Configuració d'un servidor Apache segur amb un certificat autosignat (HTTPS).

Nom i Cognom: Carles Molina Espinós

Curs: 2CFGS DAW

Index

Objectius

- Entendre el funcionament dels sistemes d'encriptació asimètrics
- Generar un certificat
- Instal·lar i un certificat sobre Apache per poder establir una connexió segura?

Enunciat

1. Crea un certificat autosignat i configura'l en Apache de forma que en accedir a l'URL https://##.aula218.lan s'establisca una connexió segura. Guarda el certificat en la carpeta /var/cert.

1. Generació del certificat autosignat

Per generar un certificat autosignat i configurar-lo en Apache, seguim els passos següents:

1.1. Crear el directori per emmagatzemar el certificat

```
sudo mkdir -p /var/cert
```

1.2. Generar una clau privada:

El comandament que he escrit serveix per generar una clau privada RSA mitjançant OpenSSL**:**

- openssl: Crida l'eina OpenSSL, que s'utilitza per gestionar certificats i claus criptogràfiques.
- genpkey: Indica que vols generar una nova clau privada.
- algorithm RSA: Especificab que vols generar una clau RSA.
- -out /var/cert/servidor.key: Especifica la ubicació i el nom del fitxer on es guardarà la clau privada generada.

```
sudo openssl genpkey -algorithm RSA -out /var/cert/servidor.key
```

1.3. Generar una certificat autosignat

El comandament serveix per a crear un certificat autosignat utilitzant la clau privada generada prèviament:

- openssl req: Indica que vols generar una sol·licitud de certificat.
- new :Especifica que es crearà una nova sol·licitud de certificat.
- x509: Indica que el certificat es autosignat, es a dir no estara validat per Autoritat de Certificació .
- key /var/cert/servidor.key: Indica la clau privada per a signar el certificat.
- out /var/cert/servidor.crt: Defineix el fitxer on es guardarà el certificat generat.
- days 365: Validesa del certificat

```
sudo openssl req -new -x509 -key /var/cert/servidor.key -out /var/cert/servidor.crt -days 365
```

2. Configuració d'Apache per utilitzar el certificat

2.1. Modificar la configuració del lloc segur

Editar el fitxer de configuració SSL d'Apache:

El comandament serveix per editar la configuració del lloc web segur (SSL) d'Apache.

```
sudo nano /etc/apache2/sites-available/default-ssl.conf
```

Afegir les línies seguents:

- VirtualHost *:443: Configura el servidor per escoltar peticions HTTPSal port 443.
- ServerName 15.aula128.lan: Nom del domini del servidor.
- SSLEngine on: Activa SSL/TLS.
- SSLCertificateFile /var/cert/servidor.crt: Ruta del certificat SSL.
- SSLCertificateKeyFile /var/cert/servidor.key: Ruta de la clau privada

```
<VirtualHost *:443>
   ServerName  15.aula128.lan
   SSLEngine on
   SSLCertificateFile /var/cert/servidor.crt
   SSLCertificateKeyFile /var/cert/servidor.key
</VirtualHost>
```

2.2. Activar el mòdul SSL i el lloc segur

Habilitar o activar el mòdul SSL a Apache.

```
sudo a2enmod ssl
sudo a2ensite default-ssl
```

