



172- [JAWS] - Lab - [Reto]

Ejercicio de instancia EC2

Datos Generales:

Nombre: Tomás Alfredo Villaseca Constantinescu

País: Chile

Fecha: 20/10/2023

Contacto: tomas.villaseca.c@gmail.com

Después de completar este desafío, usted podrá ser capaz de hacer lo siguiente:

- Configurar una red virtual.
- Colocar una instancia de Amazon Linux EC2 en esta red virtual.
- Instalar un servidor web y desplegar y ejecutar una aplicación sencilla en él.

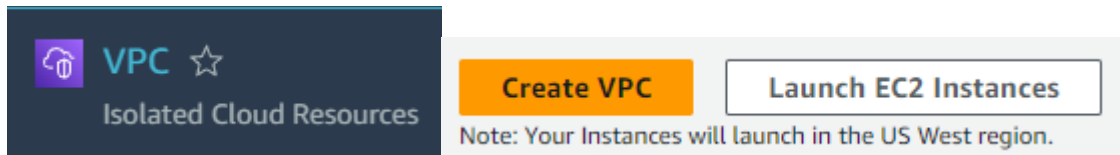
Desafío

En este desafío de laboratorio, aplicará lo que ha aprendido hasta ahora sobre Amazon EC2.

Seguirá algunos pasos de alto nivel para crear una aplicación web que se ejecute en una instancia EC2 de Amazon Linux.

Desafío 1.1 – Crear VPC para poder lanzar una Instancia EC2 Web Server.

Paso 1: AWS Management Console → Search → VPC → Create VPC



Paso 2: Create VPC → VPC Settings

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

☐ VPC only ☒ VPC and more

Name tag auto-generation [Info](#)
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☒ Auto-generate
Lab VPC

Number of Availability Zones (AZs) [Info](#)
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1 2 3

► **Customize AZs**

Number of public subnets [Info](#)
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0 1

Number of private subnets [Info](#)
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0 1 2

IPv4 CIDR block [Info](#)
Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16 65,536 IPs

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

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block ☐ Amazon-provided IPv6 CIDR block

Tenancy [Info](#)

Default

▼ **Customize subnets CIDR blocks**

Public subnet CIDR block in us-west-2a

10.0.0.0/24 256 IPs

NAT gateways (\$) [Info](#)
Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway.

None In 1 AZ 1 per AZ

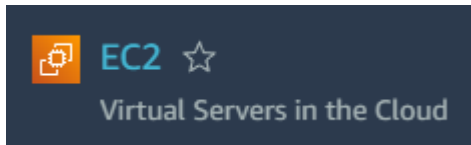
VPC endpoints [Info](#)
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None S3 Gateway

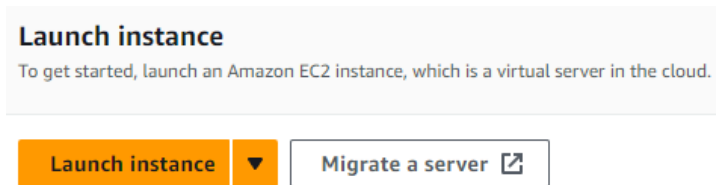
	Name	VPC ID	State	IPv4 CIDR
<input type="checkbox"/>	–	vpc-0555ed4a99e11dfe2	Available	172.31.0.0/16
<input checked="" type="checkbox"/>	Lab VPC-vpc	vpc-0f43a8887c122a518	Available	10.0.0.0/16

Desafío 1.2 – Crear una instancia EC2 para ejecutar una aplicación web.

Paso 1: AWS Management Console → Search → EC2



Paso 2: EC2 → Launch Instance



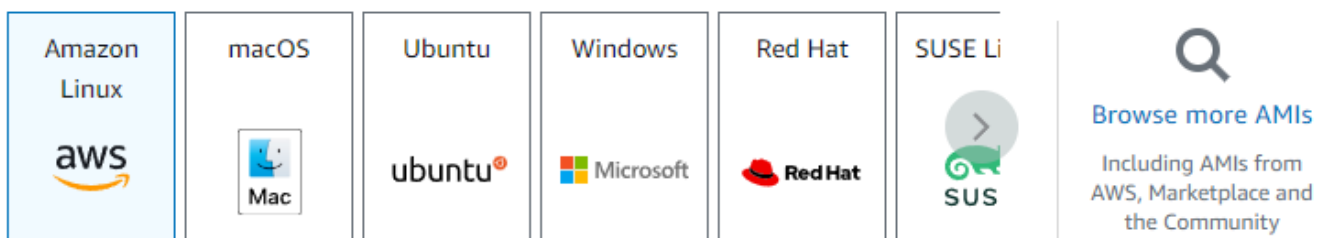
Paso 3: Launch Instance → Name and Tags

- Name = Web Server

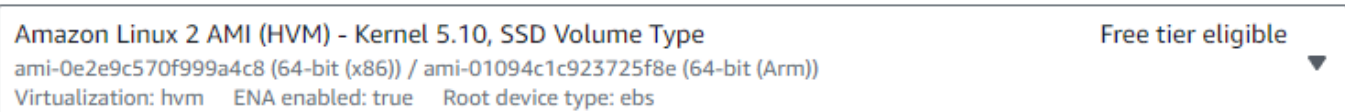
Name

Paso 4: Launch Instance → Choose an AMI

- Seleccionar Amazon Linux 2



Amazon Machine Image (AMI)



Paso 5: Launch Instance → Instance Type

- Instance type → t3.micro

▼ Instance type [Info](#)

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

▼

☒ All generations
[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

Paso 6: Launch Instance → Key Pair

- Proceed without key pair (not recommended)

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Proceed without a key pair (Not recommended) Default value ▼

[Create new key pair](#)

Paso 7: Launch Instance → Configure Network Settings

- VPC → Lab VPC
- Subnet → Default
- Seleccionar “Enable” para “Auto-assign Public IP”
- Security Groups → Create Security Group
- Security Group Name = Bastion Security Group
- Description = Permit HTTP, HTTPS, and SSH connections.

