

A thick dark green vertical bar is positioned on the left side of the page. A light green arrow-shaped banner points to the right from this bar, containing the date. Below the banner, several thin, curved lines in dark green and light grey sweep upwards from the bottom left corner.

25-11-2022

Tarea 2.2.

Servidor Web módulos

DAW

Manuel Ruiz Jimenez
2ºDAW

Índice

Tarea 2.2. Servidor Web módulos	1
A) Módulos en Linux	1
A.1) Módulos	2
A.2) Módulo userdir	4
A.3) Módulo userdir en el servidor de clase	7
B) Control de acceso por IP y nombre de dominio	8
C) Autenticación y autorización Basic y Digest	13
C.1) Autenticación Basic	14
C.2) Autenticación Digest	17
D) Ficheros .htaccess (si no sale poner pantallazo de haberlo intentado)	21
E) Ficheros de registros (logs)	24
F) Módulos status e info	27
G) Webalizer	31
F) GitHub	33



Tarea 2.2. Servidor Web módulos

A) Módulos en Linux

El servidor HTTP Apache es **MODULAR**, lo cual quiere decir que se pueden añadir módulos para darle otras funcionalidades al servidor HTTP. En este apartado vamos a ver como se cargan nuevos módulos y como se descargan dichos módulos en Linux y le daremos uso.

Existen módulos estáticos, que se cargan al compilar el servidor y se pueden ver mediante el comando:

```
sudo apache2ctl -l
```

También existen módulos dinámicos, los cuales pueden cargarse y descargarse de manera dinámica. En Linux, los módulos disponibles se encuentran en el directorio

```
/etc/apache2/mods-available/
```

Los archivos **.load** sirven para cargar el módulo y los **.conf** para configurarlo.

Mientras que los módulos que están cargados se encuentran en el directorio

```
/etc/apache2/mods-enabled/
```

Para habilitar y deshabilitar módulos se usan los comandos:

```
a2enmod nombre_del_modulo  
a2dismod nombre_del_modulo
```

Cada vez que se carga/descarga un módulo, tendrás que reiniciar el servidor Apache.

Los módulos existentes se pueden consultar en: <http://httpd.apache.org/docs/2.2/mod/>



A.1) Módulos

PASO 1) Comprueba los módulos estáticos que se han cargado al compilar el servidor ejecutando el comando correspondiente.

```

ruiz_jimenez@ServidorLinuxmrj:~$ sudo apache2ctl -l
Compiled in modules:
  core.c
  mod_so.c
  mod_watchdog.c
  http_core.c
  mod_log_config.c
  mod_logio.c
  mod_version.c
  mod_unixd.c
ruiz_jimenez@ServidorLinuxmrj:~$
  
```

Estos son los módulos compilados.

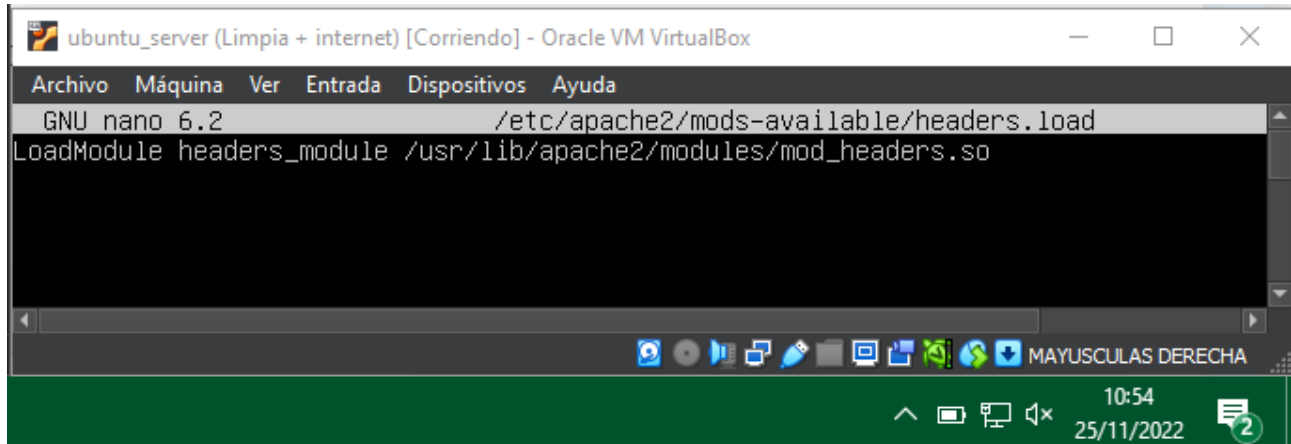
PASO 2) Comprueba los módulos que se han cargado dinámicamente al arrancar el servidor.

```

ubuntu_server (Limpia + internet) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

access_compat.load  cgi.load  log_debug.load  ratelimit.load
actions.conf        charset_lite.load  log_forensic.load  reflector.load
actions.load        data.load  lua.load  remoteip.load
alias.conf          dav_fs.conf  macro.load  reqtimeout.conf
alias.load          dav_fs.load  md.load  reqtimeout.load
allowmethods.load  dav.load  mime.conf  request.load
asis.load           dav_lock.load  mime.load  rewrite.load
auth_basic.load     dbd.load  mime_magic.conf  sed.load
auth_digest.load    deflate.conf  mime_magic.load  session_cookie.l
auth_form.load      deflate.load  mpmm_event.conf  session_crypto.l
authn_anon.load     dialup.load  mpmm_event.load  session_dbd.load
authn_core.load     dir.conf  mpmm_prefork.conf  session.load
authn_dbd.load      dir.load  mpmm_prefork.load  setenvif.conf
authn_dbm.load      dump_io.load  mpmm_worker.conf  setenvif.load
authn_file.load     echo.load  negotiation.conf  slotmem_plain.lo
authn_socache.load  env.load  negotiation.load  slotmem_shm.load
authnz_fcgi.load    expires.load  proxy_balancer.conf  socache_dbm.load
authnz_ldap.load    ext_filter.load  proxy_balancer.load  socache_memcache
authnz_core.load    file_cache.load  proxy.conf  socache_redis.lo
authnz_dbd.load     filter.load  proxy_connect.load  socache_shmcb.lo
authnz_dbm.load     headers.load  proxy_express.load  spelling.load
authnz_groupfile.load  heartbeat.load  proxy_fcgi.load  ssl.conf
authnz_host.load    http2.conf  proxy_fcgi.load  ssl.load
authnz_owner.load   http2.load  proxy_fdpass.load  status.conf
authnz_user.load    ident.load  proxy_ftp.conf  status.load
autoindex.conf      imagemap.load  proxy_ftp.load  substitute.load
autoindex.load      include.load  proxy_hcheck.load  suexec.load
brotli.load         info.conf  proxy_html.conf  unique_id.load
buffer.load         info.load  proxy_html.load  userdir.conf
cache_disk.conf     lbmethod_bybusyness.load  proxy_http2.load  userdir.load
cache.load          lbmethod_byrequests.load  proxy_http.load  usertrack.load
cache_socache.load  lbmethod_bytraffic.load  proxy.load  vhost_alias.load
cern_meta.load      lbmethod_heartbeat.load  proxy_scgi.load  xml2enc.load
cgid.conf           ldap.conf  proxy_uwsgi.load
cgid.load           ldap.load  proxy_wstunnel.load
ruiz_jimenez@ServidorLinuxmrj:~$ _
  
