

Paso 1 — Crear una instancia EC2

Creamos una instancia y la configuramos de la siguiente manera:

Nombre y etiquetas

Nombre

Practica-HTTPS

Agregar etiquetas adicionales

▼ Imágenes de aplicaciones y sistemas operativos (Imagen de máquina de Amazon)

Una AMI posee el sistema operativo, el servidor de aplicaciones y las aplicaciones de la instancia. Si a continuación no ve una AMI adecuada, utilice el campo de búsqueda o elija [Buscar más AMI](#).

Q

Busque en nuestro catálogo completo que incluye miles de imágenes de sistemas operativos y aplicaciones

Inicio rápido

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE Linux

Debian

Buscar más AMI

Inclusión de AMI de AWS, Marketplace y la comunidad

Imágenes de máquina de Amazon (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
ami-0360c520857e3138f (64 bits (x86)) / ami-026fcd88-446aa0bf (64 bits (Arm))
Virtualización: hvm Activado para ENA: true Tipo de dispositivo raíz: ebs

Apto para la capa gratuita

Descripción

Ubuntu Server 24.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Canonical, Ubuntu, 24.04, amd64 noble image

Arquitectura

64 bits (x86)

ID de AMI

ami-0360c520857e3138f

Fecha de publicación

2025-08-21

Nombre de usuario

ubuntu

Proveedor verificado

▼ Tipo de instancia

Tipo de instancia

t2.micro
Familia: t2 1 vCPU 1 GiB Memoria Generación actual: true
Bajo demanda Windows base precios: 0.0162 USD por hora Bajo demanda Ubuntu Pro base precios: 0.0154 USD por hora
Bajo demanda SUSE base precios: 0.0116 USD por hora Bajo demanda RHEL base precios: 0.026 USD por hora
Bajo demanda Linux base precios: 0.0116 USD por hora

Todas las generaciones

Comparar tipos de instancias

Número de instancias

1

Imagen de software (AMI)

Canonical, Ubuntu, 24.04, amd64...[más información](#)
ami-0360c520857e3138f

Tipo de servidor virtual (tipo de instancia)

t2.micro

Firewall (grupo de seguridad)

Nuevo grupo de seguridad

Almacenamiento (volúmenes)

Volúmenes: 1 (8 GiB)

Cancelar

Lanzar instancia

[Código de versión preliminar](#)

En la configuración de red activamos el trafico ssh, https y http

▼ Configuraciones de red

Red

vpc-0bca90e5d71aaef76

Subred

Sin preferencias (subred predeterminada en cualquier zona de disponibilidad)

Asignar automáticamente la IP pública

Habilitar

Firewall (grupos de seguridad)

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

Crear grupo de seguridad

Seleccionar un grupo de seguridad existente

Crearemos un nuevo grupo de seguridad denominado "launch-wizard-1" con las siguientes reglas:

Permitir el tráfico de SSH desde

Ayuda a establecer conexión con la instancia

Cualquier lugar
0.0.0.0/0

Permitir el tráfico de HTTPS desde Internet

Para configurar un punto de enlace, por ejemplo, al crear un servidor web

Permitir el tráfico de HTTP desde Internet

Para configurar un punto de enlace, por ejemplo, al crear un servidor web

Las reglas con origen 0.0.0.0/0 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.

▼ Configurar almacenamiento

1x 8 GiB gp3

Volumen raíz, 3000 IOPS, No cifrado

Agregar un nuevo volumen

Editar

Avanzado

Paso 2 — Asignar IP elástica

Despues de crear la instancia, creamos una IP elastica y la asociamos con la instancia.

Dirección IP elástica: 54.145.36.185

Tipo de recurso
Elija el tipo de recurso al que desea asociar la dirección IP elástica.

☒ Instancia

☐ Interfaz de red

⚠

Si asocia una dirección IP elástica a una instancia que ya tiene una dirección IP elástica asociada, la dirección IP elástica asociada anteriormente se desasociará, pero la dirección seguirá asignándose a su cuenta. [Más información](#)

Si no se especifica ninguna dirección IP privada, la dirección IP elástica se asociará a la dirección IP privada principal.

