



Servicio de Red e Internet

Volodimir Yarmash Yarmash

Índice

Usando una instancia AWS debemos instalar Apache con las siguientes opciones de configuración:.....	3
Activar la autenticación con MySql.....	3
Crear un certificado autofirmado y activar el módulo SSL.....	5
Bibliografía:.....	10

Usando una instancia AWS debemos instalar Apache con las siguientes opciones de configuración:

Para instalar apache2 en la instancia de AWS EC2 debemos de lanzar esta instancia antes que nada y conectarnos para poder manipular ubuntu.

Hacemos un update con `sudo apt update`

Instalamos Apache2 con el comando `sudo apt install apache2`

```
ubuntu@ip-172-31-20-162:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.58-1ubuntu8.5).
0 upgraded, 0 newly installed, 0 to remove and 47 not upgraded.
ubuntu@ip-172-31-20-162:~$
```

Activar la autenticación con MySQL

Para activar la autenticación con MySQL debemos descargar MySQL-server antes.

Para ello usamos el comando `sudo apt install mysql-server`.

```
ubuntu@ip-172-31-20-162:~$ sudo apt install mysql-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libbcgi-fast-perl libbcgi-pm-perl libclone-perl libencode-locale-perl libevent-pth
  libhttp-date-perl libhttp-message-perl libio-html-perl liblwp-mediatypes-perl lib
  mysql-client-core-8.0 mysql-common mysql-server-8.0 mysql-server-core-8.0
Suggested packages:
  libdata-dump-perl libipc-sharedcache-perl libio-compress-brotli-perl libbusiness
The following NEW packages will be installed:
```

Accedemos a MySQL usando el comando `sudo mysql -u root -p`.

```
ubuntu@ip-172-31-20-162:~$ sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 8.0.40-0ubuntu0.24.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Introducimos `Select user, plugin FROM mysql.user;` para comprobar si el plugin de auth_socket está presente.

```
mysql> select user, host, plugin FROM mysql.user;
+-----+-----+-----+
| user          | host      | plugin          |
+-----+-----+-----+
| debian-sys-maint | localhost | caching_sha2_password |
| mysql.infoschema | localhost | caching_sha2_password |
| mysql.session   | localhost | caching_sha2_password |
| mysql.sys       | localhost | caching_sha2_password |
| root           | localhost | auth_socket      |
+-----+-----+-----+
5 rows in set (0.00 sec)
```

Modificamos la contraseña con este comando mysql: `ALTER USER 'root'@'localhost' identified WITH mysql_native_password by 'user123';`

```
mysql> ALTER USER 'root'@'localhost' identified WITH mysql_native_password by 'user123';
Query OK, 0 rows affected (0.01 sec)

mysql>
```

Y usamos `Flush PRIVILEGES;` para aplicar cambios en los privilegios.

```
mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)

mysql>
```

Salimos del modo sql usando `exit`

Usamos el comando `sudo mysql -u root -p` para entrar con root e introducimos una contraseña errónea. Como podéis observar, nos ha negado el acceso.

Ahora introducimos la contraseña correcta y nos da el acceso a root.

```
mysql> exit
Bye
ubuntu@ip-172-31-20-162:~$ sudo mysql -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
ubuntu@ip-172-31-20-162:~$ sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.40-0ubuntu0.24.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