```

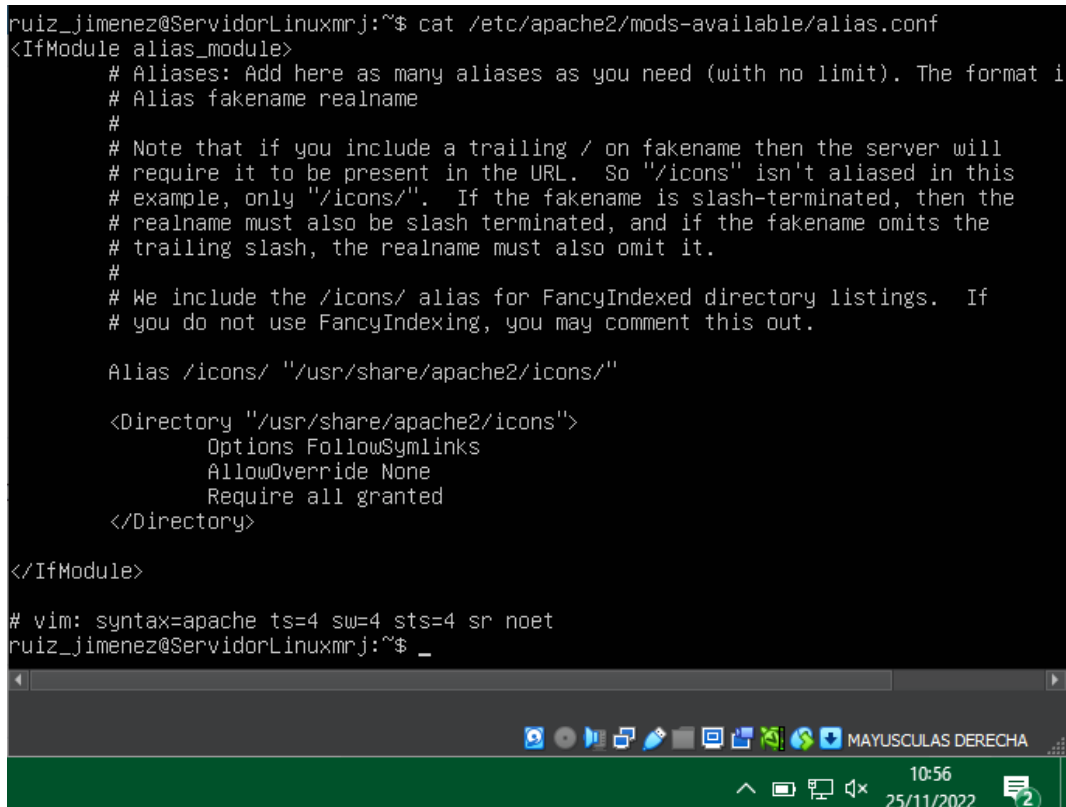
PASO 3) Edita uno de los archivos `.load` y observa cómo se usa la directiva `LoadModule`. ¿Qué extensión tienen los archivos donde está el código del módulo?



```
ubuntu_server (Limpia + internet) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 6.2 /etc/apache2/mods-available/headers.load
LoadModule headers_module /usr/lib/apache2/modules/mod_headers.so
```

La extensión es `.so`

PASO 4) Edita uno de los archivos `.conf` y observa cómo se añaden directivas dentro del módulo. ¿Qué etiquetas se utilizan en estos archivos?



```
ruiz_jimenez@ServidorLinuxmrj:~$ cat /etc/apache2/mods-available/alias.conf
<IfModule alias_module>
    # Aliases: Add here as many aliases as you need (with no limit). The format is
    # Alias fakename realname
    #
    # Note that if you include a trailing / on fakename then the server will
    # require it to be present in the URL. So "/icons" isn't aliased in this
    # example, only "/icons/". If the fakename is slash-terminated, then the
    # realname must also be slash terminated, and if the fakename omits the
    # trailing slash, the realname must also omit it.
    #
    # We include the /icons/ alias for FancyIndexed directory listings. If
    # you do not use FancyIndexing, you may comment this out.

    Alias /icons/ "/usr/share/apache2/icons/"

    <Directory "/usr/share/apache2/icons">
        Options FollowSymLinks
        AllowOverride None
        Require all granted
    </Directory>
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
ruiz_jimenez@ServidorLinuxmrj:~$ _
```

Se usa la etiqueta `Directory`.



Unión Europea

Fondo Social Europeo
"El FSE invierte en tu futuro"

PASO 5) Consulta el directorio `/usr/lib/apache2/modules/` ¿qué archivos contiene?

Contiene archivos con extensión `.so`

A.2) Módulo userdir

El módulo **userdir** se utiliza para usar como directorio raíz del servidor HTTP el directorio home de un usuario.

Al utilizar este módulo, el usuario desde el que se va a usar, en el directorio raíz (`/home/usuario`) tendrá un directorio `public_html` que hará las veces de raíz web para Apache2.

En el caso de directorios raíz de usuarios, para acceder a ellos habrá que usar el carácter `~`, o sea, la dirección será de la forma <http://hostname/~username/>

PASO 1) Comprueba si el módulo `userdir` está habilitado. ¿Lo está?

No está activo

PASO 2) Si no lo está, habilita el módulo `userdir`.

```
ruiz_jimenez@ServidorLinuxmrj:~$ sudo a2enmod userdir
[sudo] password for ruiz_jimenez:
Enabling module userdir.
To activate the new configuration, you need to run:
  systemctl restart apache2
ruiz_jimenez@ServidorLinuxmrj:~$
```

```
ruiz_jimenez@ServidorLinuxmrj:~$ sudo systemctl restart apache2
ruiz_jimenez@ServidorLinuxmrj:~$ _
```

PASO 3) Verifica ahora si el módulo está habilitado.

```
ruiz_jimenez@ServidorLinuxmrj:~$ ls /etc/apache2/mods-enabled/
access_compat.load  authz_core.load    deflate.load       mime.load          reqtimeout.load    userdir.load
alias.conf          authz_host.load    dir.conf           mpm_event.conf     setenvif.conf
alias.load          authz_user.load    env.load           negotiation.conf   setenvif.load
auth_basic.load     autoindex.conf     filter.load        negotiation.load    status.conf
authn_core.load     autoindex.load     filter.load        negotiation.load    status.load
authn_file.load     deflate.conf        mime.conf          reqtimeout.conf     userdir.conf
ruiz_jimenez@ServidorLinuxmrj:~$ _
```

Como podemos ver los dos últimos son referente a userdir

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

PASO 5) Consulta el archivo `/etc/apache2/mods-enabled/userdir.conf`. ¿Cuál es el único usuario para el que está deshabilitado el uso de directorios personales? ¿Cuál es el subdirectorio que deben crear los usuarios en su carpeta home para poner sus páginas personales?

```
ruiz_jimenez@ServidorLinuxmrj:~$ cat /etc/apache2/mods-enabled/userdir.conf
<IfModule mod_userdir.c>
    UserDir public_html
    UserDir disabled root

    <Directory /home/*/public_html>
        AllowOverride FileInfo AuthConfig Limit Indexes
        Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
        Require method GET POST OPTIONS
    </Directory>
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
ruiz_jimenez@ServidorLinuxmrj:~$
```

El único usuario deshabilitado es root.

Tienen que crear la carpeta `public_html`.



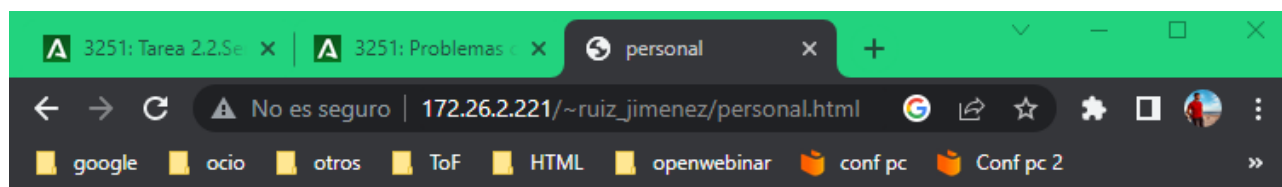
PASO 6) Crea el directorio necesario dentro de tu usuario y añade un fichero denominado **personal.html** con el contenido Tu nombre e indicando que es personal.

PASO 7) Desde la máquina física, abre un navegador y accede al directorio raíz de tu usuario Linux.

