# Practica 4

ADMINISTRACIÓN DE APACHE II

Paulo Gustavo Soares Teixeria

1. **Control de acceso por IP y nombre de dominio.**

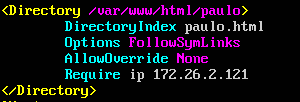
**Toma una captura de los pasos 3,4,5,6,7 y 9.**

**PASO 1)** Comprueba si está habilitado el módulo authz\_host. ¿Lo está? NO

**PASO 2)** Crea un directorio /var/www/html/tuNombre/. Dentro del directorio crea un archivo y llámalo tuNombre.html y añade el contenido que quieras.

**PASO 2)** Edita el fichero de configuración /etc/apache2/sites-available/000-default.conf y añade la directiva Directory para el recurso creado anteriormente.

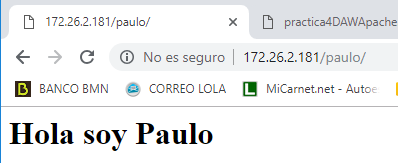
**PASO 3)** Añade dentro de la directiva anterior las directivas de acceso necesarias para que la máquina física, a partir de su dirección IP, pueda acceder a este recurso pero no el servidor Windows 2008.



**PASO 4)** Reinicia el servidor para que los cambios tengan efecto.



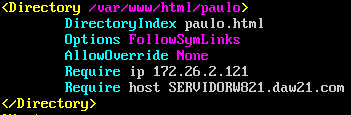
**PASO 5)** Abre un navegador desde tu máquina física e intenta acceder al recurso /tuNombre/ y comprueba que se puede.



**PASO 6)** Abre un navegador desde tu máquina servidor Windows 2008 e intenta acceder al recurso /tuNombre/ y comprueba que no se puede.

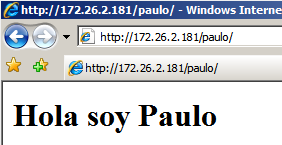


**PASO 7)** Añade el acceso al recurso de tu carpeta para el servidor windows 2008 pero usando su nombre de host en vez de su IP.



**PASO 8)** Reinicia el servidor para que los cambios tengan efecto.

**PASO 9)** Abre un navegador desde tu máquina servidor Windows 2008 e intenta acceder al recurso /tuNombre/ y comprueba que ahora sí se puede.



1. **Autenticación y autorización Basic y Digest.**

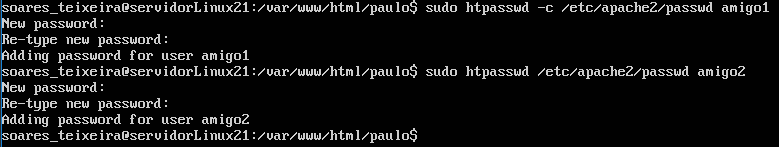
**B1) Autenticación Basic:**

**Toma capturas de los pasos 3,4, 6 y 7.**

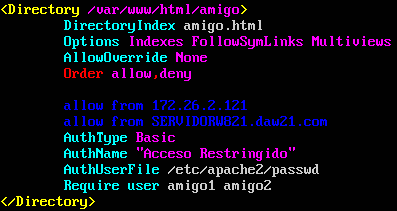
**PASO 1)** Comprueba si el módulo auth\_basic está habilitado, si no lo está, habilítalo.

**PASO 2)** Vamos a crear el directorio /amigo/ dentro de nuestro directorio raíz /var/www/html/. Dentro añadiremos un archivo amigo.html donde incluiremos el contenido que queramos.

**PASO 3)** Para usar la autenticación Basic hay que crear un fichero accesible (el fichero que se creará será /etc/apache2/passwd) en el que se guardarán los usuarios y contraseñas. Para crear ese fichero se utilizará el comando httpaswd (ver cuadro arriba). Añade los usuarios amigo1 y amigo2.

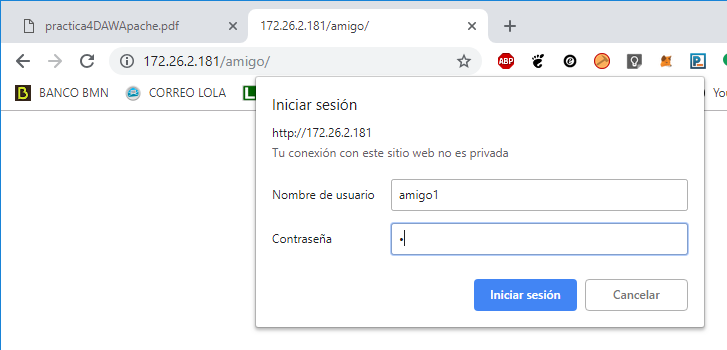


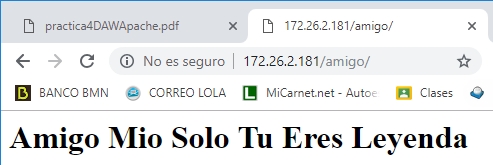
**PASO 4)** Edita el fichero de configuración /etc/apache2/sites-available/000-default.conf y permite el acceso al directorio /var/www/html/amigo a los usuarios amigo1 y amigo2 (ver cuadro ejemplo arriba).



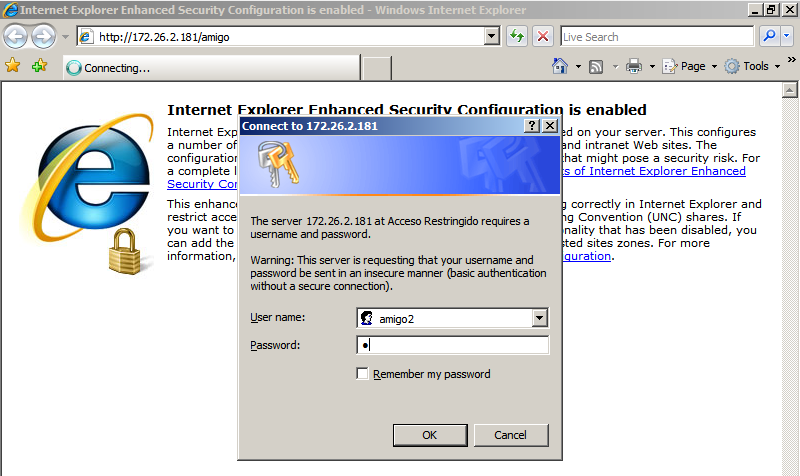
**PASO 5)** Reinicia el servidor para que los cambios tengan efecto.