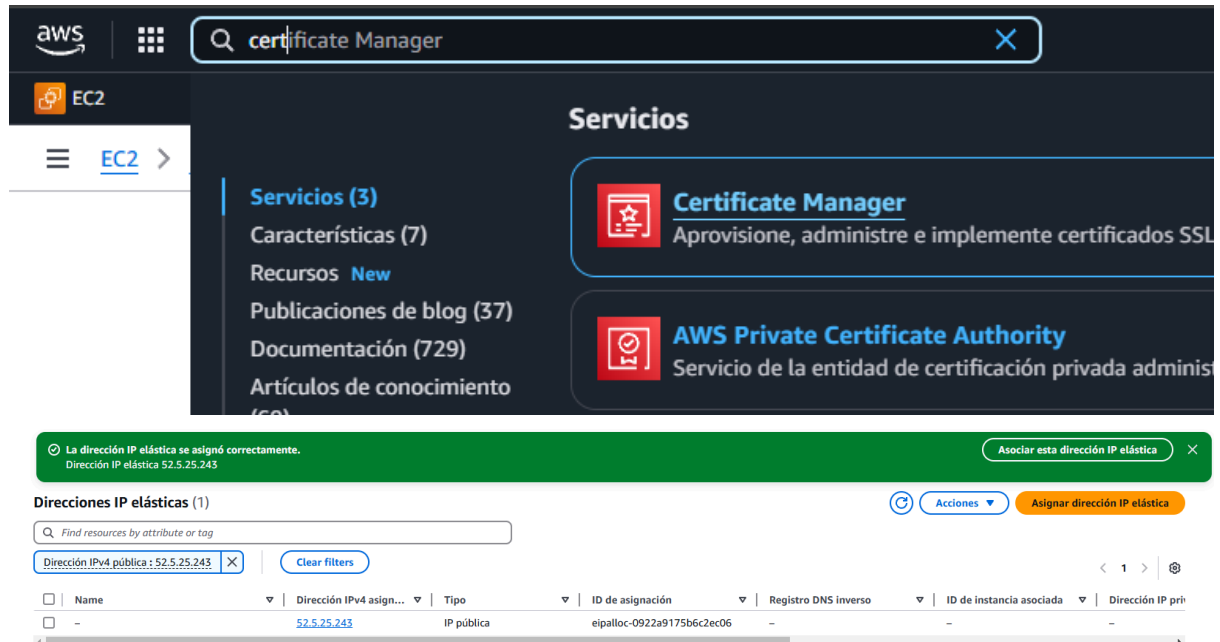
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Crear un certificado autofirmado y activar el módulo SSL

Entramos en el manager de certificados.



Solicitamos el certificado pulsando este boton.



Introducimos el dns que nos interesa, en nuestro caso voy a introducir **volodimirprueba.com** como dns (Borramos el de aws e introducimos el nuevo)

Solicitar certificado público

Nombres de dominio

Proporcione uno o más nombres de dominio para el certificado.

Nombre de dominio completo [Información](#)

ec2-52-5-25-243.compute-1.amazonaws.com

[Agregar otro nombre a este certificado](#)

Puede agregar nombres adicionales a este certificado. Por ejemplo, si solicita un certificado para "www.example.com", es posible que desee agregar el nombre "example.com".

Método de validación [Información](#)

Seleccione un método para validar la propiedad del dominio.

☒ Validación de DNS: recomendado

Elija esta opción si está autorizado para modificar la configuración de DNS de los dominios de la solicitud de certificado.

☐ Validación por email

Elija esta opción si no tiene permiso o no puede obtenerlo para modificar la configuración de DNS de los dominios en la solicitud de certificado.

Algoritmo de clave [Información](#)

Seleccione un algoritmo de cifrado. Es posible que algunos algoritmos no sean compatibles con todos los servicios de AWS.

☒ RSA 2048

RSA es el tipo de clave más utilizado.

☐ ECDSA P 256

Equivalente en fuerza criptográfica a RSA 3072.

☐ ECDSA P 384

Equivalente en fuerza criptográfica a RSA 7680.

Tipo de certificado [Información](#)

Los certificados de ACM se pueden utilizar para establecer un acceso seguro a las comunicaciones a través de Internet o dentro de una red interna. Elija el tipo de certificado para que ACM lo proporcione.

☒ Solicitar un certificado público

Solicite a Amazon un certificado SSL/TLS público. De forma predeterminada, los navegadores y sistemas operativos confían en los certificados públicos.

☐ Solicitar un certificado privado

No hay entidades de certificación privadas disponibles para emitir.

La solicitud de un certificado privado requiere la creación de una entidad de certificación (CA) privada. Para crear una CA privada, visite [AWS Private Certificate Authority](#).

[Cancelar](#)

[Siguiente](#)

A continuación debemos exportar la configuración DNS en csv (botón azul).

Certificado correctamente con ID 8c170fc6-6c66-4899-aa6d-f8a49a4f9969

Se ha creado una solicitud de certificado con el estado pendiente de validación. Se necesitan acciones adicionales para completar la validación y aprobación del certificado.