Index of /~profe

Name	Last modified	Size	Description
Parent Directory	-	-	-
personal.html	2016-11-22 19:55	38	-

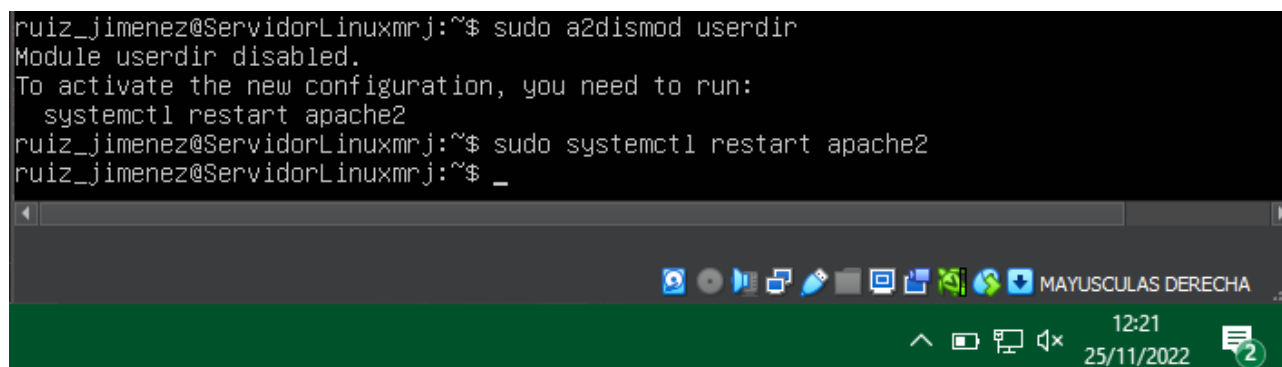
Apache/2.4.18 (Ubuntu) Server at 192.168.1.151 Port 80



Personal Manuel Ruiz Jimenez



PASO 8) Descarga el módulo y reinicia el servidor para que los cambios tengan efecto.



Toma una captura de los pasos 3,5 y 7 (en esta última, donde se vea la barra de direcciones del navegador)



Unión Europea

Fondo Social Europeo
"El FSE invierte en tu futuro"

A.3) Módulo userdir en el servidor de clase

En el servidor del aula todos tenéis un usuario y una contraseña para entrar.

Recordad que es la inicial del primer nombre y el primer apellido.

Ejemplo: Amapola Gutiérrez de la Vega, sería agutierrez. La contraseña es alumno.

PASO 1) Accede al servidor a través de Putty. IP: 172.26.255.254

```
172.26.255.254 - PuTTY
login as: mruiz
mruiz@172.26.255.254's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-132-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of vie 02 dic 2022 09:45:00 UTC

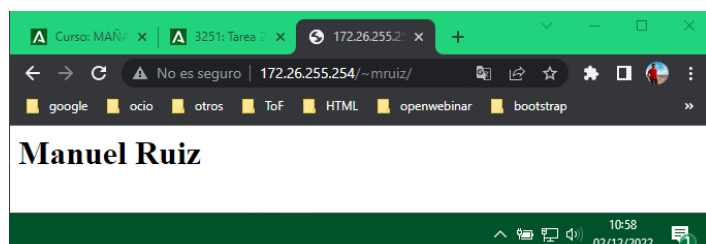
System load:  0.0               Temperature:   28.0 C
Usage of /:   17.4% of 54.22GB   Processes:    155
Memory usage: 17%              Users logged in: 2
Swap usage:   0%               IPv4 address for enp2s0: 172.26.255.254

0 updates can be applied immediately.
```

PASO 2) Da los pasos necesarios para qué al acceder a <http://172.26.255.254/~agutierrez> se vea tu página web en el servidor.

```
172.26.255.254 - PuTTY
$ mkdir public_html
mkdir: cannot create directory 'public_html': File exists
$ touch public_html/index.html
$ nano public_html/index.html
```

Primero creamos la carpeta public_html y dentro de ella un index.html en el que escribiremos el código html



La página debe contener la IP de servidor y tu nombre completo

B) Control de acceso por IP y nombre de dominio

Para poder controlar el acceso a diferentes recursos dentro de nuestro servidor web podemos hacer uso del módulo **authz_host**. Este módulo puede permitir o denegar el acceso a un recurso por parte de un host a partir de su dirección IP o su nombre de dominio.

Más información del módulo en: https://httpd.apache.org/docs/2.4/mod/mod_authz_host.html

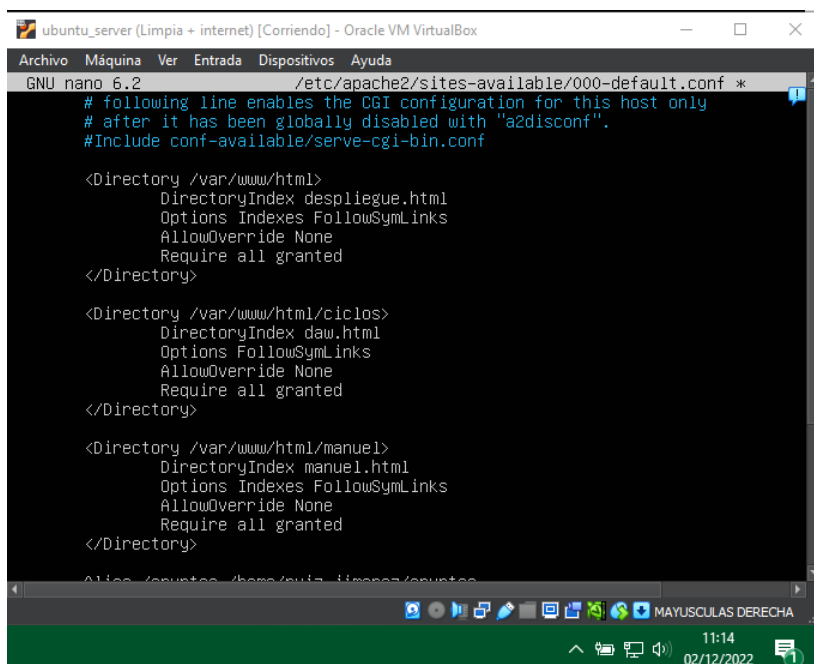
Vamos a controlar el acceso a un recurso de Apache en nuestro servidor Linux para que la máquina física tenga acceso, y la máquina de un compañero no:

PASO 1) Comprueba si está habilitado el módulo **authz_host**. ¿Lo está?

Si esta habilitado

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



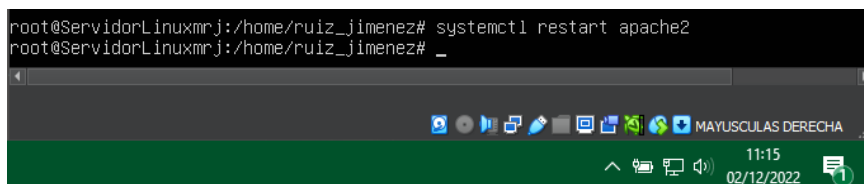
```
ubuntu_server (Limpia + internet) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 6.2 /etc/apache2/sites-available/000-default.conf *
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf

<Directory /var/www/html>
    DirectoryIndex despliegue.html
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

<Directory /var/www/html/ciclos>
    DirectoryIndex daw.html
    Options FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

<Directory /var/www/html/manuel>
    DirectoryIndex manuel.html
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

Alias /runtest /home/ruiz_jimenez/runtest
```



```
root@ServidorLinuxmrj:/home/ruiz_jimenez# systemctl restart apache2
root@ServidorLinuxmrj:/home/ruiz_jimenez# _
```

PASO 4) 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 la máquina del compañero (échale un vistazo al enlace informativo del módulo `authz_host` que hay más arriba).

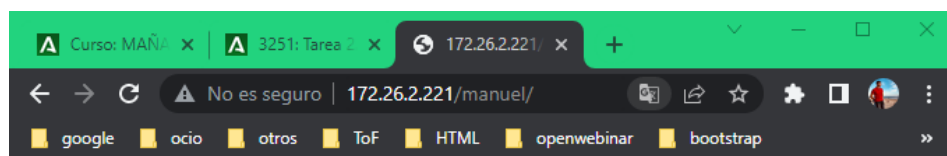
```
<Directory /var/www/html/manuel>
    DirectoryIndex manuel.html
    Options Indexes FollowSymLinks
    AllowOverride None
    Require ip 172.26.2.221 172.26.58.171
</Directory>

Alias /apuntes /home/ruiz_jimenez/apuntes
<Directory /home/ruiz_jimenez/apuntes>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

vidorLinuxmrj:/home/ruiz_jimenez# systemctl restart apache2
vidorLinuxmrj:/home/ruiz_jimenez#
```

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

PASO 6) Abre un navegador desde tu máquina física e intenta acceder al recurso `/tuNombre/` y comprueba que se puede.