**PASO 6)** Abre un navegador desde tu máquina física y accede al recurso /amigo como usuario amigo1.





**PASO 7)** Abre un navegador desde tu servidor Windows 2008 y accede al recurso /amigo como usuario amigo2.





**B2) Autenticación Digest:**

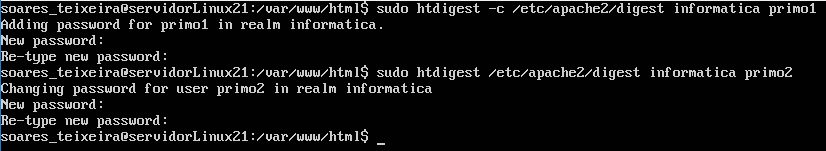
**Toma capturas de los pasos 3,4, 6 y 7.**

**Paso 1)** Comprueba si el módulo auth\_digest está habilitado, si no lo está, habilítalo.

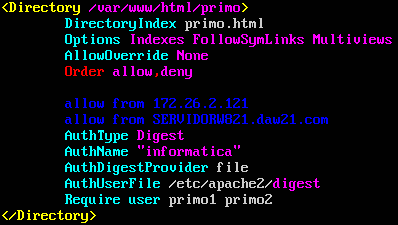
**PASO 2)** Vamos a crear el directorio /primo/ dentro de nuestro directorio raíz /var/www/html/. Dentro añadiremos un archivo primo.html donde incluiremos el contenido que queramos.

**PASO 3)** Para usar la autenticación Digest también hay que crear un fichero accesible (el fichero que se creará será también /etc/apache2/passwd pero para digest) en el que se guardarán los usuarios y contraseñas, pero esta vez asociados a un dominio (en el cuadro ejemplo de arriba el dominio o “realm” es informática). Para crear ese fichero se utilizará el comando httdigest (ver cuadro arriba).

Añade los usuarios primo1 y primo2.



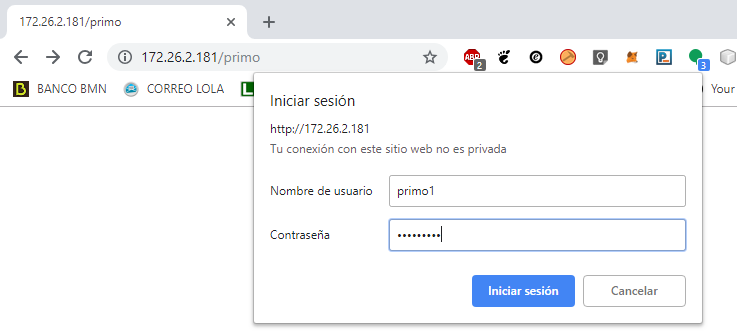
**PASO 4)** Edita el fichero de configuración /etc/apache2/sites-available/000-default.conf y permite el acceso al directorio /var/www/html/primo a los usuarios primo1 y primo2 (ver cuadro ejemplo arriba).

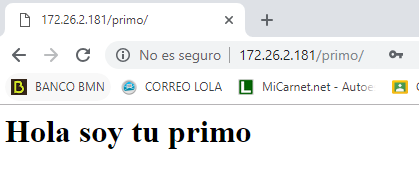


Ten en cuenta que en la directiva AuthName tienes que poner lo mismo que pusiste en el dominio o “realm”.

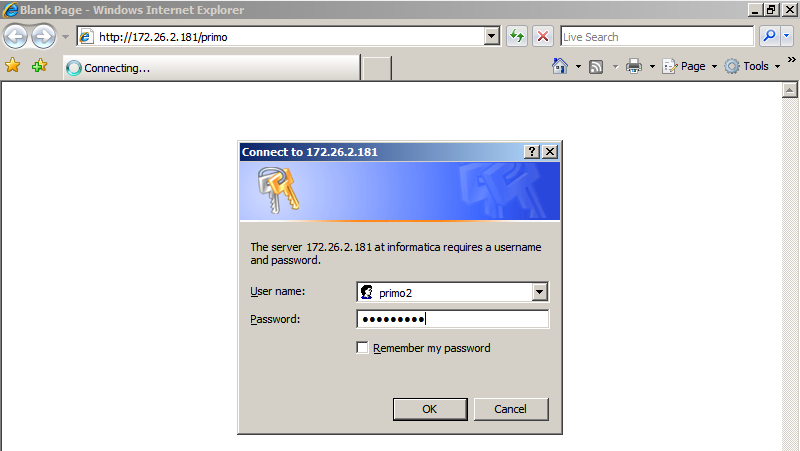
**PASO 5)** Reinicia el servidor para que los cambios tengan efecto.

**PASO 6)** Abre un navegador desde tu máquina física y accede al recurso /primo como usuario primo1.





**PASO 7)** Abre un navegador desde tu servidor Windows 2008 y accede al recurso /primo como usuario primo2.



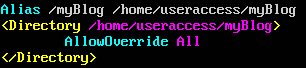


1. **Ficheros .htaccess.**

**Toma una captura de los pasos 2,6,7 y 8.**

**PASO 1)** Crea el usuario useraccess.

**PASO 2)** Abre el fichero de configuración 000-default y crea el alias myBlog dentro de la carpeta personal del nuevo usuario useraccess. Deja como única directiva AllowOverride All.

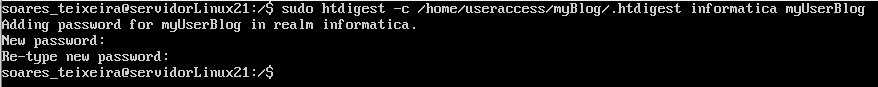


**PASO 3)** Reinicia el servidor para que los cambios tengan efecto.

**PASO 4)** Inicia sesión con el nuevo usuario useraccess.

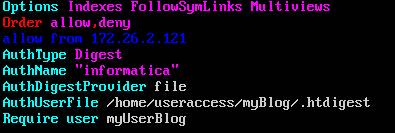
**PASO 5)** Crea dentro del directorio home de este usuario el directorio myBlog. Crea dentro el archivo myBlog.html con el contenido que quieras.

