associations	Edge associations	Route propagation	Tags
Routes (1)				
<input type="text" value="Filter routes"/>				
Destination	Target	Status		
10.0.0.0/16	local	Active		

Paso 4: VPC → Route tables → Create Route table

- Name = Public Route Table
- VPC → Lab VPC

Name - *optional*

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

Public Route Table

VPC

The VPC to use for this route table.

vpc-0fe72ff8017dc8aeb (Lab VPC)

Paso 5: VPC → Route tables → Public Route Table → Routes → Edit routes

- Add route
- Destination → 0.0.0.0/0
- Target → Internet Gateway → Lab IGW

Destination	Target	Status
0.0.0.0/0	igw-0e2cb2abe3458660c	✓ Active

Paso 6: VPC → Route tables → Public Route Table → Subnet associations → Edit subnet associations

- Seleccionar Public Subnet

Explicit subnet associations (1)

Find subnet association

Name	Subnet ID	IPv4 CIDR
Public Subnet	subnet-0ab2963360895931e	10.0.0.0/24

	Name	Route table ID	Explicit subnet associati...
✓	Public Route Table	rtb-0c829de5674df1ff0	subnet-0ab29633608959...

Public Subnet es ahora pública porque tiene una entrada en la tabla de rutas que envía tráfico a Internet a través del internet gateway.

Tarea 5: Lanzar un servidor bastión en la subred pública

Un Bastion Server es una instancia de EC2 en una subred pública que está configurada de forma segura para proporcionar acceso a recursos en una subred privada. Los operadores de sistemas pueden conectarse al servidor bastión y, a continuación, saltar a los recursos de la subred privada.

En esta tarea, se lanzará un Bastion Server de instancia EC2 en la subred pública que se creó anteriormente.

Paso 1: EC2 → Instances → Launch instances

Launch instances ▼

Paso 2: Launch instances → Settings

- Name and tags = Bastion Server

Name

Bastion Server

- AMI → Amazon Linux 2023 AMI

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

ami-00448a337adc93c05 (64-bit (x86)) / ami-0aa3a6456e181ec3b (64-bit (Arm))

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

- Instance type → t3.micro

Instance type

t3.micro

Family: t3 2 vCPU 1 GiB Memory Current generation: true

On-Demand SUSE base pricing: 0.0104 USD per Hour

On-Demand Windows base pricing: 0.0196 USD per Hour

On-Demand RHEL base pricing: 0.0704 USD per Hour

On-Demand Linux base pricing: 0.0104 USD per Hour

- Key pair (login) → Proceed without a key pair (not recommended)

Key pair name - *required*

Proceed without a key pair (Not recommended)

Default value ▼

Paso 3: Launch instances → Network Settings

- VPC → Lab VPC
- Subnet → Public Subnet
- Auto-assign public IP → Enable
- Security groups → Create security group
- SG name = Bastion Security Group
- SG Description = Allow SSH
- Inbound SG rules → Type: SSH / Source type: Anywhere

VPC - required [Info](#)

vpc-0fe72ff8017dc8aeb (Lab VPC)

▼

10.0.0.0/16

↺

Subnet [Info](#)

subnet-0ab2963360895931e

Public Subnet

▼

VPC: vpc-0fe72ff8017dc8aeb Owner: 166157653710 Availability Zone: us-west-2a
IP addresses available: 251 CIDR: 10.0.0.0/24

↺

[Create new subnet](#)

Auto-assign public IP [Info](#)

Enable

▼

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

Bastion Security Group

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](#)

Allow SSH

Inbound Security Group Rules

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

Remove

Type [Info](#)

ssh

▼

Protocol [Info](#)

TCP

Port range [Info](#)

22

Source type [Info](#)

Anywhere

▼

Source [Info](#)

🔍 Add CIDR, prefix list or security

Description - optional [Info](#)

e.g. SSH for admin desktop

Paso 4: Launch instances → Launch

<input checked="" type="checkbox"/>	Name ✎ ▼	Instance ID	Instance state ▼	Instance type ▼
<input checked="" type="checkbox"/>	Bastion Server	i-0434f07d30a92082c	<div>✔ Running</div> 🔍 🔍	t3.micro

Tarea 6: Crear una puerta de enlace de NAT

En esta tarea, se lanzará una NAT Gateway en la subred pública y se configurará la tabla de rutas privada para facilitar la comunicación entre los recursos de la subred privada e Internet.