▼ Network settings [Info](#)

VPC - *required* [Info](#)

vpc-0e6dc984abeba7630 (Lab VPC)
10.0.0.0/16

▼

Subnet [Info](#)

subnet-0c6cd623e778f5b2a Public Subnet
VPC: vpc-0e6dc984abeba7630 Owner: 021502630162
Availability Zone: us-west-2a IP addresses available: 250 CIDR: 10.0.0.0/24

▼

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*

Web 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](#)

Permit HTTP, HTTPS, and SSH connections.

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

▼ Security group rule 2 (TCP, 443, 0.0.0.0/0)

Remove

Type [Info](#)

HTTPS

Protocol [Info](#)

TCP

Port range [Info](#)

443

Source type [Info](#)

Anywhere

Source [Info](#)

🔍 Add CIDR, prefix list or security

Description - *optional* [Info](#)

e.g. SSH for admin desktop

▼ Security group rule 3 (TCP, 80, 0.0.0.0/0)

Remove

Type [Info](#)

HTTP

Protocol [Info](#)

TCP

Port range [Info](#)

80

Source type [Info](#)

Anywhere

Source [Info](#)

🔍 Add CIDR, prefix list or security

Description - *optional* [Info](#)

e.g. SSH for admin desktop

Paso 8: Launch Instance → Add storage

- Configure Storage → Default

▼ Configure storage [Info](#)


1x GiB ▼ Root volume (Not encrypted)

Paso 9: Launch Instance → Advanced Details

- User Data → instala e inicia el servicio httpd como tu servidor web. Conceder permisos de escritura a los usuarios en el directorio raíz de documentos del servidor web (/var/www/html).

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

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

 Choose file




```
#!/bin/bash

# Install the httpd service
yum install -y httpd

# Start the httpd service
systemctl start httpd

# Set the permissions on the web server's document root directory
chmod 775 /var/www/html
```




Paso 10: Launch Instance → Launch

Instances (1/1) Info				
<input type="text" value="Find instance by attribute or tag (case-sensitive)"/>				
<input checked="" type="checkbox"/>	Name ▼	Instance ID	Instance state ▼	Instance type ▼
<input checked="" type="checkbox"/>	Web Server	i-0e4f5abe9a534c963	 Running  	t3.micro

Desafi  1.3 – Probar Web Server.

Paso 1: EC2 → Instances → Web Server → Connect

Instances (1/1) [Info](#)

<input checked="" type="checkbox"/>	Name ▾	Instance ID	Instance state ▾	Instance type ▾	Status check	Alarm status	Availability Zone ▾	Public IP address
<input checked="" type="checkbox"/>	Web Server	i-0e4f5abe9a534c963	Running  	t3.micro	2/2 checks passed	No alarms 	us-west-2a	ec2-18-246-208-147.us-west-2.compute.amazonaws.com

Connect to instance [Info](#)

Connect to your instance i-0e4f5abe9a534c963 (Web Server) using any of these options


EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID


 i-0e4f5abe9a534c963 (Web Server)

Connection Type

☒ Connect using EC2 Instance Connect
 Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.


☐ Connect using EC2 Instance Connect Endpoint
 Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IP address

 18.246.208.147

User name

Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user.

 **Note:** In most cases, the default user name, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Cancel

Connect

```
#
~\##### Amazon Linux 2
~~~\#####
~~~\####| AL2 End of Life is 2025-06-30.
~~~~\#/
~~~~V~'-'>
~~~~
~~~~./
~/m/'-'
```

A newer version of Amazon Linux is available!

Amazon Linux 2023, GA and supported until 2028-03-15.
<https://aws.amazon.com/linux/amazon-linux-2023/>

11 package(s) needed for security, out of 11 available
Run "sudo yum update" to apply all updates.

[ec2-user@ip-10-0-9-66 ~]\$

Paso 2: Crear un archivo de texto con el comando **touch**.

```
[ec2-user@ip-10-0-9-66 ~]$ touch web.html
[ec2-user@ip-10-0-9-66 ~]$ ls
web.html
[ec2-user@ip-10-0-9-66 ~]$
```

Paso 3: Editar el documento de texto con **nano** y copiar el siguiente código HTML:

```
<!DOCTYPE html>
<html>
<body>
<h1>YOUR-NAME's re/Start Project Work</h1>
<p>EC2 Instance Challenge Lab</p>
</body>
</html>
```

```
GNU nano 2.9.8

<!DOCTYPE html>
<html>
<body>
<h1>TomasVC re/Start Project Work</h1>
<p>EC2 Instance Challenge Lab</p>
</body>
</html>
```

Paso 4: Mover archivo HTML al directorio `var/www/html`

```
[ec2-user@ip-10-0-9-66 ~]$ sudo mv web.html /var/www/html
[ec2-user@ip-10-0-9-66 ~]$ ls /var/www/html
web.html
[ec2-user@ip-10-0-9-66 ~]$
```

Paso 5: Abrir un navegador web e ingresar el Public IPv4 Address de Web Server para acceder al sitio.



is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.

a member of the general public:

at you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing ntenance.

d like to let the administrators of this website know that you've seen this page instead of the page you expected, you d them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the : person.

e, if you experienced problems while visiting www.example.com, you should send e-mail to r@example.com".

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. I and not your content. To prevent this page from ever being

You are free to use the image below on web sites powered



Laboratorio Completado