**PASO 6)** Para el acceso a los recursos de myBlog vamos a usar un tipo de autenticación Digest, por lo que dentro de este directorio vamos a crear el fichero .htdigest para el servidor informática y para el usuario myUserBlog (ver punto anterior acceso mediante Digest).

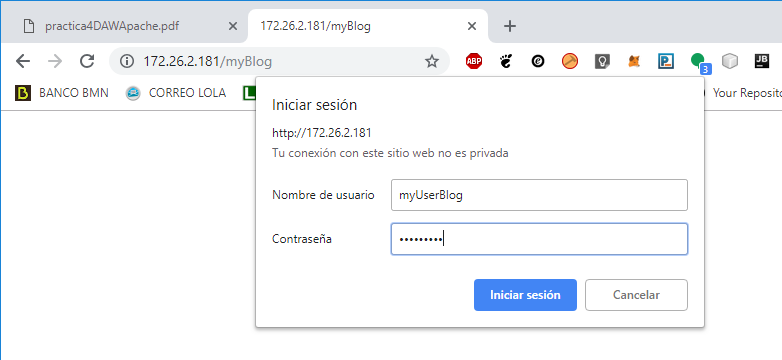


**PASO 7)** Ahora tendremos que crear el fichero .htaccess (también dentro de myBlog).

Dentro añadiremos las directivas necesarias para que se acceda solo desde nuestra máquina física (no es necesario poner las directivas Directory pues ya las incluimos en nuestro Alias para este directorio dentro de 000-default).



**PASO 8)** Vamos a acceder desde nuestra máquina física al recurso myBlog para ver que nos pide la autenticación y que podemos acceder al recurso.





1. **Ficheros de registros (logs).**

**Toma una captura de los pasos 2 y 3**

**PASO 1)** En tu servidor Linux, consulta el fichero 000-default y responde a las siguientes preguntas:

1. ¿qué directiva marca la ruta del archivo de los errores?

La Directiva es ErrorLog.

1. ¿Cuál es el fichero de logs de errores? ¿qué nivel de prioridad tiene?

El fichero es: error.log

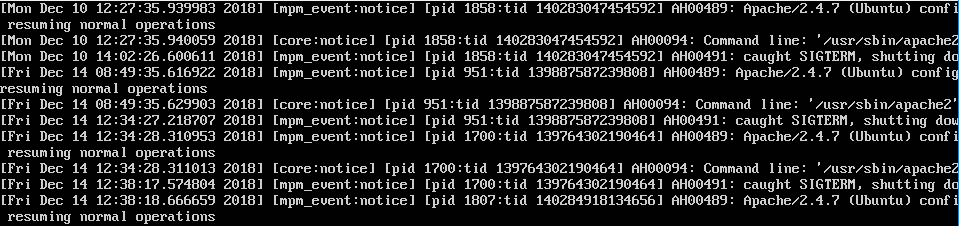
1. ¿qué directiva marca la ruta del archivo de los accesos?

El nivel es WARN.

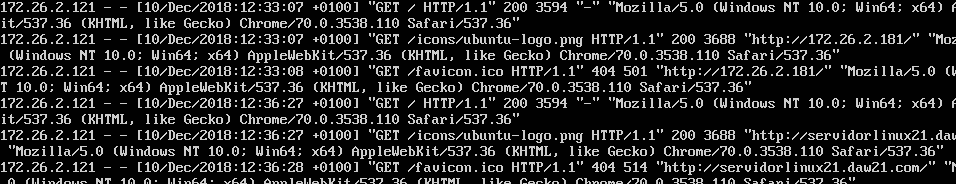
1. ¿Cuál es el fichero de logs de accesos?

El fichero es: Acces.log

**PASO 2)** Consulta el log de errores



**PASO 3)** Consulta el log de accesos



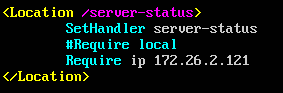
1. **Módulos status e info.**

**Toma una captura de los pasos 2 y 4, 6 y 8.**

**PASO 1)** En tu servidor Linux, habilita el módulo status.

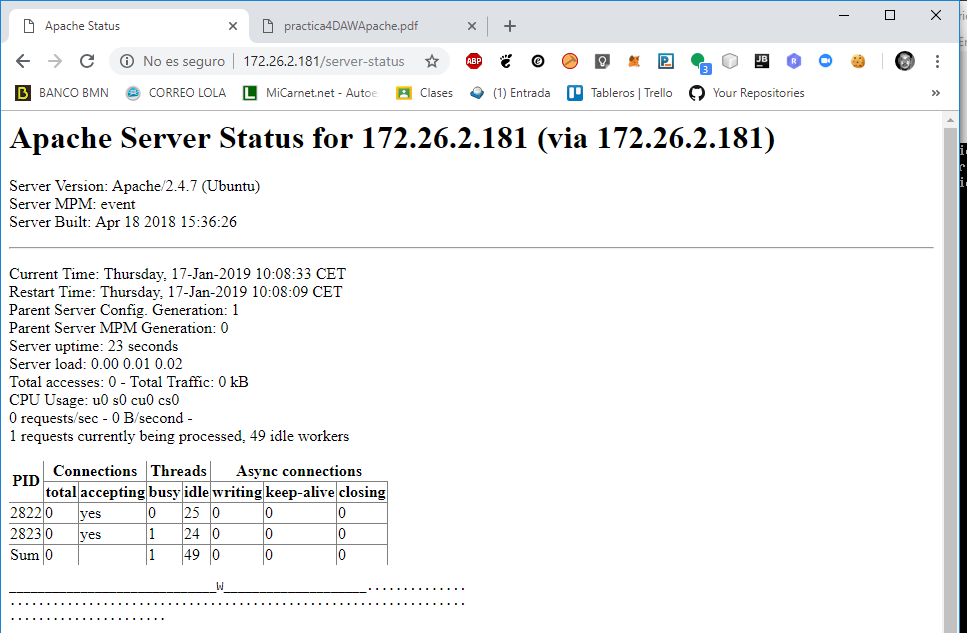
Habilito:

**PASO 2)** El fichero de configuración del módulo es status.conf, edita el fichero y habilita el acceso desde tu máquina física.