Manuel Ruiz



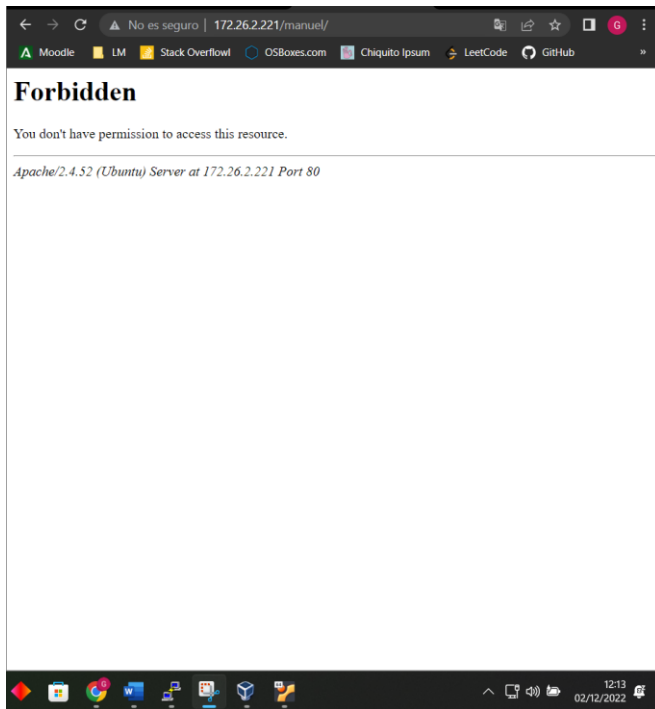
Esto sería desde mi ordenador personal



Unión Europea

Fondo Social Europeo
"El FSE invierte en tu futuro"

PASO 7) Abre un navegador desde la máquina del compañero e intenta acceder al recurso **/tuNombre/** y comprueba que no se puede.



Y esta sería desde el ordenador de mi compañero Guillermo

Desde mi máquina física:



Desde la máquina del compañero:



PASO 8) Añade el acceso al recurso de tu carpeta para la máquina del compañero, pero **usando su nombre de host en vez de su IP**.

```
ubuntu_server (Limpia + internet) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 6.2 /etc/hosts
127.0.0.1 localhost
127.0.1.1 servidor_mrj
127.0.1.1 ServidorLinuxmrj
172.26.26.110 guille
# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Añadimos al archivo /etc/hosts la ip de nuestro compañero con un nombre

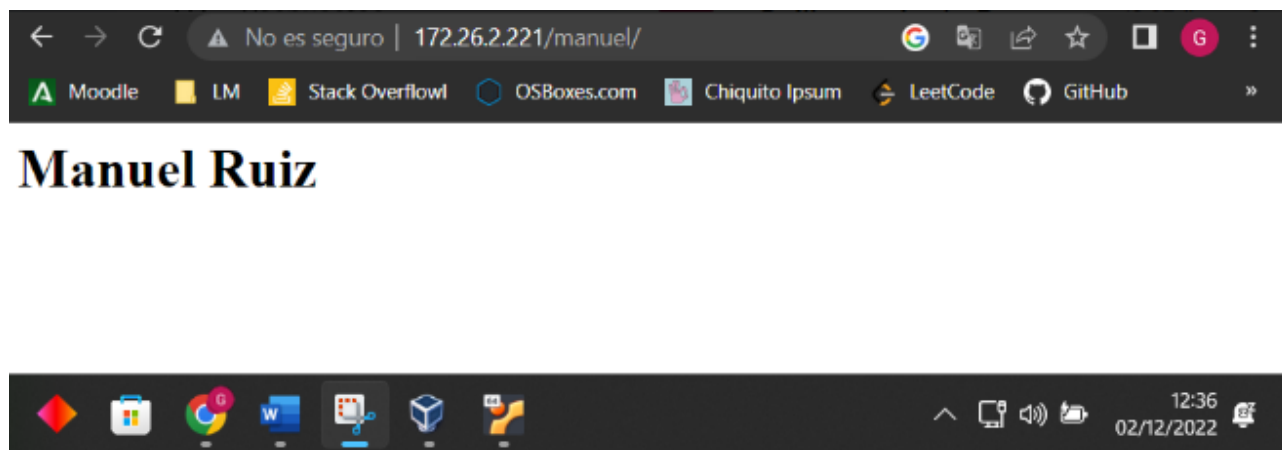
```
<Directory /var/www/html/manuel>
  DirectoryIndex manuel.html
  Options Indexes FollowSymLinks
  AllowOverride None
  Require host guille
  Require ip 172.26.58.171 172.26.2.221
</Directory>

Alias /apuntes /home/ruiz_jimenez/apuntes
<Directory /home/ruiz_jimenez/apuntes>
  Options Indexes FollowSymLinks
  AllowOverride None
  <Control>
```

Le añadimos el require host con el nombre para darle permiso de acceso

PASO 9) Reinicia el servidor para que los cambios tengan efecto.

PASO 10) Abre un navegador desde la máquina del compañero e intenta acceder al recurso /**tuNombre/** y comprueba que ahora sí se puede.





Unión Europea

Fondo Social Europeo
"El FSE invierte en tu futuro"

Desde la máquina del compañero:





C) Autenticación y autorización Basic y Digest

La autenticación es el proceso mediante el cual se puede verificar que alguien es quien dice ser. La autorización es el proceso mediante el cual se permite a acceder a un recurso solicitado.

En este punto vamos a usar las autenticaciones Basic y Digest.

(<http://httpd.apache.org/docs/2.2/es/howto/auth.html>)

Autenticación Basic:

- La contraseña es enviada por el cliente en texto plano.
- Autenticación y autorización sobre fichero de texto (comando **htpasswd**).
- Usa los módulos **authn_file** y **authz_user**.

```
# La primera vez que se invoca el comando se
# utiliza a opción -c para crear el fichero
htpasswd -c /etc/apache2/passwd profesor1

# Añade un nuevo usuario al fichero
htpasswd /etc/apache2/passwd profesor2

# Borrar un nuevo usuario al fichero
htpasswd -D /etc/apache2/passwd profesor1
```

<http://httpd.apache.org/docs/2.2/es/programs/htpasswd.html>

- Definir directivas:
 - **AuthType**: tipo de autorización
 - **AuthName**: nombre de la autorización cuando el cliente reciba el mensaje
 - **AuthUserFile**: localización del fichero donde están los usuarios que pueden autenticarse
 - **Require** solo los usuarios o grupos de usuarios que aparecen en esta directiva pueden acceder al recurso.

```
<Directory /var/www/profesor>
    Options Indexes FollowSymLinks MultiViews
    AllowOverride None
    Order allow,deny
    allow from 127.0.0.1
    allow from 192.168.1.16
    AuthType Basic
    AuthName "Acceso restringido"
    AuthUserFile /etc/apache2/passwd
    Require user profesor1 profesor2
</Directory>
```

Autenticación digest:

- La contraseña se envía cifrada (cifrado débil) por el cliente.
- Autenticación y autorización sobre fichero de texto (comando **htdigest**)
- Módulos: **mod_auth_digest** y **mod_auth_user**



Unión Europea

Fondo Social Europeo

"El FSE invierte en tu futuro"



```
# La primera vez que se invoca el comando se
# utiliza a opción -c para crear el fichero
htdigest -c /etc/apache2/digest    informatica admin1

# Añade un nuevo usuario al fichero
Htdigest /etc/apache2/digest    informatica admin2

# Borrar un nuevo usuario al fichero
htdigest -D /etc/apache2/digest    informatica admin1
```

<http://httpd.apache.org/docs/2.2/es/programs/htdigest.html>

- Definir directivas:
 - AuthType: tipo de autorización
 - AuthName: nombre de la autorización cuando el cliente reciba el mensaje
 - AuthDigestProvider: establecen el método de almacenamiento de las contraseñas del servidor, en nuestro caso se almacenarán en un archivo y por tanto tendrán el valor file
 - AuthUserFile: localización del fichero donde están los usuarios que pueden autenticarse
 - Require solo los usuarios o grupos de usuarios que aparecen en esta directiva pueden acceder al recurso

```
<Directory /var/www/departamento>
  Options Indexes FollowSymLinks MultiViews
  AllowOverride None
  AuthType Digest
  AuthName "informatica"
  AuthDigestProvider file
  AuthUserFile /etc/apache2/digest
  Require user admin1 admin2
</Directory>
```

En este punto vamos a configurar la autenticación Basic y Digest para recursos de Apache en nuestro servidor Linux.

C.1) Autenticación Basic

PASO 1) Comprueba si el módulo **auth_basic** está habilitado, si no lo está, habilítalo.

Este habilitado

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

Ya la tenemos creada del apartado anterior



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 **htpasswd** (ver cuadro arriba). Añade los usuarios **apellido1** y **apellido2**.

