

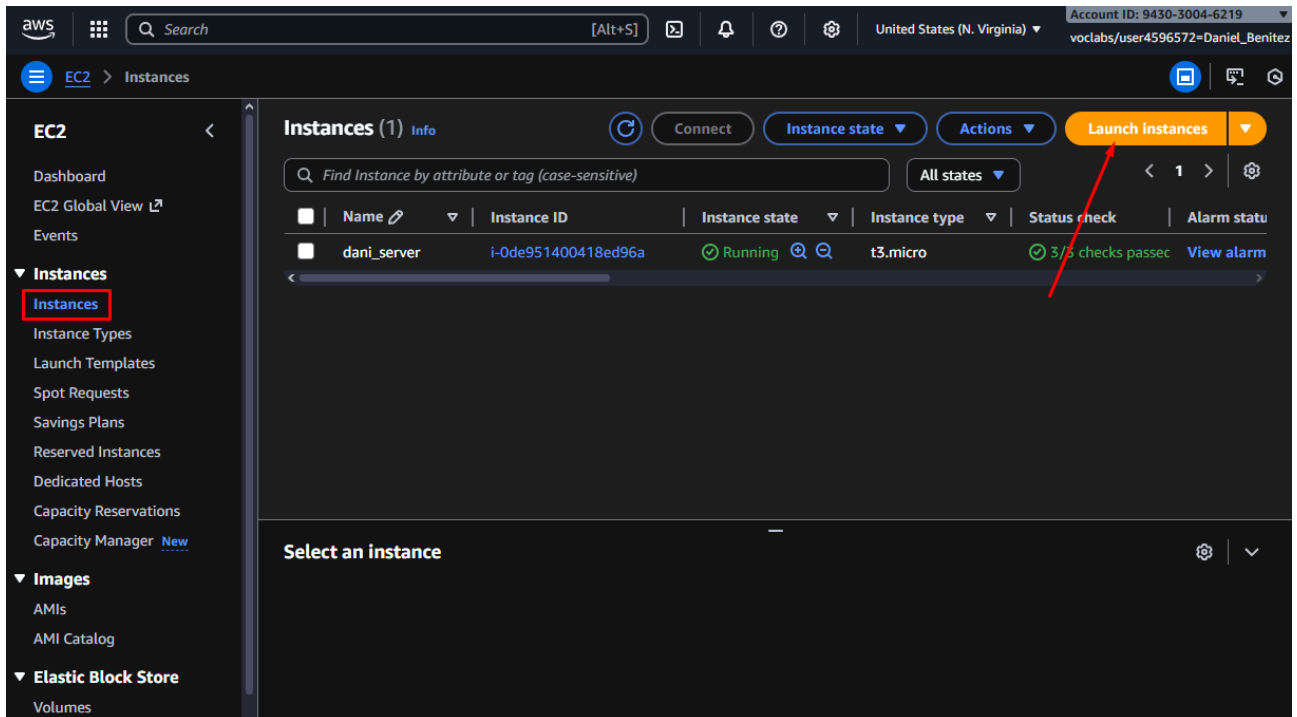
SSL

Sumario

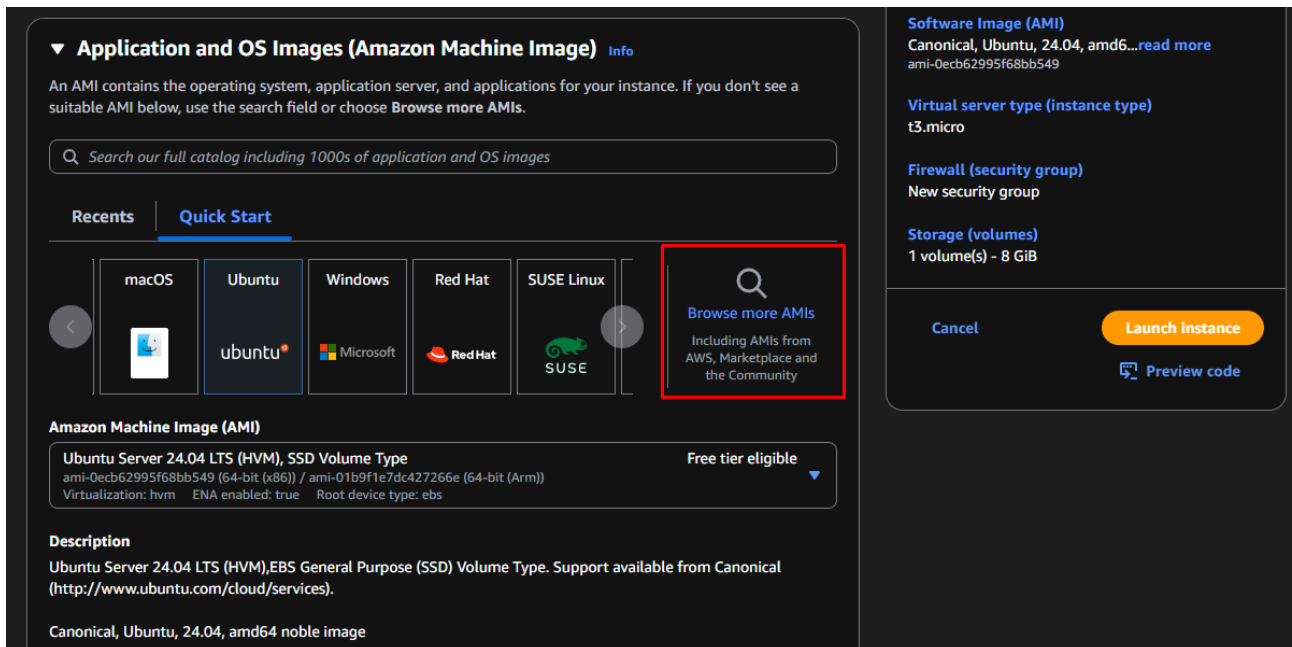
1. Instancia EC2 en AWS.....	2
1.1. Crear una clave.....	3
1.2. Reglas de seguridad.....	4
2. Uso de openssl.....	6