Paso 1: VPC → NAT Gateways → Create NAT gateway

- Name = Lab NAT Gateway
- Subnet → Public Subnet
- Allocate Elastic IP

NAT gateway settings

Name - optional

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

The name can be up to 256 characters long.

Subnet

Select a subnet in which to create the NAT gateway.

Connectivity type

Select a connectivity type for the NAT gateway.

- ☒ Public
- ☐ Private

Elastic IP allocation ID [Info](#)

Assign an Elastic IP address to the NAT gateway.

Allocate Elastic IP

	Name ▾	NAT gateway ID ▾	Connectivit... ▾
<input checked="" type="radio"/>	Lab NAT Gateway	nat-044e74b9a0a6456d7	Public

Paso 2: VPC → Route Tables → Private Route Table → Routes → Edit routes

- Add route
- Destination → 0.0.0.0/0
- Target → NAT Gateway → Lab NAT Gateway

Destination ▾	Target ▾	Status
0.0.0.0/0	nat-044e74b9a0a6456d7	✓ Active

Tarea 7: Probar la subred privada

En esta tarea, lanzará una instancia EC2 en la Private Subnet y verificará que se puede conectar a internet.

Tarea 7.1 – Crear una instancia EC2 en la Private Subnet

Paso 1: EC2 → Instances → Launch instances

Launch instances

Paso 2: Launch instances → Settings

- Name and tags = Private Instance

Name

Private Instance

- AMI → Amazon Linux 2023 AMI

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

ami-00448a337adc93c05 (64-bit (x86)) / ami-0aa3a6456e181ec3b (64-bit (Arm))

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

- Instance type → t3.micro

Instance type

t3.micro

Family: t3 2 vCPU 1 GiB Memory Current generation: true

On-Demand SUSE base pricing: 0.0104 USD per Hour

On-Demand Windows base pricing: 0.0196 USD per Hour

On-Demand RHEL base pricing: 0.0704 USD per Hour

On-Demand Linux base pricing: 0.0104 USD per Hour

- Key pair (login) → Proceed without a key pair (not recommended)

Key pair name - *required*

Proceed without a key pair (Not recommended)

Default value ▼

Paso 3: Launch instances → Network Settings

- VPC → Lab VPC
- Subnet → Private Subnet
- Security groups → Create security group
- SG name = Private Instance SG
- SG Description = Allow SSH from Bastion
- Inbound SG rules → Type: SSH / Source type: 10.0.0.0/16

VPC - *required* [Info](#)

vpc-0fe72ff8017dc8aeb (Lab VPC)
10.0.0.0/16



Subnet [Info](#)

subnet-0ffc3edc0b3e79ea6 Private Subnet
VPC: vpc-0fe72ff8017dc8aeb Owner: 166157653710 Availability Zone: us-west-2a
IP addresses available: 251 CIDR: 10.0.2.0/24



[Create new subnet](#)

Auto-assign public IP [Info](#)

Disable

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*

Private Instance SG

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](#)

Allow SSH from Bastion Server

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 10.0.0.0/16)

Remove

Type [Info](#)

ssh

Protocol [Info](#)

TCP

Port range [Info](#)

22

Source type [Info](#)

Custom

Source [Info](#)

🔍 Add CIDR, prefix list or security

10.0.0.0/16 ✕

Description - *optional* [Info](#)


e.g. SSH for admin desktop

Paso 3: Launch instances → Advanced details → User data

```
#!/bin/bash
# Turn on password authentication for lab challenge
echo 'lab-password' | passwd ec2-user --stdin
sed -i 's|[#]*PasswordAuthentication no|PasswordAuthentication yes|g' /etc/ssh/sshd_config
systemctl restart sshd.service
```

User data - *optional* | [Info](#)







Upload a file with your user data or enter it in the field.

