

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

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with sections like Dashboard, EC2 Global View, Events, Instances (with 'Instances' selected), Images, and Elastic Block Store. In the main area, it says 'Instances (1) Info' and shows a table with one row: 'dani_server' (Instance ID: i-0de951400418ed96a), 'Running' (Status check: 3/3 checks passed), and 't3.micro'. At the top right, there are buttons for Connect, Instance state, Actions, and Launch instances (which has a red arrow pointing to it). Below the table, there's a section titled 'Select an instance'.

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

The screenshot shows the 'Launch instance' wizard. It's on the 'Application and OS Images (Amazon Machine Image)' step. It shows a grid of OS icons: macOS, Ubuntu, Windows, Red Hat, and SUSE Linux. To the right, there's a 'Browse more AMIs' button with a red box around it, which is described as including AMIs from AWS, Marketplace and the Community. On the right side, there are sections for Software Image (AMI), Virtual server type (instance type), Firewall (security group), Storage (volumes), and buttons for Cancel, Launch instance (which is orange), and Preview code.

Elegimos un Ubuntu Server.

The screenshot shows the AWS Lambda console interface for selecting an AMI. The search bar at the top contains the text "ubuntu server". Below the search bar, there are four categories: "Quick Start AMIs (4)", "My AMIs (0)", "AWS Marketplace AMIs (980)", and "Community AMIs (500)". The "Quick Start AMIs" category is selected and highlighted in blue. The results list shows three entries for "ubuntu":

- ubuntu** (Ubuntu) - Free tier eligible, Verified provider. Description: Ubuntu Server 24.04 LTS (HVM), SSD Volume Type. AMI IDs: ami-0ecb62995f68bb549 (64-bit (x86)) / ami-01b9f1e7dc427266e (64-bit (Arm)). Select button and 64-bit (x86) radio button selected.
- ubuntu** (Ubuntu) - Free tier eligible, Verified provider. Description: Ubuntu Server 22.04 LTS (HVM), SSD Volume Type. AMI IDs: ami-0c398cb65a93047f2 (64-bit (x86)) / ami-0f14ad9f1d341c53d (64-bit (Arm)). Select button and 64-bit (x86) radio button selected.
- ubuntu** (Ubuntu) - Verified provider. Description: Ubuntu Server 22.04 LTS (HVM) with SQL Server 2022 Standard. AMI ID: ami-051e483428ae60e7d (64-bit (x86)). Select button and 64-bit (x86) radio button selected.

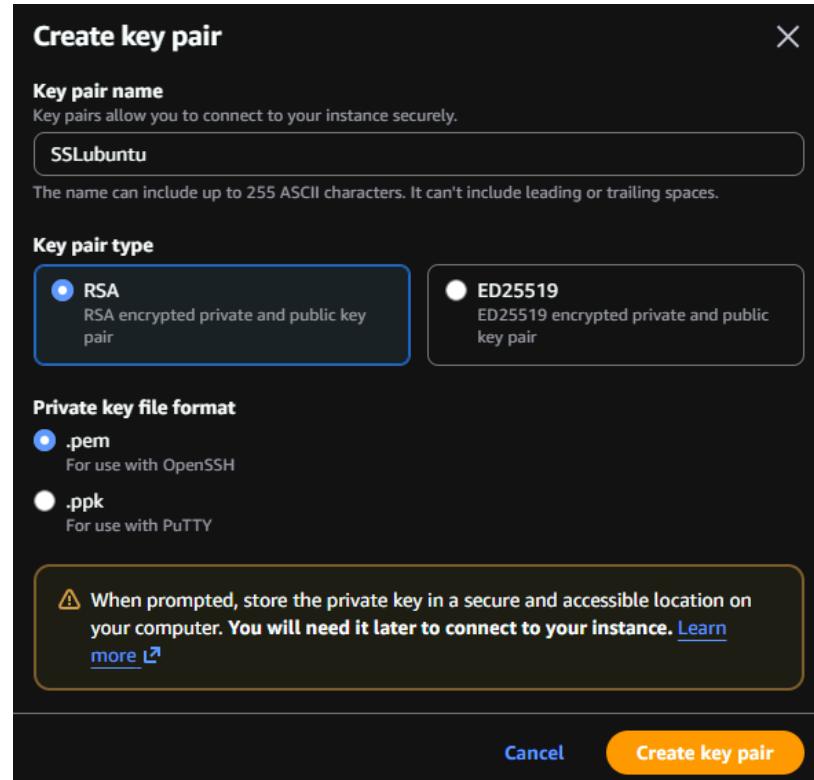
A red arrow points from the text "Elegimos un Ubuntu Server." to the first result entry.