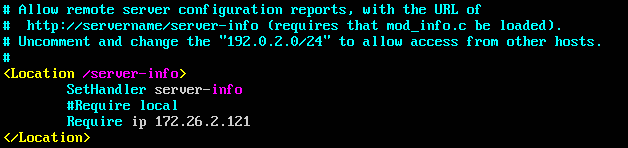
**PASO 3)** Reinicia el servidor para aplicar los cambios.

**PASO 4)** Desde tu máquina física conéctate al recurso server-status



**PASO 5)** En tu servidor Linux, habilita el módulo info.

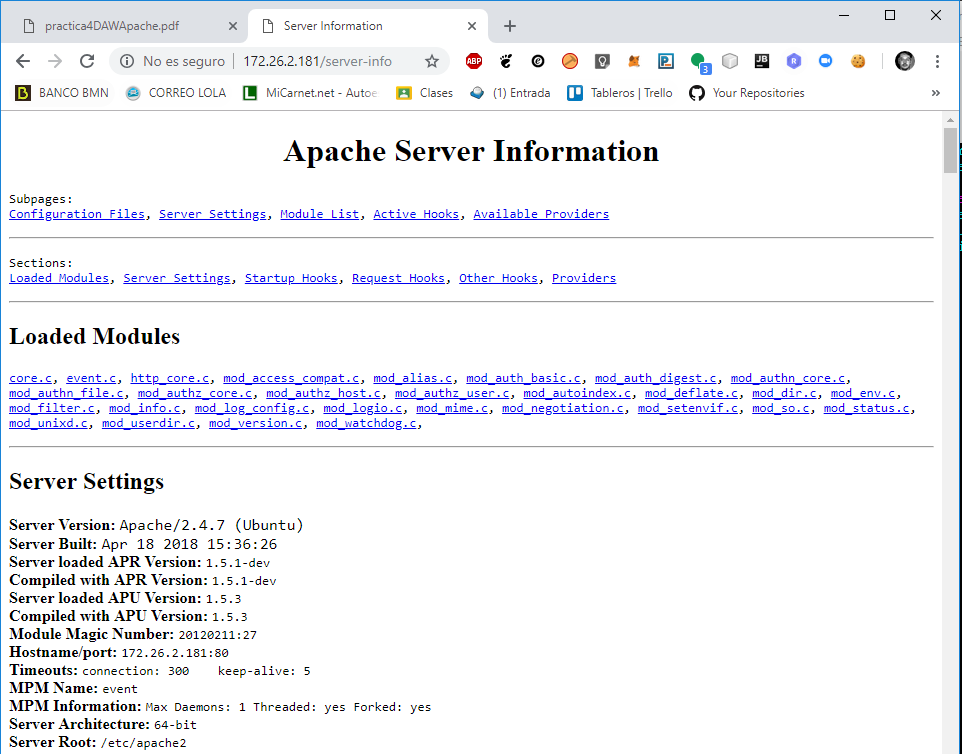
**PASO 6)** El fichero de configuración del módulo es info.conf, edita el fichero y habilita el acceso desde tu máquina física.



**PASO 7)** Reinicia el servidor para aplicar los cambios.

**PASO 8)** Desde tu máquina física conéctate al recurso server-info

Consulta el fichero server-info.



¿tienes cargado el módulo mod\_mime?



¿en caso que lo tuvieras, tiene el módulo cargada la configuración de caracteres UTF-32?

1. **Webalizer.**

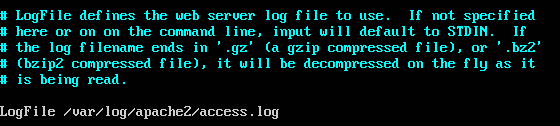
**Toma una captura de los pasos 2 y 5.**

**PASO 1)** En tu servidor Linux, instala la aplicación Webalizer (usa apt-get install, pero antes actualiza el servidor Linux).

**PASO 2)** Una vez instalado se habrá creado un directorio para la aplicación en el directorio /etc/.

Abre el fichero de configuración de webalizer.

* ¿de qué fichero log coge los datos para hacer las estadísticas?
  + Coge los datos del Access.log.
* ¿es correcta la ruta y el nombre del fichero? Si no es así, modifícala.
* La ruta si, el nombre no.



**PASO 3)** La instalación también implica la creación del recurso que se servirá desde el navegador.

¿Dónde está este fichero?

* + - Esta en var/www/html/webalizer

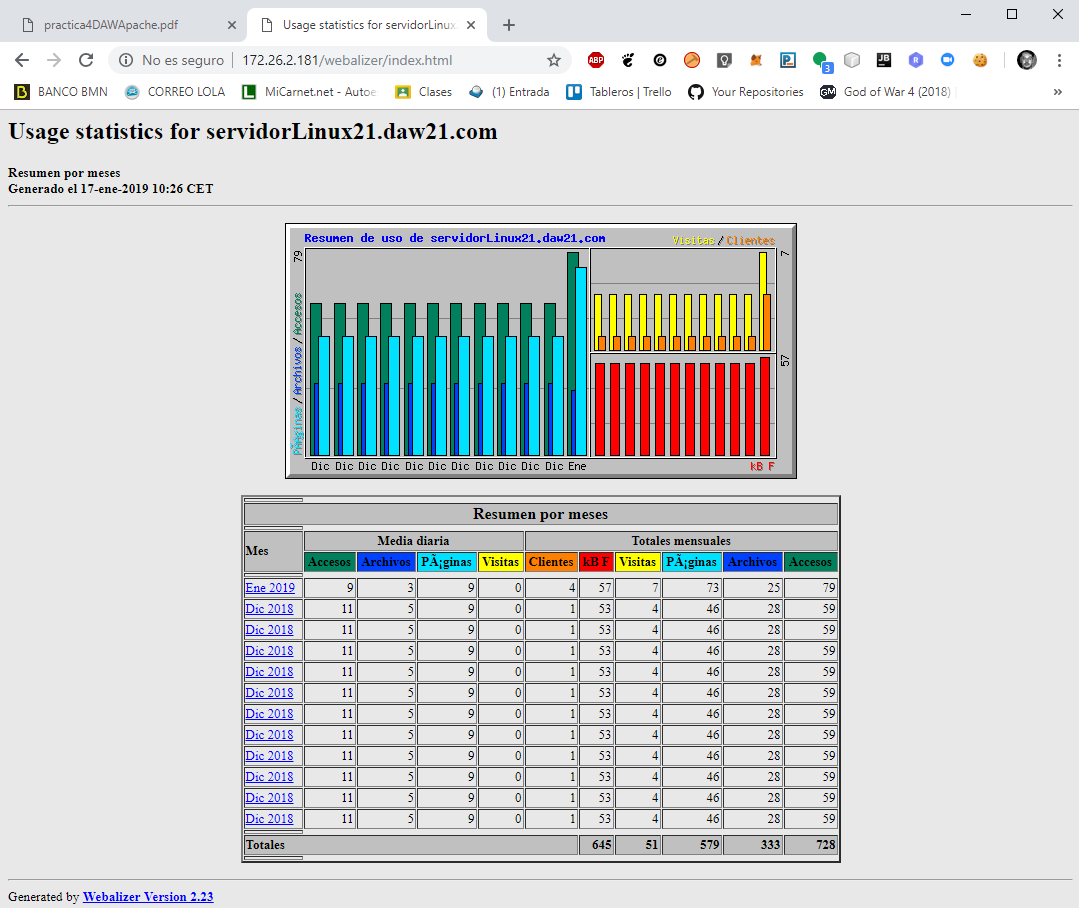
¿Es correcta la ubicación para servirlo? Si no es así, muévelo a la ubicación correcta.