3. Informacion del certificado.....	6
4. Configuración de SSL.....	6
5. Comprobar en navegador.....	7

1. Instancia EC2 en AWS

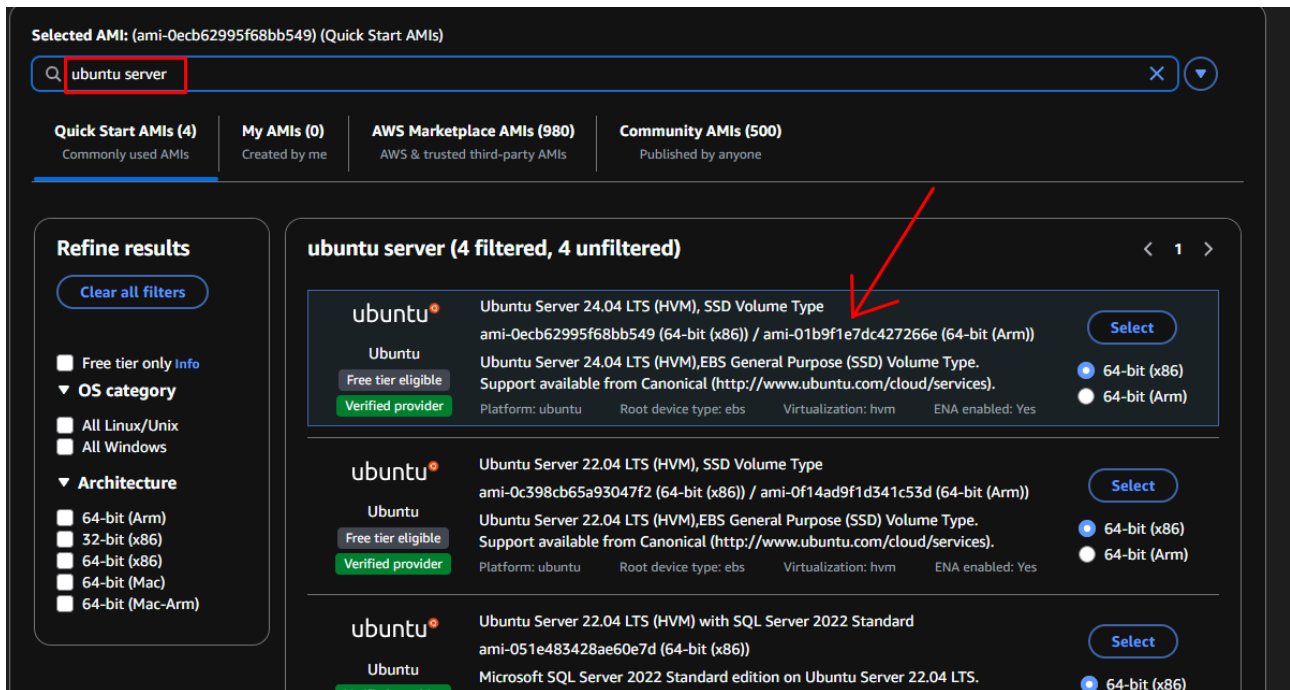
Entramos en EC2 y en la barra lateral vamos a Instances > Launch instances



