Previo:

asignar direcciones estáticas al servidor ALMA con ntui (verificar el fichero host de vuestro windows).

Verificar que el servidor DNS (/etc/resolv.conf) es el adecuado para acceso externo (172.16.2.2) En caso contrario no podremos instalar.

Instalación APACHE

ALMA:

1. dnf update
2. dnf install httpd
3. systemctl status httpd
4. nmap localhost (dnf install nmap)
5. firewall-cmd –permanent –add-port=80/tcp (también 443/tcp para uso posterior)
6. Crea una página con chatGPT y ubícala en /var/www/html
7. curl localhost

UBUNTU

1. apt install apache2
2. systemctl status apache2
3. nmap localhost
4. ufw allow 80/tcp (y 443/tcp)
5. curl localhost
6. elimina en /var/www/html la página index.html y crea el directorio data con tres ficheros en su interior.

## Crear sitios virtuales:

En ubuntu:

1. Crea las rutas en /var/www/html con tres directorios (www, web, red)
2. En cada uno de ellos genera una página web “significativa”
3. Accede a /etc/apache2/sites-available
4. Copia 00-default.conf como www.conf red.conf web.conf (tres ficheros de configuración)
5. Modifica las directivas Servername y DocumentRoot acorde a las configuraciones del aula. (ejemplo: ServerName red[.aula11.local](http://www.aula11.local/) DocumentRoot /var/www/html/red)
6. Ejecuta el comando a2ensite por cada fichero de configuración (ejemplo: a2ensite red.conf)
7. Recarga apache: systemctl reload apache2
8. Modificamos el cliente dns /etc/resolv.conf para que consulte el dns de la clase y resuelva los nombres pertinentes. EN LAS CABECERAS DE HTTP SE ENVÍA EL FQDN.

## Creación de un certificado autofirmado para poder activar SSL

1. Generamos una clave (ojo al tamaño!!! mínimo 2048):
2. openssl genrsa -out w3.key 2048
3. Creamos una solicitud y contestamos los campos:
4. openssl req -new -key w3.key -out w3.csr
5. Nos lo firmamos nosotros mismos y le damos validez de un año:
6. openssl x509 -req -days 365 -in w3.csr -signkey w3.key -out w3.crt
7. Almacenamos las clave y certificado en sitio seguro:
8. cp w3.crt /etc/ssl/certs/ && cp w3.key /etc/ssl/certs/
9. Activamos el módulo de ssl:
10. a2enmod ssl
11. Creamos directorio /var/www/html/seguro y un index.html “significativo”
12. Creamos una web virtual llamada sec.conf (en sites-available) con algo parecido a esto (ajustado a los nombres del aula)

root@ubuntu:~# cat /etc/apache2/sites-available/sec.conf

<VirtualHost \*:443>

ServerName w3.aula11.local

DocumentRoot /var/www/html/seguro

SSLEngine on

SSLCertificateFile /etc/ssl/certs/w3.crt

SSLCertificateKeyFile /etc/ssl/certs/w3.key

</VirtualHost>

1. habilitamos el sitio con: a2ensite sec.conf
2. systemctl restart apache2

## AUTENTICACiÖN CON USUARIO

1. Creamos una cuenta de usuario:
   1. sudo htpasswd -c /etc/apache2/.htpasswd curso
2. Agregamos estas directivas a nuestro sitio virtual y quedaría algo similar a:

<VirtualHost \*:443>

ServerName w3.aula11.local

DocumentRoot /var/www/html/seguro

<Directory "/var/www/html/seguro">

AuthType Basic

AuthName "Restricted Content"

AuthUserFile /etc/apache2/.htpasswd

Require valid-user

</Directory>

SSLEngine on

SSLCertificateFile /etc/ssl/certs/w3.crt

SSLCertificateKeyFile /etc/ssl/certs/w3.key

</VirtualHost>

## PROPUESTA:

1. Crea certificados para cada Virtualhost
2. Redirecciona las peticiones http (80, puertoinseguro) a https con la directiva redirect permanent. Ejemplo:

<VirtualHost \*:80>

ServerName w3.aula11.local

ServerAlias w3.aula12.local

DocumentRoot /var/www/html/w3

Redirect permanent / https://w3.aula11.local

</VirtualHost>