2.3. Reiniciar Apache

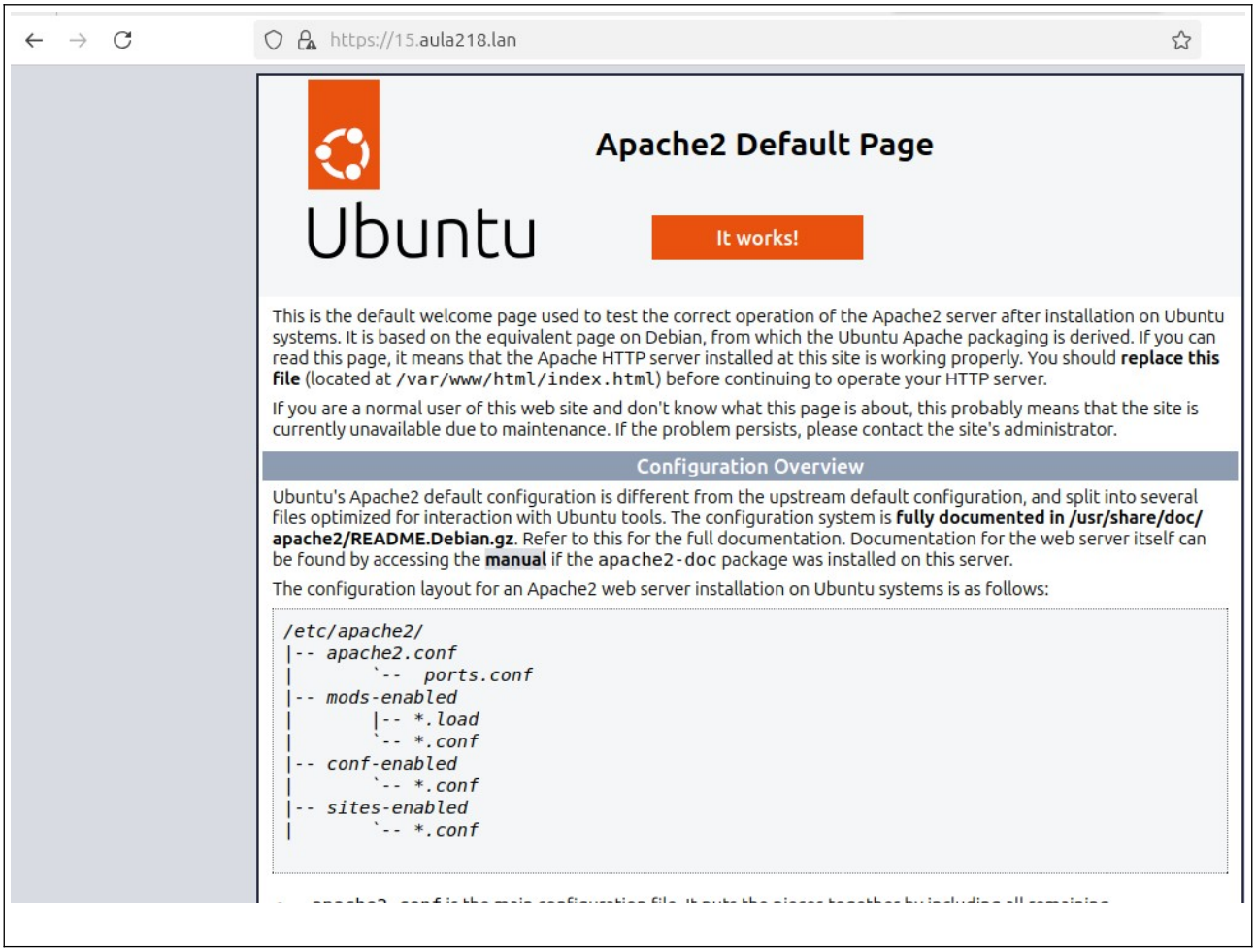
```
sudo systemctl restart apache2
```

3. Verificació de la connexió segura

3.1. Accedir a l'URL

Obrir un navegador i accedir a:

```
https://15.aula218.lan
```



3.2. Acceptar el certificat autosignat

Els navegadors permeten acceptar manualment certificats autosignats. En alguns casos, cal afegir-loncom a excepció de seguretat.

4. Conclusions

- La connexió segura s’ha establert correctament però amb un avís de seguretat per ser un certificat autosignat.
- Per evitar aquest avís, caldria obtenir un certificat d’una de certificació reconeguda.

5. Webgrafia

Documentació crear un certificat SSL autosignat per Apache :

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