Le ponemos un nombre cualquiera y en las OS images le damos a “Browse more AMIs”.

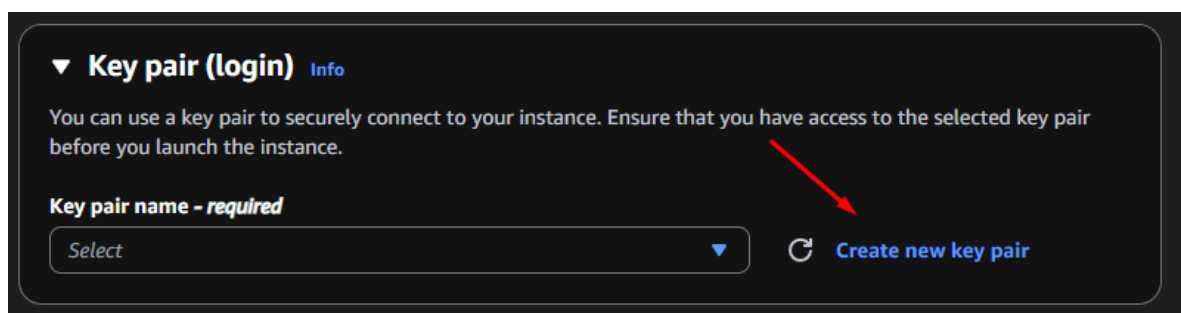


Elegimos un Ubuntu Server.



1.1. Crear una clave

Ademas tambien tendremos que crear una nueva clave para esta instancia, le damos a “Create new key pair”.



Escogemos para la nueva clave la opcion de RSA y .pem

The screenshot shows the 'Create key pair' dialog box. It has a title bar with a close button. The first section is 'Key pair name' with a text input field containing 'SSLubuntu'. Below it is a note: 'The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.' The second section is 'Key pair type' with two radio buttons: 'RSA' (selected) and 'ED25519'. The third section is 'Private key file format' with two radio buttons: '.pem' (selected) and '.ppk'. At the bottom, there is a warning box: 'When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. Learn more'. At the very bottom are 'Cancel' and 'Create key pair' buttons.

Create key pair

Key pair name
Key pairs allow you to connect to your instance securely.

SSLubuntu

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ **RSA**
RSA encrypted private and public key pair

☐ **ED25519**
ED25519 encrypted private and public key pair

Private key file format

☒ **.pem**
For use with OpenSSH

☐ **.ppk**
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#)

Cancel Create key pair

1.2. Reglas de seguridad

Entramos en Firewall de la instancia, en ssh ponemos “My IP”, para HTTP y HTTPS le elegimos “anywhere”.