* + - No es correcta como viene en el servidor.Lo modifico.
    - /var/www/html/webalizer

**PASO 4)** Lanza el programa (con permisos de administrador) para que lea el fichero de log correspondiente y genere el documento html con las estadísticas.

sudo webalizer.

**PASO 5)** Accede al recurso /webalizer/ desde tu máquina física.



1. **Alojamiento virtual de sitios web en Linux.**

**Toma una captura de los pasos 1, 7, 8, 9, 11, 13 y 16.**

**PASO 1)** Lo primero es que se puedan resolver estos nombres a partir de la IP de nuestro servidor Linux (asociar estos nombres con la dirección IP del servidor Linux). Tendremos que crear en nuestro servidor DNS (en el Windows Server) los registros correspondientes (tipo Address).



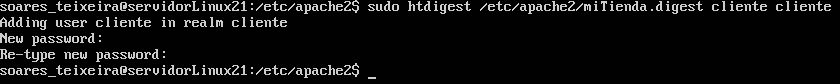
**PASO 2)** Deshabilita el servidor virtual por defecto 000-default.conf (una vez hecho, verifica que el archivo ya no está en sites-enabled).

**PASO 4)** Reinicia el servidor para que los cambios tengan efecto.

**PASO 5)** Crea el directorio /var/www/html/miTienda y dentro de éste el archivo index.html con el contenido que quieras.

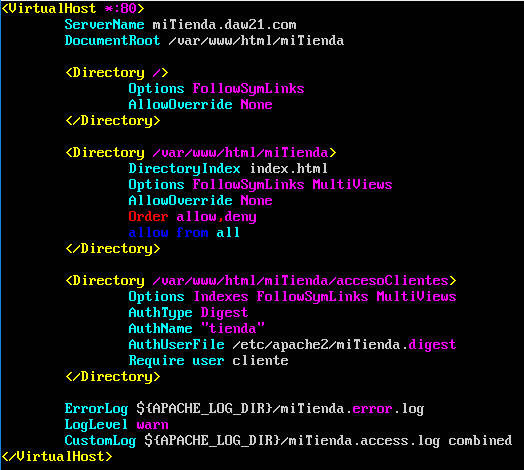
**PASO 6)** Crea el directorio accesoClientes dentro de miTienda. Dentro de éste, el archivo accesoClientes.html con el contenido que quieras.

**PASO 7)** Crea el fichero /etc/apache2/miTienda.digest y añade el usuario cliente al dominio tienda (revisa el uso de digest que usamos en puntos anteriores).



**PASO 8)** En este punto es donde crearemos el servidor virtual. Si te fijas, la estructura es la misma que la del servidor virtual por defecto 000-default.conf, pero las directivas ServerName y DocumentRoot son distintas.

Crea el fichero /etc/apache2/sites-available/miTienda.conf con las siguientes directivas:



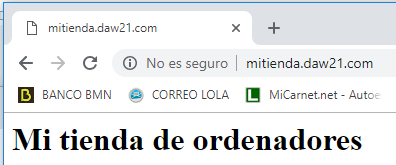
**PASO 9)** Habilita el servidor virtual miTienda y verifica que se ha creado el enlace en sites-enabled.

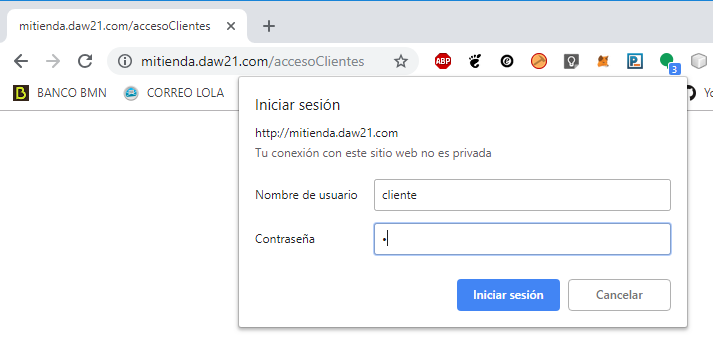


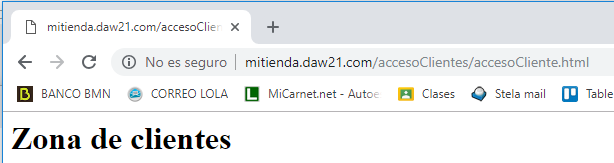


**PASO 10)** Reinicia el servidor para que los cambios tengan efecto.

**PASO 11)** Accede desde tu máquina física a miTienda.dawXX.com y a miTienda.dawXX.com/accesoClientes.

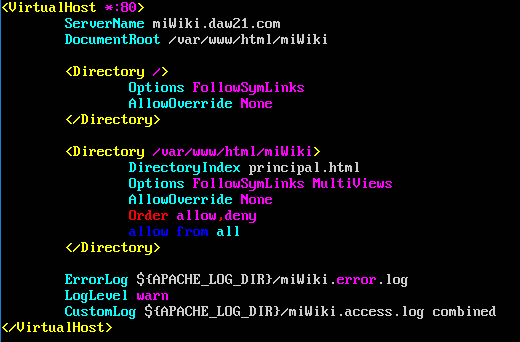






**PASO 12)** Crea el directorio /var/www/html/miWiki y dentro de éste el archivo principal.html con el contenido que quieras.