Instancia

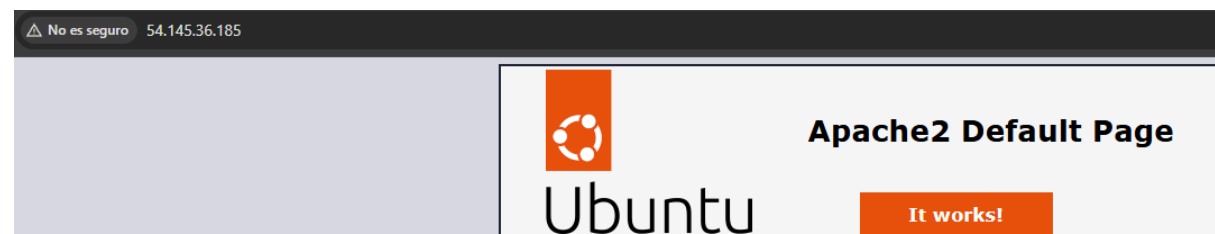
Dirección IP privada
La dirección IP privada a la que se asociará la dirección IP elástica.

Reasociación
Especifique si la dirección IP elástica se puede volver a asociar a un recurso diferente si ya está asociada a un recurso.
☐ Permitir que se vuelva a asociar esta dirección IP elástica

Paso 3 — Actualizar repositorios e instalar Apache

```
ubuntu@ip-172-31-24-108:~$ sudo apt update
sudo apt install apache2 -y
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [1270 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1545 kB]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [294 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [175 kB]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [15.4 kB]
Get:18 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1498 kB]
Get:19 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [303 kB]
Get:20 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [378 kB]
Get:21 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [31.4 kB]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [2175 kB]
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [490 kB]
Get:24 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:25 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 c-n-f Metadata [516 B]
Get:26 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [30.3 kB]
Get:27 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [5564 B]
Get:28 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:29 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 c-n-f Metadata [484 B]
Get:30 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 Packages [40.4 kB]
```

Comprobamos que apache esta instalado y funcionando entrando en la ip elastica que he asociado antes



Paso 4 — Habilitar el módulo SSL de Apache

```
ubuntu@ip-172-31-24-108:~$ sudo a2enmod ssl
sudo systemctl restart apache2
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2

ubuntu@ip-172-31-24-108:~$ sudo systemctl restart apache2
```

Paso 5 — Crear un certificado SSL autofirmado

```
ubuntu@ip-172-31-24-108:~$ sudo mkdir /etc/apache2/ssl
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt
.....
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Valencia
Locality Name (eg, city) []:Valencia
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IES El Grao
Organizational Unit Name (eg, section) []:DAW
Common Name (e.g. server FQDN or YOUR name) []:
54.145.36.185Email Address []:hugcorcor@alu.edu.gva.es
```

Captura con zoom:

```
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Valencia
Locality Name (eg, city) []:Valencia
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IES el grao
Organizational Unit Name (eg, section) []:DAW
Common Name (e.g. server FQDN or YOUR name) []:Hugo
Email Address []:hugcorcor@alu.edu.gva.es
```

Paso 6 — Crear un nuevo sitio HTTPS en Apache

Creamos el archivo de configuracion:

```
ubuntu@ip-172-31-24-108:~$ sudo nano /etc/apache2/sites-available/default-ssl.conf
```

Lo dejamos con el siguiente contenido:

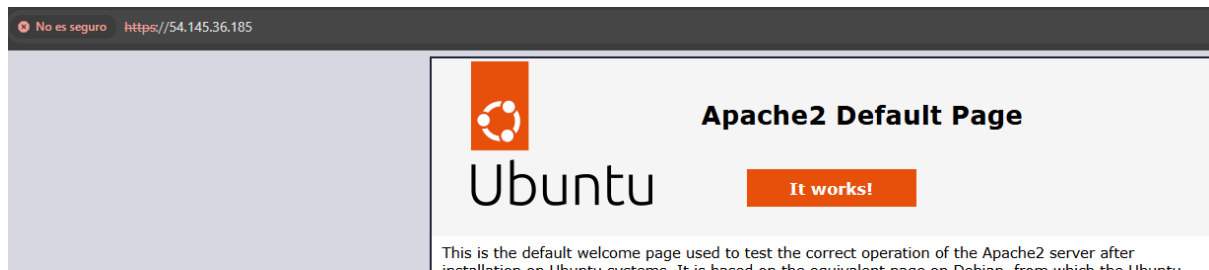
```
<VirtualHost *:443>
    #ServerName practica-https.local
    DocumentRoot /var/www/html
    DirectoryIndex index.php index.html

    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
    SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key
</VirtualHost>
```

Paso 7 — Habilitar el sitio SSL y reiniciar Apache

```
ubuntu@ip-172-31-24-108:~$ sudo a2ensite default-ssl.conf
sudo systemctl reload apache2
Site default-ssl already enabled
```

Al entrar al navegador nos sale una alerta, que si ignoramos no deja entrar y ver el contenido



Paso 8 — Crear todo lo necesario para entregar la practica

Creamos la estructura de todas las carpeta y copiamos los archivos de configuracion de Apache, tambien creamos el archivo .env con las variables

```
ubuntu@ip-172-31-24-108:~$ cd ~
mkdir -p practica-https/conf
mkdir -p practica-https/scripts
ubuntu@ip-172-31-24-108:~$ cp /etc/apache2/sites-available/000-default.conf ~/practica-https/conf/
cp /etc/apache2/sites-available/default-ssl.conf ~/practica-https/conf/
ubuntu@ip-172-31-24-108:~$ nano ~/practica-https/scripts/.env
```

```
OPENSSL_COUNTRY="ES"
OPENSSL_PROVINCE="Valencia"
OPENSSL_LOCALITY="Valencia"
OPENSSL_ORGANIZATION="Ies el grao"
OPENSSL_ORGUNIT="DAW"
OPENSSL_COMMON_NAME="Hugo"
OPENSSL_EMAIL="hugcorcor@alu.edu.gva.es"

SSL_CERT_FILE="/etc/ssl/certs/apache-selfsigned.crt"
SSL_KEY_FILE="/etc/ssl/private/apache-selfsigned.key"
```

Creamos el script install_lamp.sh

```
#!/bin/bash
set -e

sudo apt update
sudo apt install apache2 mysql-server php libapache2-mod-php php-mysql -y

sudo systemctl enable apache2
sudo systemctl enable mysql
sudo systemctl start apache2
sudo systemctl start mysql

echo "LAMP instalado y servicios iniciados correctamente"

ubuntu@ip-172-31-24-108:~$ nano ~/practica-https/scripts/install_lamp.sh
ubuntu@ip-172-31-24-108:~$ chmod +x ~/practica-https/scripts/install_lamp.sh
```

Creamos el script setup_selfsigned_certificate.sh

```
ubuntu@ip-172-31-24-108:~$ nano ~/practica-https/scripts/setup_selfsigned_certificate.sh
ubuntu@ip-172-31-24-108:~$ chmod +x ~/practica-https/scripts/setup_selfsigned_certificate.sh
```

```
sudo openssl req -x509 -nodes -days 365 \
  -newkey rsa:2048 \
  -keyout $SSL_KEY_FILE \
  -out $SSL_CERT_FILE \
  -subj "/C=$OPENSSL_COUNTRY/ST=$OPENSSL_PROVINCE/L=$OPENSSL_LOCALITY/O=$OPENSSL_ORGANIZATION/OU=$OPENSSL_ORGUNIT/CN=$O

sudo a2enmod ssl
sudo a2ensite default-ssl.conf
sudo systemctl reload apache2

echo "Certificado SSL creado y Apache recargado correctamente"
```