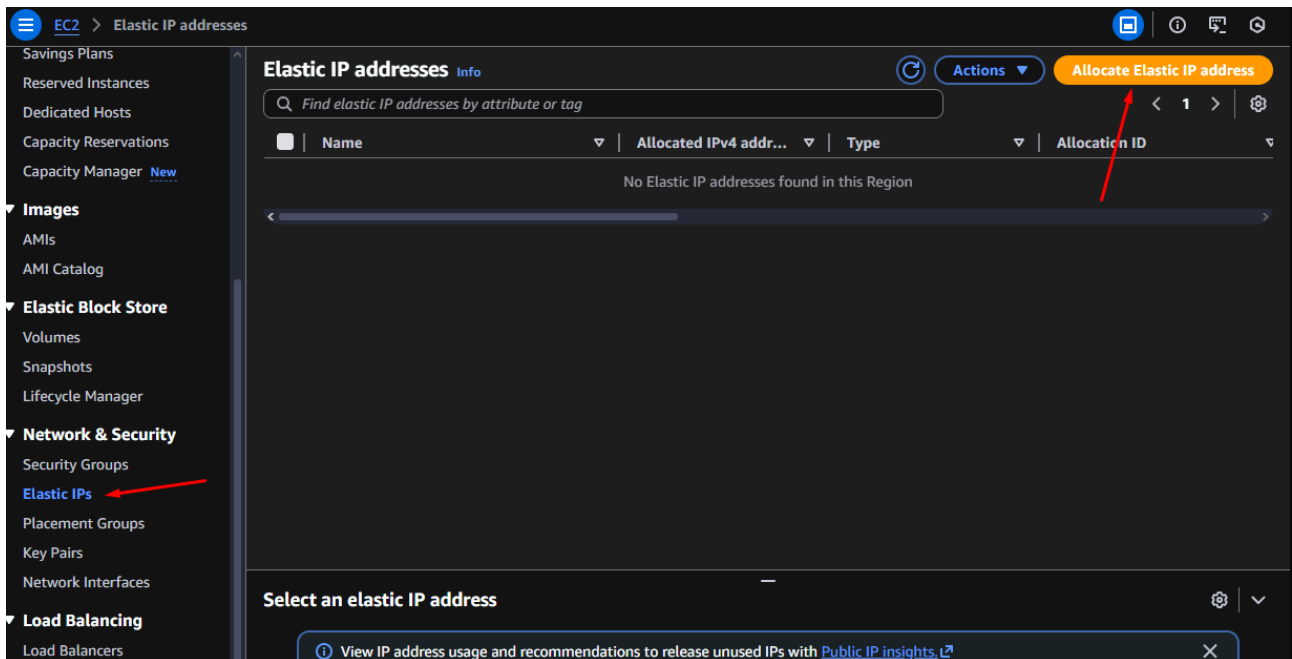
The screenshot shows the 'Inbound Security Group Rules' configuration page. It lists three rules. The first rule is for SSH (TCP, port 22) with source 'My IP' and CIDR '212.104.181.12/32'. The second rule is for HTTP (TCP, port 80) with source 'Anywhere' and CIDR '0.0.0.0/0'. The third rule is for HTTPS (TCP, port 443) with source 'Anywhere' and CIDR '0.0.0.0/0'. Red boxes highlight the 'Type' and 'Source type' fields for the HTTP and HTTPS rules.

Inbound Security Group Rules

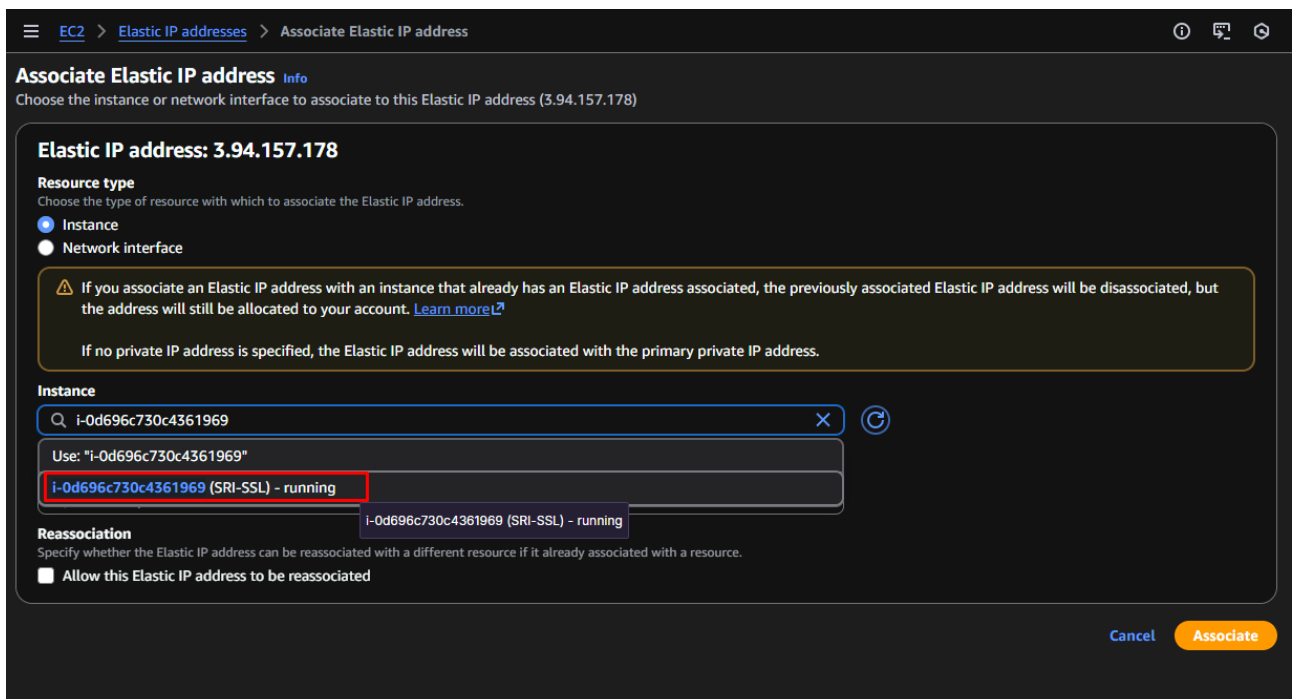
▼ Security group rule 1 (TCP, 22, 212.104.181.12/32) Remove