**PASO 13)** Crea el fichero /etc/apache2/sites-available/miWiki.conf, guíate por el fichero del servidor virtual que hemos creado anteriormente miTienda.conf



**PASO 14)** Habilita el servidor virtual miWiki y verifica que se ha creado el enlace en

sites-enabled.

**PASO 15)** Reinicia el servidor para que los cambios tengan efecto.

**PASO 16)** Accede desde tu máquina física a miWiki.dawXX.com, debe servir el archivo

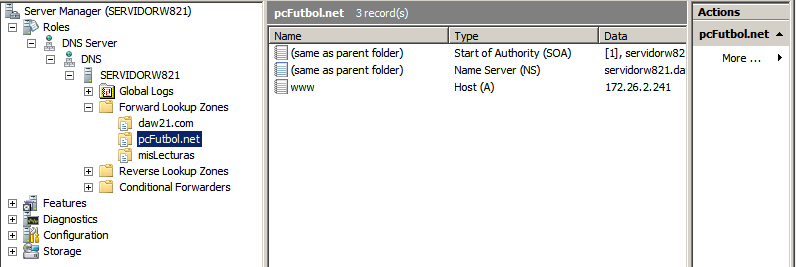
principal.html

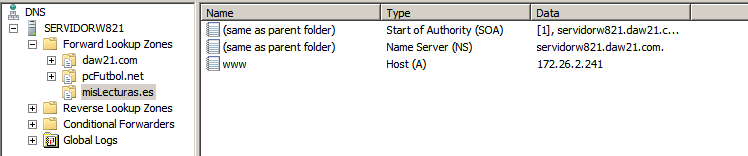


1. **Alojamiento virtual de sitios web en Windows.**

**Toma instantáneas de los puntos 1,2,3,4,5 y 7.**

**PASO 1:** Lo primero es que se puedan resolver estos nombres a partir de la IP de nuestro servidor Windows (asociar estos nombres con la dirección IP del servidor Windows). Tendremos que crear en nuestro servidor DNS (en el Windows Server) dos nuevas zonas.

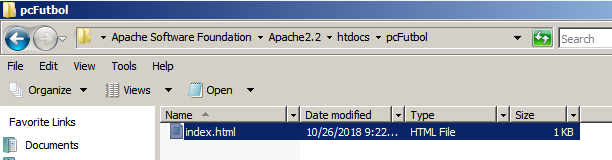
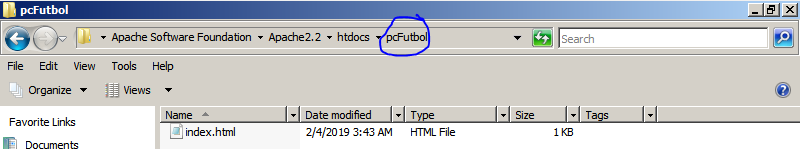




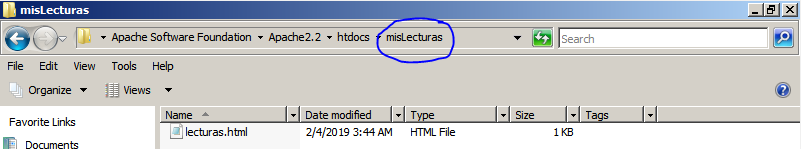
**PASO 2)** Ahora habilitaremos el módulo para el uso de servidores virtuales, quitando el comentario de la directiva include para httpd-vhosts.conf dentro del archivo httpd.conf



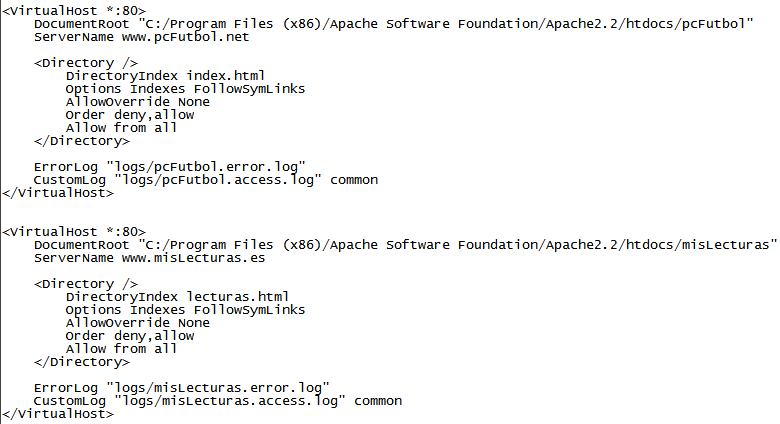
**PASO 3)** Dentro de la carpeta htdocs, crearemos la carpeta pcFutbol y dentro de ésta, el archivo index.html con el contenido que quieras.



**PASO 4)** Dentro de la carpeta htdocs, crearemos la carpeta misLecturas. Dentro de ésta, el archivo lecturas.html con el contenido que quieras.



**PASO 5)** Edita el fichero httpd-vhosts.conf e incluye las directivas para poder servir los contenidos creados anteriormente (te muestro el que necesitas para pcFutbol y tienes que construir el otro a partir de éste).



