

 Universidad Autónoma de Madrid	CATÁLOGO DE SERVICIOS TI	Fecha 11/02/2026
	CERTIFICADOS SSL DE SERVIDOR	TECNOLOGÍAS DE LA INFORMACIÓN UAM

Configuración de ACME en servidor web Linux Apache o Nginx

Contenido

1	Descripción	1
2	Objetivo y requisitos	1
3	Instrucciones de configuración	1
4	Enlaces de ayuda	1

1 Objetivo y requisitos

Esta documentación describe como instalar y configurar certbot para solicitar, renovar o revocar certificados usando su cuenta ACME personal de HARICA. Incluye el despliegue en Apache o Nginx.

Requisitos:

- Cuenta ACME personal en Harica - para poder seguir estas instrucciones previamente debe haber creado una cuenta ACME personal en HARICA. Si no lo ha hecho consulte la guía de creación de cuentas ACME personales.
- Servidor con dominio valido - todos los comandos de esta guía deben ejecutarse desde el servidor en el que su IP resuelva por el nombre DNS de dominio del certificado que está solicitando.
- Apache o Nginx - debe estar instalado uno de los 2 servidores web y debe estar levantado y escuchando por el puerto 80 y accesible desde internet.

Aviso: Las siguientes instrucciones son una guía para facilitar una instalación inicial. Tienen carácter meramente orientativo y están destinadas a personal técnico cualificado. No se dará soporte a servidores web instalados usando estas instrucciones.

2. Instrucciones de configuración

2.1. Recopilamos las variables ACME de nuestra cuenta

Durante la creación de la cuenta ACME personal, habrá obtenido 3 valores que necesitaremos durante este proceso: “Key ID”, “HMAC Key” y “Server URL”. En la guía de creación de cuentas ACME personales viene descrito como acceder a esta información.

A efectos de esta guía usaremos los siguientes **valores ficticios (NO LOS USE EN SUS PETICIONES)**:

- Key ID: f48a_TEST_f1qzzl
- HMAC Key: acf09faae53cf9e1f2_TEST_be243a64e5df25037f2d35e3ee
- Server URL: https://acme-v02.harica.gr/acme/96faf73b3c-2f0f-TEST-8a99-7f23f6884fe4/directory

Recuerde sustituirlos por los tuyos cuando sigas esta guía.

2.2. Instalamos certbot

Certbot es el cliente ACME que realizará el trabajo de gestión de los certificados. Instalaremos también los plugins para configurar los certificados en Apache y Nginx.

Abriremos una consola para ejecutar todos los comandos de esta guía a lo largo del todo el proceso sin cerrarla.

y ejecutamos los siguientes comandos:

```
sudo apt-get update
sudo apt install certbot python3-certbot-apache python3-certbot-nginx
```

2.3. Registro de la cuenta de ACME en el equipo

En la consola ejecutamos el proceso de registro, sustituyendo los valores de ACME ficticios por los nuestros. El correo debe ser el del responsable del web y se usa a efectos de notificación.

```
# Primero exportamos las variables de entorno de la cuenta ACME
export key_id="f48a_TEST_f1qzzj"
export hmac_key="acf09faae53cf9e1f2_TEST_be243a64e5df25037f2d35e3ee"
export server_url="https://acme-v02.harica.gr/acme/96faf73b3c-2f0f-TEST-8a99-7f23f6884fe4/directory"

# Registramos la cuenta en el servidor
sudo certbot register --server $server_url --eab-kid $key_id --eab-hmac-key $hmac_key
--email correo\_del\_administrador@uam.es --agree-tos
```

2.4. Obtención y despliegue de certificado

En este paso se produce la verificación HTTP-01¹ y tenemos que asegurarnos de que el servidor web (Apache o Nginx) está levantado y que tiene accesible el puerto 80 desde Internet.

En la misma consola (si la hemos cerrado, volver a exportar las variables de la cuenta ACME) ejecutaremos el comando apropiado para nuestro servidor web. Por ejemplo si nuestro servidor tiene como nombre de dominio "mi-web.ti.uam.es"

```
#### Elegir en cada caso

# Si usa Apache
sudo certbot apache --server $server_url -d mi-web.ti.uam.es

# Si usa Nginx
sudo certbot nginx --server $server_url -d mi-web.ti.uam.es
```

Si todo ha ido bien:

- El certificado queda instalado. Podremos probarlo conectando a <https://mi-web.ti.uam.es>
- El servidor queda configurado para que verifique cada 12h la validez del certificado. En caso de que tenga una validez de 30 días o menos, lo renovará y reiniciará el servidor web de forma automática para que se apliquen los cambios.

¹ Tipos de desafíos ACME: <https://letsencrypt.org/docs/challenge-types/>

3. Comandos de interés

A continuación, se detallan comandos de interés usando certbot o comandos del sistema relacionados con la gestión del certificado o certificados que acabamos de instalar.

Comprobar certificados gestionados por certbot:

```
sudo certbot certificates
```

Comprobar cron para la renovación automática antes de que expire:

```
systemctl list-timers | grep certbot
```

Forzar la actualización de todos los certificados instalados con certbot (sólo prueba):

```
sudo certbot renew --force-renewal --dry-run
```

Forzar la actualización de todos los certificados instalados con certbot:

```
sudo certbot renew --force-renewal
```

Forzar la actualización de un certificado específico con certbot (sólo prueba):

```
sudo certbot renew --force-renewal --dry-run --cert-name nombre_del_servidor
```

Forzar la actualización de un certificado específico con certbot:

```
sudo certbot renew --force-renewal --cert-name nombre_del_servidor
```

4. Enlaces de ayuda

[¿Qué es ACME?](#)

[¿Por qué usar ACME?](#)