 Choose file

```
#!/bin/bash
# Turn on password authentication for lab challenge
echo 'lab-password' | passwd ec2-user --stdin
sed -i 's|[#]*PasswordAuthentication no|PasswordAuthentication yes|g'
/etc/ssh/sshd_config
systemctl restart sshd.service
```

Este script permite iniciar sesión utilizando una contraseña. Se incluye para ayudar a acortar los pasos del laboratorio, pero no se recomienda para despliegues de instancias normales.

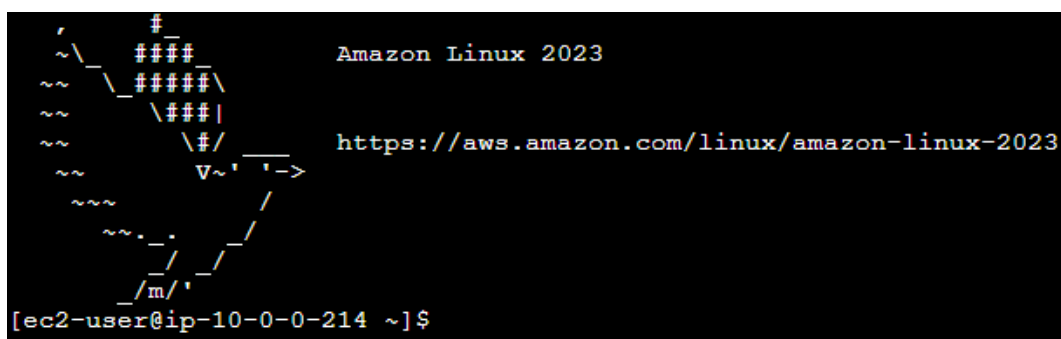
Paso 4: Launch instances → Launch

	Name 	Instance ID	Instance state 
<input checked="" type="checkbox"/>	Private Instance	i-0a0aa3898aa7b51ec	 Running  

Tarea 7.2 – Conectarse al Bastion Server

La instancia que acaba de lanzar se encuentra en la subred privada, por lo que no es posible iniciar sesión directamente en la instancia. En su lugar, primero debe iniciar sesión en el servidor bastión de la subred pública y, a continuación, iniciar sesión en la instancia privada desde el servidor bastión.

Paso 1: EC2 → Instances → Bastion Server → Connect



```
~\_#####_ Amazon Linux 2023
~~~\#####\
~~~\####|
~~~\#/ https://aws.amazon.com/linux/amazon-linux-2023
~~~v~' '->
~~~
~~~.-.-.-.-.-
~~~/_m/'
[ec2-user@ip-10-0-0-214 ~]$
```

Tarea 7.3 – Conectarse a Private Instance

Paso 1: EC2 → Instances → Private Instance

Private IPv4 addresses

- Private IPv4 address → 10.0.2.208

10.0.2.208

Paso 2: Ingresar el siguiente comando en el terminal de Bastion Server para conectarse a la Private Instance:

ssh PRIVATE-IP

- Reemplazar “PRIVATE-IP” por Private IPv4 address copiado anteriormente.
- Password = lab-password

[illegible]

Tarea 7.4 – Testear la NAT Gateway

Paso 1: Ingresar el siguiente comando para probar la conexión a internet de Private Instance:

```
ping -c 3 amazon.com
```

```
[ec2-user@ip-10-0-2-208 ~]$ ping -c 3 amazon.com
PING amazon.com (205.251.242.103) 56(84) bytes of data.
64 bytes from s3-console-us-standard.console.aws.amazon.com (205.251.242.103): icmp_seq=1 ttl=220 time=60.6 ms
64 bytes from s3-console-us-standard.console.aws.amazon.com (205.251.242.103): icmp_seq=2 ttl=220 time=59.9 ms
64 bytes from s3-console-us-standard.console.aws.amazon.com (205.251.242.103): icmp_seq=3 ttl=220 time=59.9 ms

--- amazon.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 59.920/60.152/60.612/0.324 ms
[ec2-user@ip-10-0-2-208 ~]$
```

El output indica que Private Instance se ha comunicado con éxito con amazon.com en Internet.

La instancia privada está en la subred privada, y la única manera de que esto sea posible en el escenario actual es pasando a través de la NAT Gateway.

A horizontal banner with a dark blue background featuring a network of glowing blue nodes and lines. The text "Laboratorio Completado" is centered in a white, sans-serif font.

Laboratorio Completado