**PASO 6)** Reinicia el servidor para que los cambios tengan efecto.

**PASO 7)** Desde tu máquina física, accede a www.pcFutbol.net y a [www.misLecturas.es](http://www.misLecturas.es).



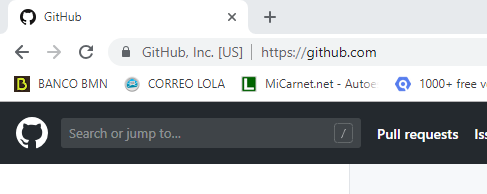


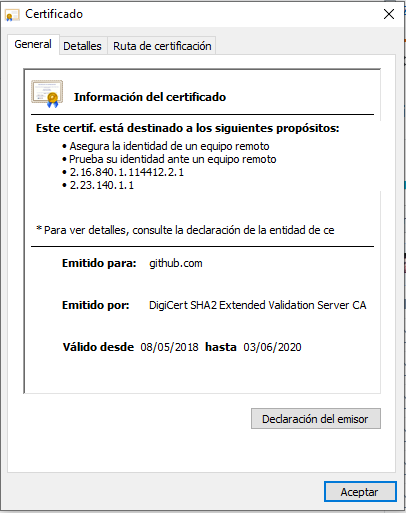


1. **HTTPS y Certificados Digitales.**

**Toma instantáneas de los puntos 1 y del certificado en el paso 3.**

**PASO 1)** Accede desde tu navegador a una página que use el protocolo https.





**PASO 2)** En la parte izquierda de la barra de direcciones, debe aparecer un candado indicando que la URL es segura. Si pinchas sobre el candado podrás acceder a la información sobre el certificado digital de la misma.

**PASO 3)** Accede al certificado digital y contesta las siguientes preguntas:

* ¿Qué algoritmo de clave pública usa el certificado?
  + El Algoritmo de clave publica es : ECC.
* ¿Para qué se usa el algoritmo de clave pública?
  + El Algoritmo de clave publica es aquel en el se basa en el uso de una pareja de clave pública y privada de las cuales una se usa para cifrar y otra para descifrar.
* ¿De qué tamaño es la clave pública del certificado?
  + 256 bits
* ¿Qué algoritmo de firma usa el certificado?
  + Sha256.
* ¿Qué longitud tiene?
  + 256 bits.
* ¿Qué autoridad de certificación ha firmado el certificado?
  + Google Internet Authority G3.

1. **Servidor virtual HTTPS por defecto en Linux.**

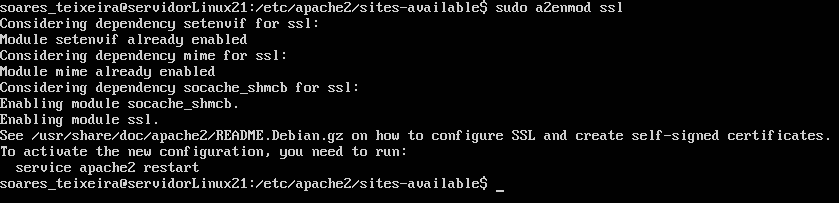
**Toma instantáneas del punto 4,6,8,10,11,12,13**

**PASO 1)** Habilita el servidor virtual por defecto en apache. Verifica que se ha habilitado correctamente.

**PASO 2)** Deshabilita los servidores virtuales creados en puntos anteriores.

**PASO 3)** Reinicia el servidor para que los cambios tengan efecto.

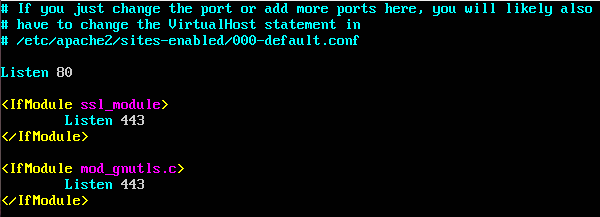
**PASO 4)** Habilita el módulo ssl para poder hacer uso de servidores virtuales seguros.



**PASO 5)** Reinicia el servidor para que los cambios tengan efecto.

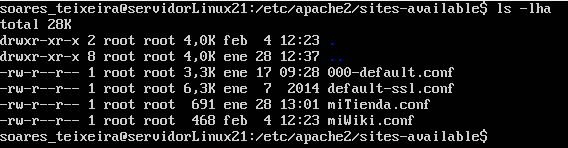
**PASO 6)** Consulta el fichero port.conf en etc/apache2/.

* ¿En qué puerto escucha el servidor por defecto?
  + Se ESCUCHA POR EL 80.
* ¿Qué puerto está a la escucha si habilitamos el módulo ssl?
  + 443
* ¿Qué directiva lo marca?
  + ifModule ssl\_module>

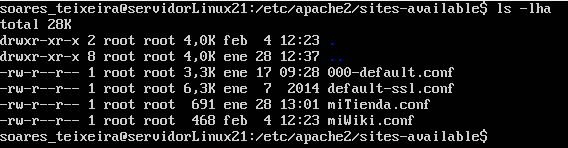


**PASO 7)** Verifica que los puertos para el servidor apache están realmente a la escucha mediante el comando netstat –ltn

**PASO 8)** Accede al directorio sites-available y realiza un listado,



* ¿qué archivo hay en este directorio para que podamos definir servidores virtuales seguros? Habilítalo.
  + El archivo es default-ssl.conf.
  + HABILITADO



**PASO 9)** Reinicia el servidor.

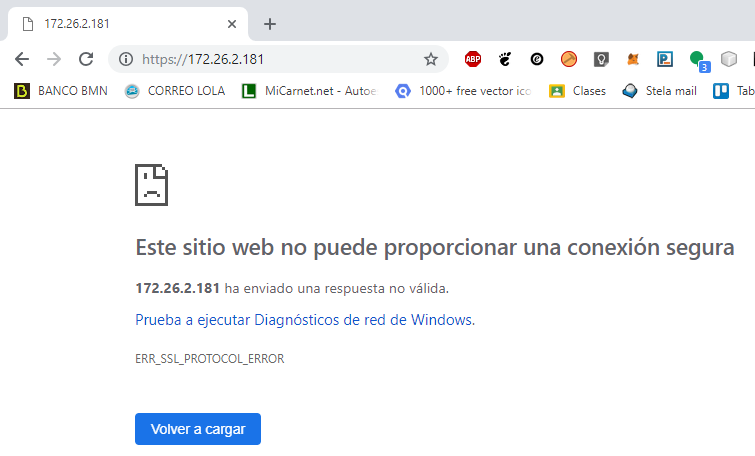
**PASO 10)** Abre el archivo indicado en el paso 8.