Ver certificado

Notificaciones 0 0 2 1 0

8c170fc6-6c66-4899-aa6d-f8a49a4f9969

Eliminar

Estado del certificado

Identificador

8c170fc6-6c66-4899-aa6d-f8a49a4f9969

ARN

arn:aws:acm:us-east-1:822250914516:certificate/8c170fc6-6c66-4899-aa6d-f8a49a4f9969

Tipo

Emitido por Amazon

Estado

Pendiente de validación Información

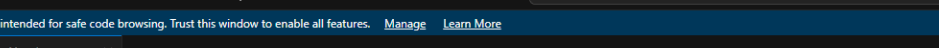
Dominios (1)

Crear registros en Route 53 Exportar a CSV

< 1 >

Dominio	Estado	Estado de renovación	Tipo	Nombre CNAME
vologimirprueba.com	Pendiente de validación	-	CNAME	_4ba5d7ec5fb47b554fdb54c7ba5663ef.vologimirprueba.com.

Se nos descargará un archivo con los siguientes datos.



The screenshot shows a Windows terminal window with the following content:

```
File Edit Selection View Go Run Terminal Help
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More


Configuración_de_DNS.csv X
C: > Users > vladt > Downloads > Configuración_de_DNS.csv
1 Nombre de dominio,Nombre CNAME,Tipo,Valor CNAME
2 volodimirprueba.com,_4ba5d7ec5fb47b554fdb54c7ba5663ef.volodimirprueba.com.,CNAME,_58e997794beaf1ceb5dd068e93a55de8.zfyfvmchrl1.acm-validations.aws.
```


Ahora en el buscador entramos en el servicio de route 53.

Servicios

Ver los 6 resultados

Servicios (6)
Características (42)
Recursos **New**
Publicaciones de blog (24)
Documentación (2705)
Artículos de conocimiento (136)
Tutoriales (6)

**Ground Station**
Comunicación con satélites

**Route 53**
Registro escalable de DNS y nombres de dominio

Características principales

[Flujo de tráfico](#) [Comprobaciones de estado](#) [Zonas alojadas](#) [Nombres de dominio](#) [Puntos de enlace del solucionador](#)

Creamos una zona alojada, introducimos el nombre de dominio del archivo, y de comentario el segundo código que actúa como validador.

Crear una zona alojada [Información](#)

Configuración de zona alojada

Una zona alojada es un contenedor que incluye información sobre cómo usted desea dirigir el tráfico de un dominio (como example.com) y sus subdominios.

Nombre de dominio [Información](#)

Este es el nombre del dominio al que desea dirigir el tráfico.

_4ba5d7ec5fb47b554fdb54c7ba5663ef

Caracteres válidos: a-z, 0-9, ! * # \$ % & ' () * + , - / : ; < = > ? @ [\] ^ _ ` { | } . ~

Descripción - opcional [Información](#)

Este valor le permite distinguir las zonas alojadas que tienen el mismo nombre.

_58e997794beaf1ceb5dd068e93a55de8.zfyvmchrl.acm-validations.aws.

La descripción puede tener un máximo de 256 caracteres. 65/256

Tipo [Información](#)

El tipo indica si desea dirigir el tráfico en Internet o en una VPC de Amazon.

☒ Zona alojada pública

Una zona alojada pública determina cómo se dirige el tráfico en Internet.

☐ Zona alojada privada

Una zona alojada privada determina cómo se direcciona el tráfico dentro de una VPC de Amazon.

✓ _4ba5d7ec5fb47b554fdb54c7ba5663ef.volodimirprueba.com se creó correctamente.
Ahora puede crear registros en la zona alojada para especificar cómo desea que Route 53 dirija el tráfico del dominio.