```
htpasswd: password verification error
root@ServidorLinuxmrj:/home/ruiz_jimenez# htpasswd -c /etc/apache2/passwd ruiz
New password:
Re-type new password:
Adding password for user ruiz

root@ServidorLinuxmrj:/home/ruiz_jimenez# htpasswd /etc/apache2/passwd jimenez
New password:
Re-type new password:
Adding password for user jimenez
root@ServidorLinuxmrj:/home/ruiz_jimenez# _
```

PASO 4) Edita el fichero de configuración **/etc/apache2/sites-available/000-default.conf** y permite el acceso al directorio **/var/www/html/nombreAlumno** a los usuarios **apellido1** y **apellido2** (ver cuadro ejemplo arriba).

```
<Directory /var/www/html/manuel>
    DirectoryIndex manuel.html
    Options Indexes FollowSymLinks
    AllowOverride None
    Require host guille
    Require ip 172.26.58.171 172.26.2.221
    AuthType Basic
    AuthName "Acceso restringido"
    AuthUserFile /etc/apache2/passwd
    Require user ruiz jimenez
</Directory>

Alias /apuntes /home/ruiz_jimenez/apuntes
<Directory /home/ruiz_jimenez/apuntes>
    Options Indexes FollowSymLinks
    AllowOverride None

ServidorLinuxmrj:/home/ruiz_jimenez# ls /etc/apache2/mods-enabled/
```

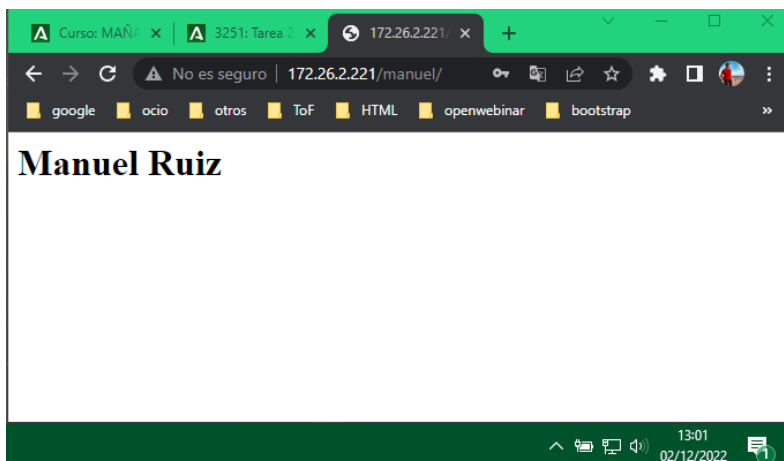
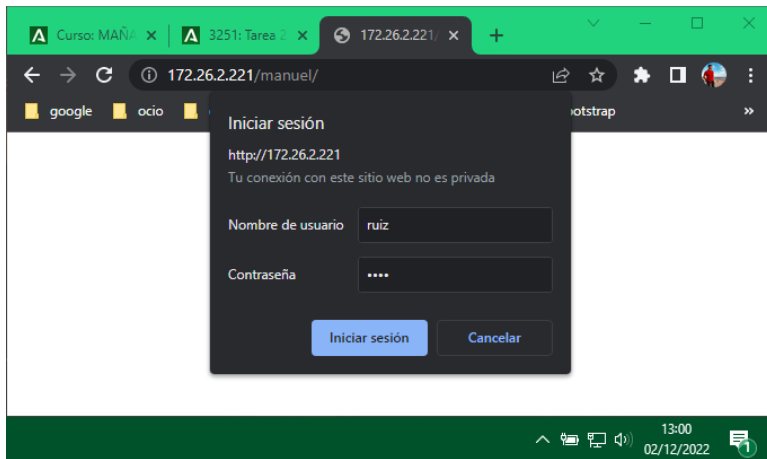


Unión Europea

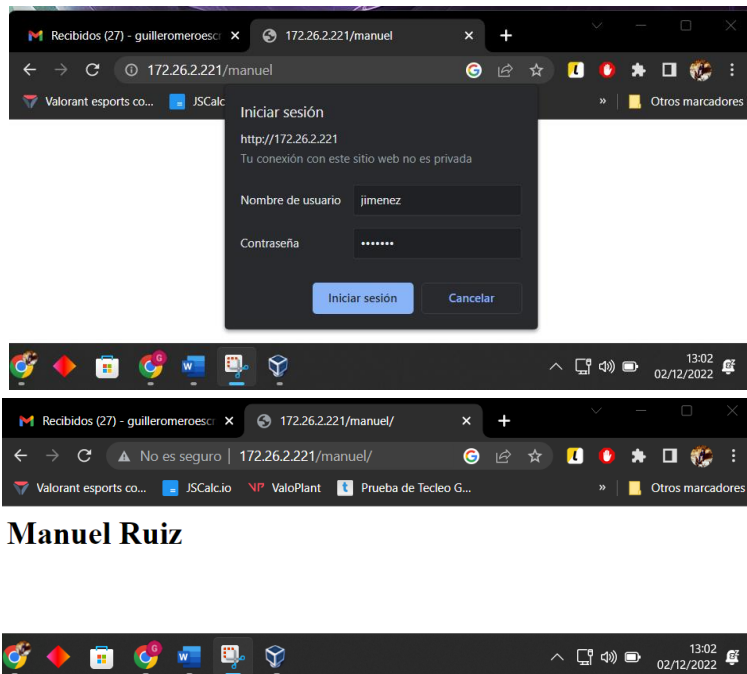
Fondo Social Europeo
"El FSE invierte en tu futuro"

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

PASO 6) Abre un navegador desde tu máquina física y accede al recurso `/nombreAlumno` como usuario `apellido01`.



PASO 7) Abre un navegador desde la máquina de un compañero y accede al recurso **/nombreAlumno** como usuario **apellido2**.



Toma capturas de los pasos 3,4, 6 y 7 (de estas últimas una captura cuando sale el cuadro para autenticarte y luego una vez dentro del recurso /amigo).

C.2) Autenticación Digest

PASO 1) Comprueba si el módulo **auth_digest** está habilitado, si no lo está, habilítalo.

Si estaba habilitado

PASO 2) Vamos a crear el directorio **/tareac2/** dentro de nuestro directorio raíz **/var/www/html/**. Dentro añadiremos un archivo **tareac2.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 **inicialPrimerApellidoNombre** y **inicialSegundoApellidoNombre**.



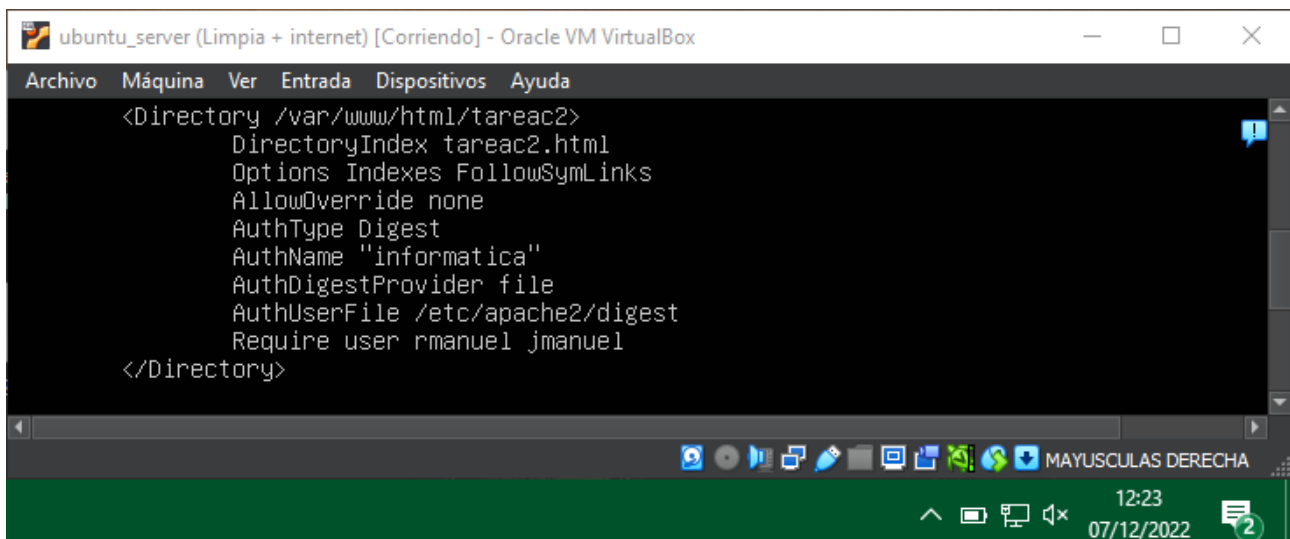
Ejemplo: Amapola Gutierrez de la Vega:

gamapola

vamapola