1.1. Crear una clave

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

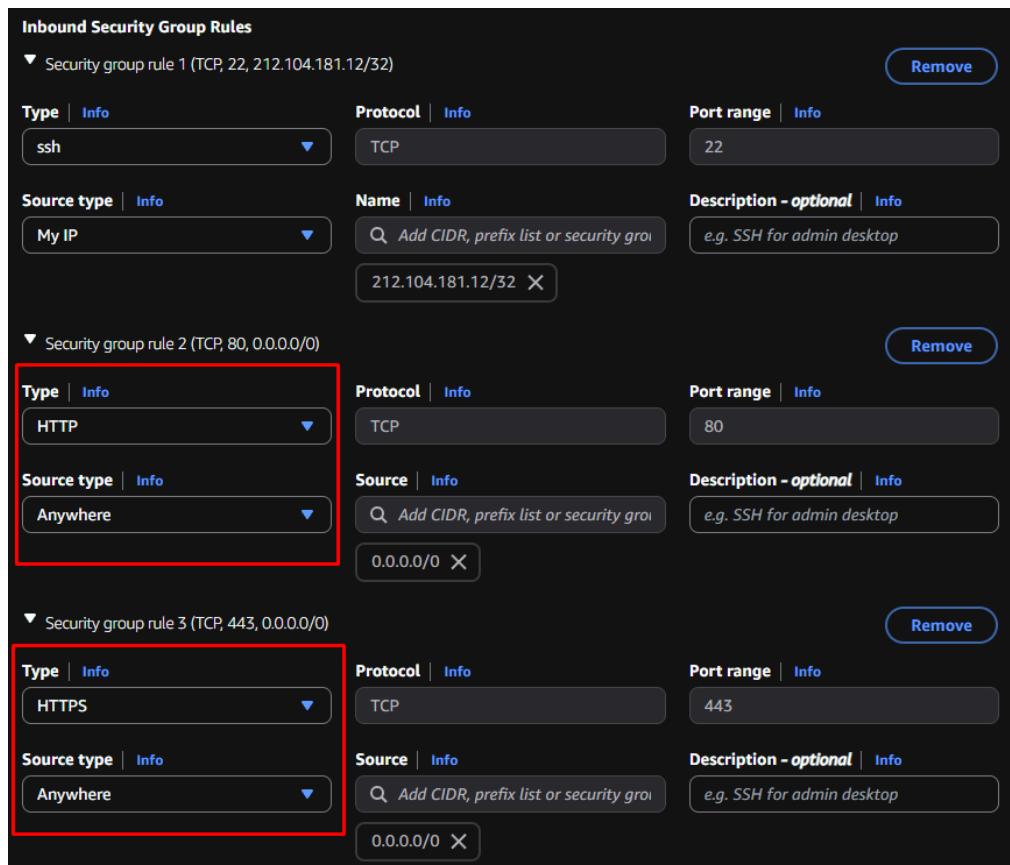
The screenshot shows the "Key pair (login)" section of the AWS Lambda console. It includes a note: "You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance." A red arrow points from the text "Create new key pair" to the "Create new key pair" button. The "Key pair name - required" dropdown menu has "Select" highlighted. The "Create new key pair" button is located at the bottom right of the form.

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



1.2. Reglas de seguridad

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



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.

The screenshot shows the AWS EC2 console with the 'Elastic IP addresses' page selected. The left sidebar includes sections for Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Capacity Manager, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security (with 'Elastic IPs' highlighted by a red arrow), Placement Groups, Key Pairs, Network Interfaces, Load Balancing, and Load Balancers. At the top right, there is an 'Actions' dropdown and a prominent yellow 'Allocate Elastic IP address' button. A red arrow also points to this button. Below the table, a message states 'No Elastic IP addresses found in this Region'.

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

The screenshot shows the 'Associate Elastic IP address' dialog box. It starts with the message 'Choose the instance or network interface to associate to this Elastic IP address (3.94.157.178)'. Below this, it says 'Elastic IP address: 3.94.157.178'. Under 'Resource type', there are two options: 'Instance' (selected) and 'Network interface'. A warning message states: '⚠ If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. [Learn more](#)' and 'If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.' In the 'Instance' section, a search bar shows 'i-0d696c730c4361969' and a dropdown menu lists 'Use: "i-0d696c730c4361969"' and 'i-0d696c730c4361969 (SRI-SSL) - running'. The latter is highlighted with a red box. At the bottom, under 'Reassociation', there is a checkbox 'Allow this Elastic IP address to be reassociated' and two buttons: 'Cancel' and 'Associate'.

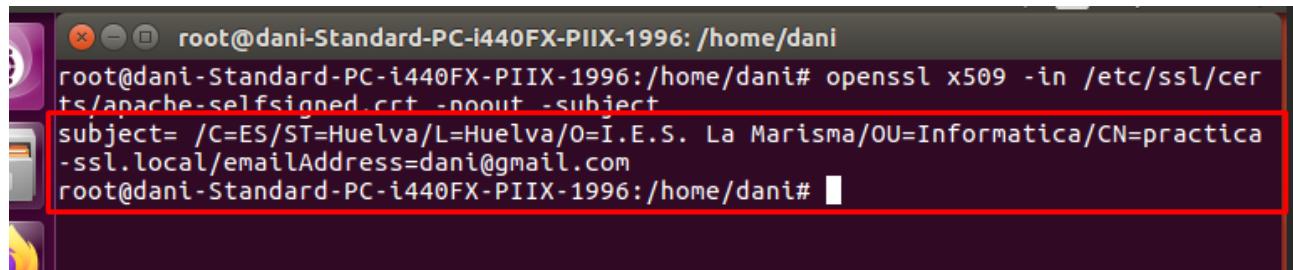
2. Uso de openssl

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. Informacion del certificado

Luego pondremos la info de nuestra organización y datos en general, aqui 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/certs/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,
# 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 self-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