Type	Protocol	Port range	Source type	Name	Description - optional
ssh	TCP	22	My IP	212.104.181.12/32	e.g. SSH for admin desktop
HTTP	TCP	80	Anywhere	0.0.0.0/0	e.g. SSH for admin desktop
HTTPS	TCP	443	Anywhere	0.0.0.0/0	e.g. SSH for admin desktop

Creamos la instancia despues de eso y ahora tenemos que asignarle a esa misma instancia una IP elastica. Vamos a la barra lateral > Elastic IPs > Allocate Elastic IP address.



A la IP elastica, le damos clic derecho > Associate y elegimos la instancia que habiamos creado.



2. Uso de openssl

Usando openssl pondremos las siguientes directivas para poder configurar el certificado:

```
root@dani-Standard-PC-i440FX-PIIX-1996:/home/dani# openssl req \
> -x509 \
> -nodes \
> -days 365 \
> -newkey rsa:2048 \
> -keyout /etc/ssl/private/apache-selfsigned.key \
> -out /etc/ssl/certs/apache-selfsigned.crt
Generating a 2048 bit RSA private key
.....+++
.....+++
```

3. Información del certificado

Luego pondremos la info de nuestra organización y datos en general, aquí podremos ver un ejemplo de los datos introducidos.

```
root@dani-Standard-PC-i440FX-PIIX-1996:/home/dani
root@dani-Standard-PC-i440FX-PIIX-1996:/home/dani# openssl x509 -in /etc/ssl/cer
ts/apache-selfsigned.crt -noout -subject
subject= /C=ES/ST=Huelva/L=Huelva/O=I.E.S. La Marisma/OU=Informatica/CN=practica
-ssl.local/emailAddress=dani@gmail.com
root@dani-Standard-PC-i440FX-PIIX-1996:/home/dani#
```

4. Configuración de SSL

Ahora deberemos ir a “/etc/apache2/sites-available/default-ssl.conf” y editar lo siguiente del archivo:

```
# If both key and certificate are stored in the same file, a
# SSLCertificateFile directive is needed.
SSLCertificateFile      /etc/ssl/certs/apache-selfsigned.crt
SSLCertificateKeyFile   /etc/ssl/private/apache-selfsigned.key

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
```

Despues activamos el ssl.

```
root@dani-Standard-PC-i440FX-PIIX-1996:/home/dani# a2ensite default-ssl.conf
Enabling site default-ssl.
To activate the new configuration, you need to run:
    service apache2 reload
root@dani-Standard-PC-i440FX-PIIX-1996:/home/dani# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
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 s
elf-signed certificates.
To activate the new configuration, you need to run:
    service apache2 restart
root@dani-Standard-PC-i440FX-PIIX-1996:/home/dani#
```

Vamos al archivo “/etc/apache2/sites-available/000-default.conf” y cambiamos a esto:

```
ServerAdmin webmaster@localhost
#ServerName practica-ssl.local
DocumentRoot /var/www/html

RewriteEngine On
RewriteCond %{HTTPS} off
Rewrite ^ https://%{HTTPS_HOST}%{REQUEST_URI} [L,R=301]
```

5. Comprobar en navegador

Despues podremos comprobar en el navegador