```
root@ServidorLinuxmrj:/var/www/html# htdigest -c /etc/apache2/digest informatica rmanuel
Adding password for rmanuel in realm informatica.
New password:
Re-type new password:
root@ServidorLinuxmrj:/var/www/html# htdigest /etc/apache2/digest informatica jmanuel
Adding user jmanuel in realm informatica
New password:
Re-type new password:
root@ServidorLinuxmrj:/var/www/html#
```

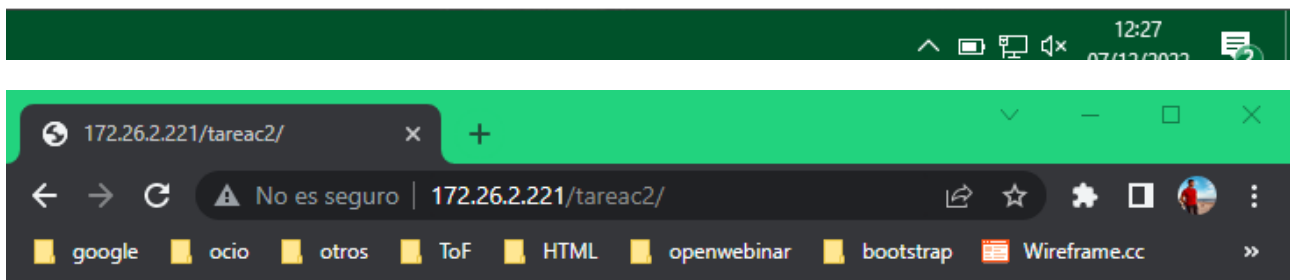
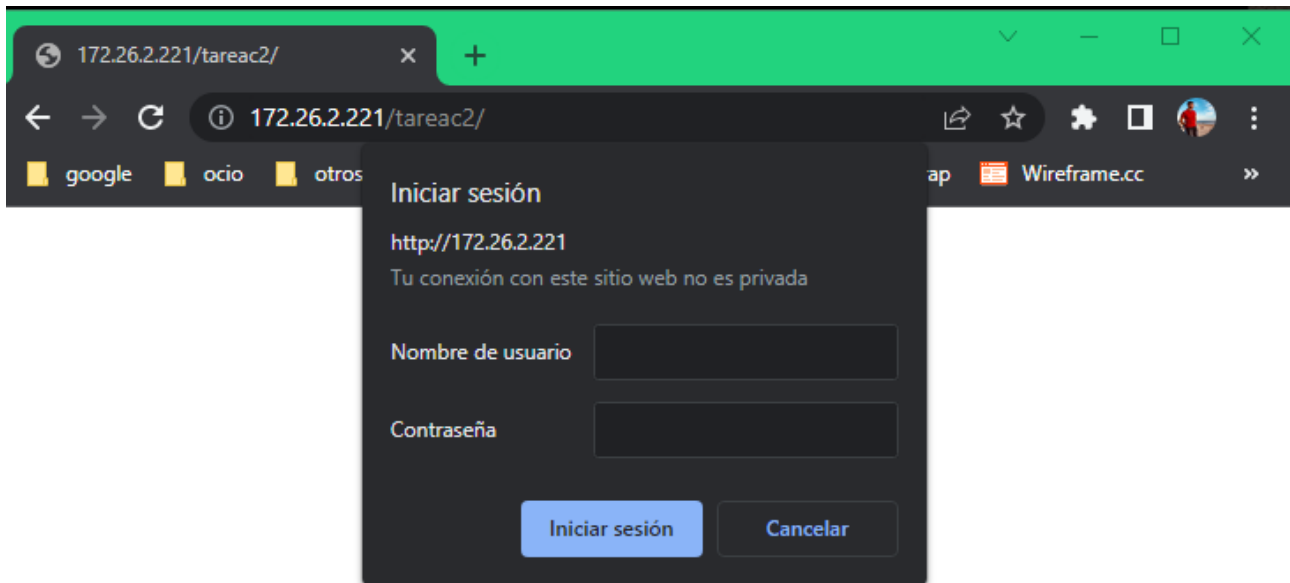
PASO 4) Edita el fichero de configuración `/etc/apache2/sites-available/000-default.conf` y permite el acceso al directorio `/var/www/html/tareac2` a los usuarios `inicialPrimerApellidoNombre` y `inicialSegundoApellidoNombre` (ver cuadro ejemplo arriba). Ten en cuenta que en la directiva `AuthName` tienes que poner lo mismo que pusiste en el dominio o "realm".



```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
<Directory /var/www/html/tareac2>
  DirectoryIndex tareac2.html
  Options Indexes FollowSymLinks
  AllowOverride none
  AuthType Digest
  AuthName "informatica"
  AuthDigestProvider file
  AuthUserFile /etc/apache2/digest
  Require user rmanuel jmanuel
</Directory>
```

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

PASO 6) Abre un navegador desde tu máquina física y accede al recurso **/tareac2** como usuario **inicialPrimerApellidoNombre**.



Tareac2 prueba

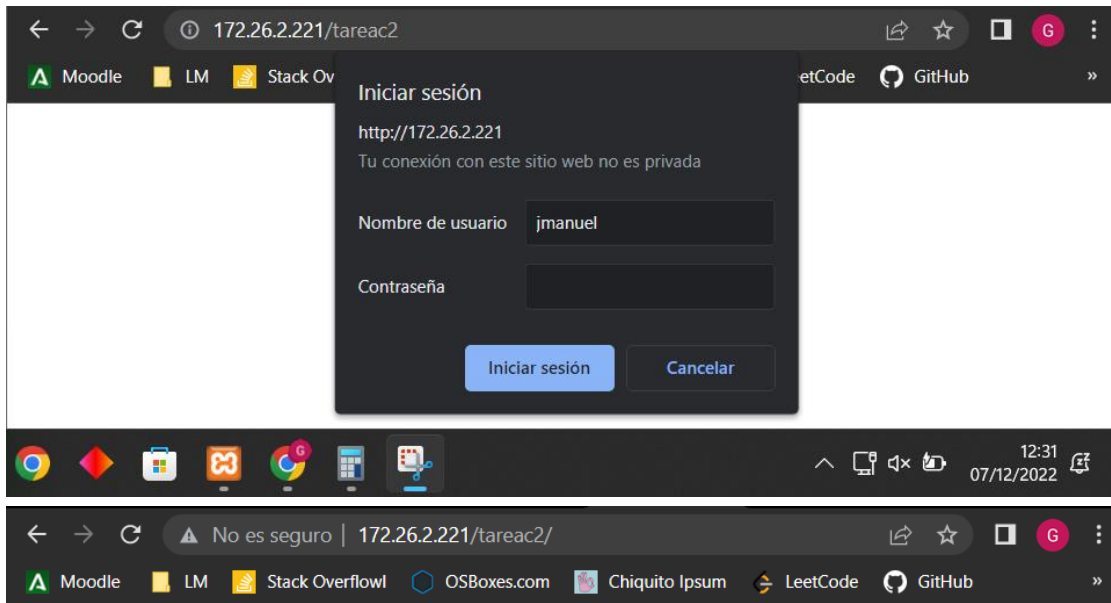




Unión Europea

Fondo Social Europeo
"El FSE invierte en tu futuro"

PASO 7) Abre un navegador desde la máquina de un compañero y accede al recurso **/tareac2** como usuario **inicialSegundoApellidoNombre**.



Tareac2 prueba



Toma una captura de los pasos 3, 4, 6 y 7 (de estas últimos una captura cuando sale el cuadro para autenticarte y luego una vez dentro del recurso /primo).

D) Ficheros .htaccess (si no sale poner pantallazo de haberlo intentado)


Los archivos .htaccess permiten configurar de manera personalizada directorios concretos que se quieran servir desde el Servidor Apache, pero sin que estos cambios afecten a la configuración general del servidor Apache. Básicamente permite "personalizar" el cómo se sirven unos contenidos que pertenecen a un directorio concreto.

Para poder hacer uso de los ficheros .htaccess tenemos que permitir en el archivo de configuración de apache (httpd.conf) su uso mediante la directiva "AllowOverride".

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**.