[Pública](#) **_4ba5d7ec5fb47b554fdb54c7ba5663ef.volodimirprueba.com** [Información](#)

[Eliminar zona](#)

[Probar el registro](#)

[Configurar el registro de consultas](#)

► Detalles de la zona alojada

[Editar zona alojada](#)

[Registros \(2\)](#)

[Firma DNSSEC](#)

[Etiquetas de zona hospedada \(0\)](#)

Registros (2) [Información](#)



[Eliminar registro](#)

[Importar archivo de zona](#)

[Crear registro](#)

El modo Automatic es el comportamiento actual de búsqueda que se ha optimizado para obtener los mejores resultados del filtrado. [Para cambiar los modos, vaya a la configuración.](#)

Tipo ▼

Política d... ▼

Alias ▼

< 1 >



<input type="checkbox"/>	Nombre del registro	Tipo	Política...	Difer...	Alias	Valor/Dirigir el tráfico a	TTL (s...)
<input type="checkbox"/>	_4ba5d7ec5fb47b554fdb54c7ba5663ef.volodi...	NS	Simple	-	No	ns-1912.awsdns-47.co.uk. ns-1491.awsdns-58.org. ns-275.awsdns-34.com. ns-699.awsdns-23.net.	172800
<input type="checkbox"/>	_4ba5d7ec5fb47b554fdb54c7ba5663ef.volodi...	SOA	Simple	-	No	ns-1912.awsdns-47.co.uk. a...	900

Ahora volvemos al apartado de certificados y esperamos a que validen nuestro dns.

Certificados (1)



[Eliminar](#)

[Administrar eventos de vencimiento](#)

[Importar](#)

[Solicitar](#)

< 1 >



<input type="checkbox"/>	ID de certificado	Nombre de dominio	Tipo	Estado	En uso	Requisitos que se deben cumplir para la renovación	Algoritmo de clave
<input type="checkbox"/>	8c170fc6-6c66-4899-aa6d-f8a49a4f9969	volodimirprueba.com	Emitido por Amazon	Pendiente de validación	No	No se cumplen los requisitos	RSA 2048

Para hacerlo con Apache tenemos que activar el módulo ssl con el comando `sudo a2enmod ssl`.


```
root@ip-172-31-23-93:/# sudo a2enmod ssl
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for
Module socache_shmcb already enabled
Enabling module ssl.
```

Escribimos este comando: `sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt`

Si lo desmontamos:

openssl req indica que quieres ejecutar una solicitud

-x509 genera un certificado en formato X.509, que es el estándar para certificados digitales utilizados en SSL/TLS.

-nodes asegura que la clave privada no esté encriptada

-days 365 Especifica que el certificado tendrá una validez de 365 días

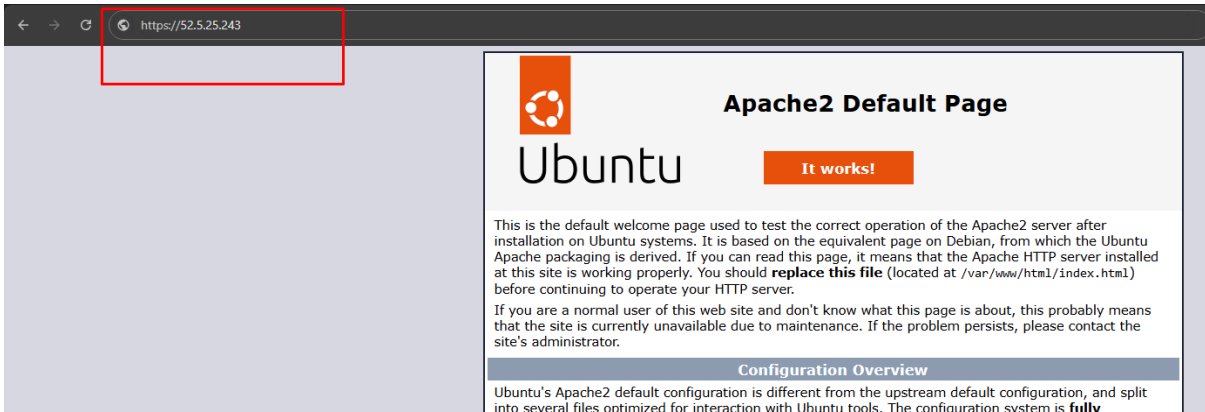
-newkey rsa:2048 Indica que se debe generar una nueva clave privada usando el algoritmo RSA con un tamaño de 2048 bits

```

root@ip-172-31-23-93:~# sudo openssl req -x509 -nodes -days 365 -newkey rsa:
lfsigned.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.

```

Tenemos que rellenar alguna información y estaría listo. Lo podemos probar con el dominio predeterminado.



Bibliografía:

<https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-apache-in-ubuntu-20-04-es>