* ¿en qué ruta se deben guardar los certificados SSL en apache?
  + /etc/ssl/certs
* ¿y las claves (key)?
  + /etc/ssl/private

**PASO 11)** Desde tu máquina física, abre un navegador y establece una conexión http con el servidor Linux.



**PASO 12)** Establece una conexión https con el servidor Linux.

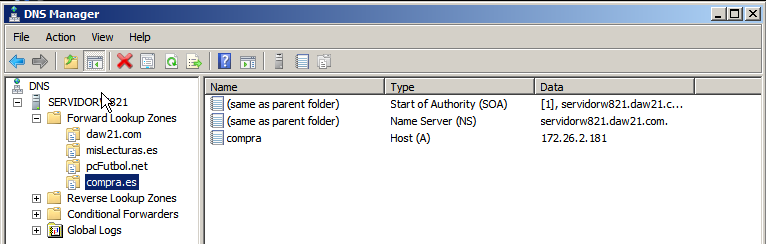


**PASO 13)** Acepta el acceso. ¿el certificado está expedido por una autoridad certificadora o es autofirmado?

1. **Creación de un servidor virtual HTTPS en Linux.**

**Toma capturas de los puntos 1,3,4,6 y 9**

**PASO 1)** Lo primero es que se puedan resolver el nombre de nuestro nuevo servidor virtual a partir de la IP de nuestro servidor Linux. Tendremos que crear en nuestro servidor DNS (que está en el servidor Windows) un registro para nuestro nuevo servidor virtual.



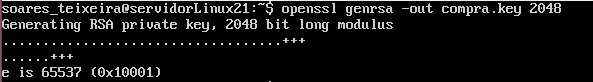
**PASO 2)** En el servidor Linux, crea el directorio /compra en /var/www/html/ y crea dentro el fichero index.html con el contenido que quieras.

**PASO 3)** Vamos a crear un certificado digital autofirmado usando el comando openssl.

- Sitúate en el directorio home del usuario con el que has iniciado sesión.

- Crea una clave privada tipo RSA de 2048 bits usando el siguiente comando:

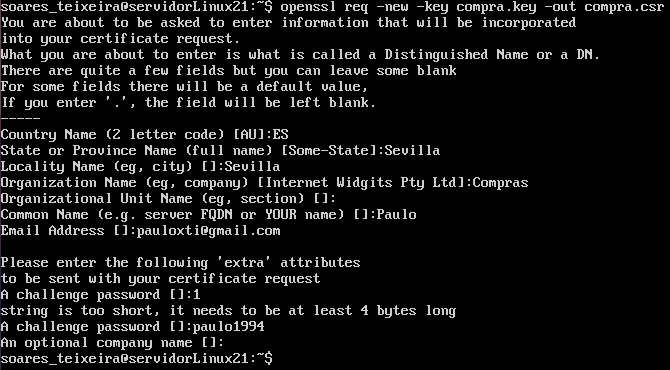
**openssl genrsa –out compra.key 2048**



- Genera una solicitud de certificado, a partir de la clave creada en el paso anterior,

usando el siguiente comando (inventa los datos introducidos):

**openssl req –new –key compra.key –out compra.csr**

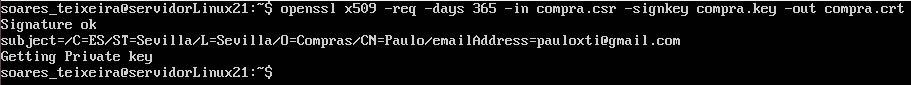


Esta solicitud de certificado se podría enviar a una autoridad de certificación para que nos generase un certificado CRT avalado por una entidad certificadora. Nosotros vamos a autofirmar el certificado para generarlo nosotros mismos.

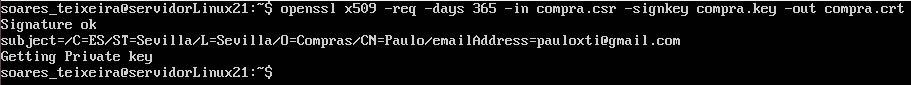
- Crea el certificado digital autofirmado usando la clave privada y la solicitud de certi-

ficado generados anteriormente. Usa el siguiente comando:

**openssl x509 –req –days 365 –in compra.csr –signkey compra.key –out compra.crt**



**PASO 4)** Mueve la clave (.key) y el certificado (.crt) a los directorios que utiliza por defecto Apache para guardar los certificados y las claves (paso 10 punto anterior).





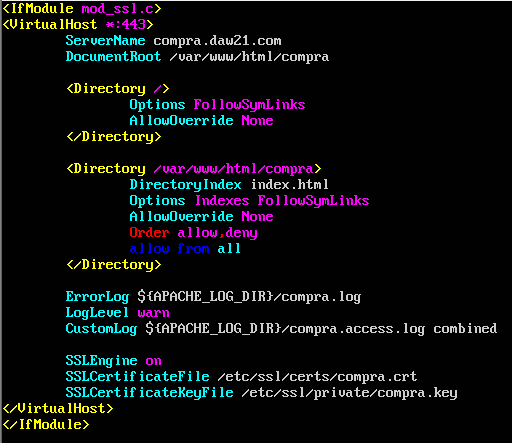
**PASO 5)** Configura los permisos adecuados de la siguiente manera.

**sudo chown root:ssl-cert /etc/..../compra.key**

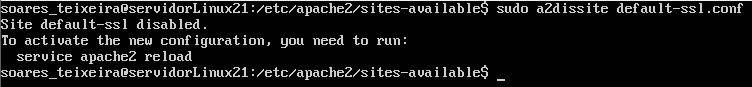
**sudo chmod 640 /etc/.../compra.key**

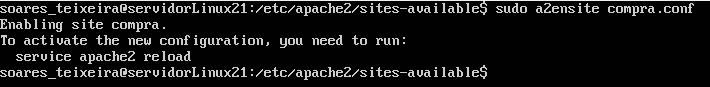
**sudo chown root:root /etc/.../compra.crt**

**PASO 6)** Crea el fichero compra.conf en el directorio correspondiente dentro de la estructura de apache2. Añade a las directivas SSLCertificateFile y SSLCertificateKeyFile las rutas necesariode los archivos compra.crt y compra.key



**PASO 7)** Deshabilita el servidor ssl por defecto y habilita compra.conf.





**PASO 8)** Reinicia el servidor para que los cambios tengan efecto.

**PASO 9)** Desde tu máquina física, abre un navegador y establece una conexión

https://compra.dawXX.com, permite en tu navegador el acceso a la página y abre el certificado

para ver la información.

* Del acceso inicial cuando aún no has aceptado el certificado
* Del acceso una vez aceptado el certificado.
* Del propio certificado digital cuando accedas a él