```
Alias /myBlog /home/useraccess/myBlog
<Directory /home/useraccess/myBlog>
    AllowOverride All
</Directory>
```



```
Alias /myBlog /home/useraccess/myBlog
<Directory /home/useraccess/myBlog>
    AllowOverride All
</Directory>

Redirect /periodico http://www.diariodesevilla.es

ErrorDocument 404 /404.html

Save modified buffer?
Y Yes
N No      ^C Cancel
```

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).

```
useraccess@ServidorLinuxmrj:~/myBlog$ htdigest -c .htdigest informatica myUserBlog
Adding password for myUserBlog in realm informatica.
New password:
Re-type new password:
useraccess@ServidorLinuxmrj:~/myBlog$ ls -ls .htdigest
```

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).

```
Options Indexes
Order allow,deny
allow from 192.168.1.101
AuthType Digest
AuthName "informatica"
AuthUserFile /home/useraccess/myBlog/.htdigest
Require user myUserBlog
```

```
ubuntu_server (Limpia + internet) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 6.2 .htaccess
Options Indexes
Order allow,deny
allow from 172.26.58.171
AuthType Digest
AuthName "informatica"
AuthUserFile /home/useraccess/myBlog/.htdigest
Require user myUserBlog
```




Unión Europea

Fondo Social Europeo
"El FSE invierte en tu futuro"

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.

The screenshot shows a web browser window with the address bar displaying `192.168.1.151/myBlog/`. The browser tabs include "Aplicaciones", "Rock Download: The E", and "15 Times Calvin And". The main content area displays the "Index of /myBlog" directory listing:

Name	Last modified	Size	Description
Parent Directory	-		
myBlog.html	2017-01-10 17:16	34	

Below the table, it says: *Apache/2.4.18 (Ubuntu) Server at 192.168.1.151 Port 80*.

An authentication dialog box titled "Se requiere autenticación" is overlaid on the right side of the browser window. It contains the following text:

http://192.168.1.151 necesita un nombre de usuario y una contraseña.
Tu conexión con este sitio no es privada.

There are two input fields: "Nombre de usuario:" and "Contraseña:". Below these fields are two buttons: "Iniciar sesión" and "Cancelar".

He intentado conectarme, pero da fallo y como se puede ver lo tengo tal y como lo pide la práctica.

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



E) Ficheros de registros (logs)

Los ficheros de registros nos ofrecen información de errores y accesos del servidor Apache.

En linux los ficheros de registro son:

Errores **`/var/log/apache2/error.log`**

Accesos **`/var/log/apache2/access.log`**

En windows:

Error **`C:\Program Files\Apache Software Foundation\Apache2.2\log\error.log`**

Accesos **`C:\Program Files\Apache Software Foundation\Apache2.2\log\access.log`**

Algunas de las directivas que tienen que ver con estos ficheros de registros son:

ErrorLog: Especifica los archivos donde se guardan los errores del servidor

LogLevel: Establece el nivel de detalle de los registros de mensajes de error

CustomLog: Identifica el archivo de registro de accesos y su formato (por defecto, combined)

LogFormat: Configura el formato para los archivos de registros del servidor Web (realmente depende de la configuración dada en CustomLog).

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

¿Qué directiva marca la ruta del archivo de los errores? ¿Cuál es el fichero de logs de errores?

¿Qué nivel de prioridad tiene?

La directiva ErrorLog, se guarda en el fichero error.log tiene la mayor prioridad

¿Qué directiva marca la ruta del archivo de los accesos? ¿Cuál es el fichero de logs de accesos?

La directiva CustomLog, el fichero Access.log



PASO 2) Consulta el log de errores

```
[Wed Dec 07 13:01:30.451717 2022] [mpm_event:notice] [pid 1887:tid 140549762054016] AH00492:
SIGWINCH, shutting down gracefully
[Wed Dec 07 13:01:30.496683 2022] [mpm_event:notice] [pid 2432:tid 140045494495104] AH00489:
2.4.52 (Ubuntu) configured -- resuming normal operations
[Wed Dec 07 13:01:30.496762 2022] [core:notice] [pid 2432:tid 140045494495104] AH00094: Comr
: '/usr/sbin/apache2'
[Wed Dec 07 13:01:35.302793 2022] [core:error] [pid 2434:tid 140045369460288] (13)Permission
[client 172.26.58.171:52626] AH00035: access to /myBlog denied (filesystem path '/home/user
yBlog') because search permissions are missing on a component of the path
[Wed Dec 07 13:01:35.631614 2022] [core:error] [pid 2434:tid 140045361067584] (13)Permission
[client 172.26.58.171:52626] AH00035: access to /myBlog denied (filesystem path '/home/user
yBlog') because search permissions are missing on a component of the path
[Wed Dec 07 13:01:35.817796 2022] [core:error] [pid 2434:tid 140045352674880] (13)Permission
[client 172.26.58.171:52626] AH00035: access to /myBlog denied (filesystem path '/home/user
yBlog') because search permissions are missing on a component of the path
[Wed Dec 07 13:01:36.009626 2022] [core:error] [pid 2434:tid 140045344282176] (13)Permission
[client 172.26.58.171:52626] AH00035: access to /myBlog denied (filesystem path '/home/user
yBlog') because search permissions are missing on a component of the path
[Wed Dec 07 13:01:36.204953 2022] [core:error] [pid 2434:tid 140045335889472] (13)Permission
[client 172.26.58.171:52626] AH00035: access to /myBlog denied (filesystem path '/home/user
yBlog') because search permissions are missing on a component of the path
[Wed Dec 07 13:01:36.500932 2022] [core:error] [pid 2434:tid 140045327496768] (13)Permission
[client 172.26.58.171:52626] AH00035: access to /myBlog denied (filesystem path '/home/user
yBlog') because search permissions are missing on a component of the path
[Wed Dec 07 13:01:49.540814 2022] [core:error] [pid 2433:tid 140045483689536] (13)Permission
[client 172.26.58.171:52627] AH00035: access to /myBlog denied (filesystem path '/home/user
yBlog') because search permissions are missing on a component of the path
[Wed Dec 07 13:03:30.415079 2022] [core:error] [pid 2433:tid 140045386245696] (13)Permission
[client 172.26.58.171:52647] AH00035: access to /myBlog denied (filesystem path '/home/user
yBlog') because search permissions are missing on a component of the path
[Wed Dec 07 13:07:44.818826 2022] [core:error] [pid 2433:tid 140045361067584] (13)Permission
[client 172.26.58.171:52676] AH00035: access to /myBlog denied (filesystem path '/home/user
yBlog') because search permissions are missing on a component of the path
[Wed Dec 07 13:08:16.673509 2022] [core:error] [pid 2433:tid 140045327496768] (13)Permission
[client 172.26.58.171:52700] AH00035: access to /myBlog denied (filesystem path '/home/user
yBlog') because search permissions are missing on a component of the path
ruiz_jimenez@ServidorLinuxmrj:~$ cat /var/log/apache2/error.log_
```



PASO 3) Consulta el log de accesos

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

172.26.58.171 - - [07/Dec/2022:12:48:05 +0000] "GET /myBlog HTTP/1.1" 403 493 "-" "Mozilla/5
ows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.
172.26.58.171 - - [07/Dec/2022:12:48:05 +0000] "GET /myBlog HTTP/1.1" 403 493 "-" "Mozilla/5
ows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.
172.26.58.171 - - [07/Dec/2022:12:48:56 +0000] "-" 408 0 "-" "-"
172.26.58.171 - - [07/Dec/2022:12:56:49 +0000] "GET /myBlog HTTP/1.1" 403 494 "-" "Mozilla/5
ows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.
172.26.58.171 - - [07/Dec/2022:12:56:57 +0000] "GET /myBlog HTTP/1.1" 403 494 "-" "Mozilla/5
ows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.
172.26.58.171 - - [07/Dec/2022:12:57:49 +0000] "-" 408 0 "-" "-"
172.26.58.171 - - [07/Dec/2022:13:01:35 +0000] "GET /myBlog HTTP/1.1" 403 494 "-" "Mozilla/5
ows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.
172.26.58.171 - - [07/Dec/2022:13:01:35 +0000] "GET /myBlog HTTP/1.1" 403 493 "-" "Mozilla/5
ows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.
172.26.58.171 - - [07/Dec/2022:13:01:35 +0000] "GET /myBlog HTTP/1.1" 403 493 "-" "Mozilla/5
ows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.
172.26.58.171 - - [07/Dec/2022:13:01:36 +0000] "GET /myBlog HTTP/1.1" 403 493 "-" "Mozilla/5
ows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.
172.26.58.171 - - [07/Dec/2022:13:01:36 +0000] "GET /myBlog HTTP/1.1" 403 493 "-" "Mozilla/5
ows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.
172.26.58.171 - - [07/Dec/2022:13:01:36 +0000] "GET /myBlog HTTP/1.1" 403 493 "-" "Mozilla/5
ows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.
172.26.58.171 - - [07/Dec/2022:13:01:49 +0000] "GET /myBlog HTTP/1.1" 403 494 "-" "Mozilla/5
ows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.
172.26.58.171 - - [07/Dec/2022:13:02:41 +0000] "-" 408 0 "-" "-"
172.26.58.171 - - [07/Dec/2022:13:03:30 +0000] "GET /myBlog HTTP/1.1" 403 494 "-" "Mozilla/5
ows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.
172.26.58.171 - - [07/Dec/2022:13:04:21 +0000] "-" 408 0 "-" "-"
172.26.58.171 - - [07/Dec/2022:13:07:44 +0000] "GET /myBlog HTTP/1.1" 403 494 "-" "Mozilla/5
ows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.
172.26.58.171 - - [07/Dec/2022:13:08:16 +0000] "GET /myBlog HTTP/1.1" 403 494 "-" "Mozilla/5
ows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.
172.26.58.171 - - [07/Dec/2022:13:08:16 +0000] "GET /favicon.ico HTTP/1.1" 404 319 "http://1
221/myBlog" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko
/108.0.0.0 Safari/537.36"
172.26.58.171 - - [07/Dec/2022:13:09:08 +0000] "-" 408 0 "-" "-"
ruiz_jimenez@ServidorLinuxmrj:~$ cat /var/log/apache2/access.log
```

F) Módulos status e info

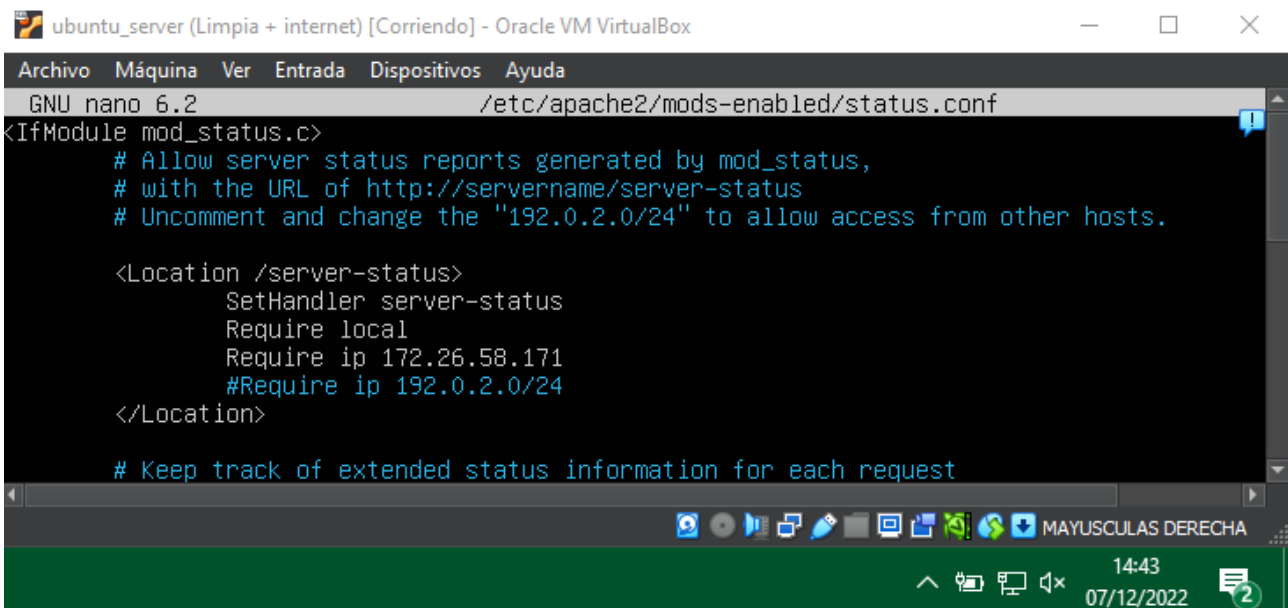
status e info son módulos de monitorización. En concreto:

status permite monitorizar el rendimiento del servidor Apache (generando un HTML).
info proporciona una vista resumida de la configuración del servidor.

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

```
ruiz_jimenez@ServidorLinuxmrj:~$ a2enmod status
Module status already enabled
ruiz_jimenez@ServidorLinuxmrj:~$ a2enmod info
Could not create /etc/apache2/mods-enabled/info.conf: Permission denied
ruiz_jimenez@ServidorLinuxmrj:~$ sudo a2enmod info
[sudo] password for ruiz_jimenez:
Enabling module info.
To activate the new configuration, you need to run:
  systemctl restart apache2
ruiz_jimenez@ServidorLinuxmrj:~$
```

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



```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 6.2  /etc/apache2/mods-enabled/status.conf
<IfModule mod_status.c>
# Allow server status reports generated by mod_status,
# with the URL of http://servername/server-status
# Uncomment and change the "192.0.2.0/24" to allow access from other hosts.

<Location /server-status>
    SetHandler server-status
    Require local
    Require ip 172.26.58.171
    #Require ip 192.0.2.0/24
</Location>

# Keep track of extended status information for each request
```



PASO 3) Reinicia el servidor para aplicar los cambios.

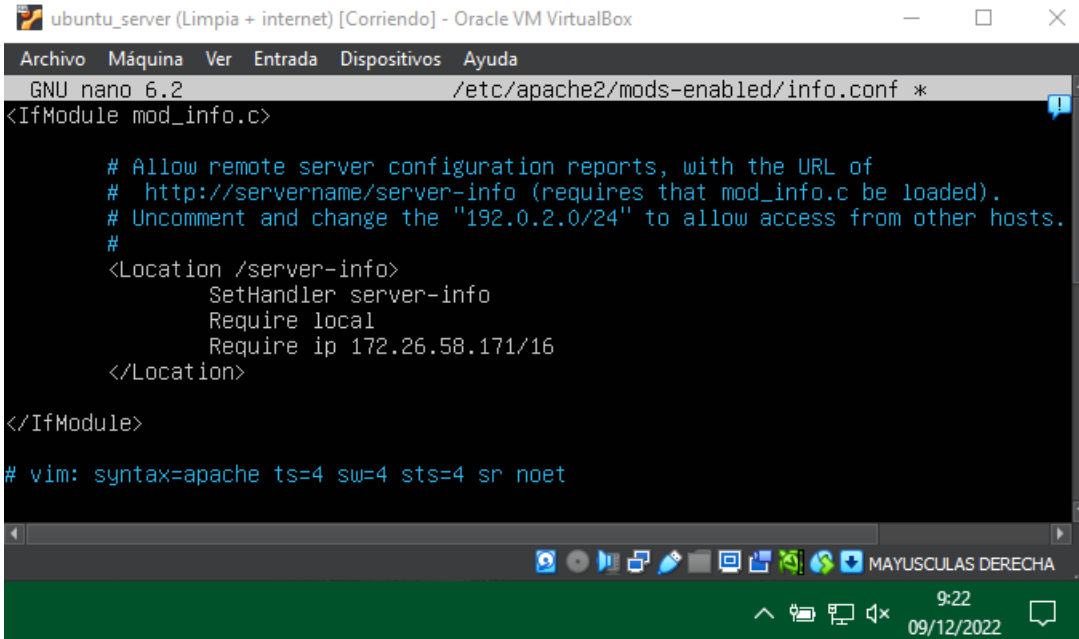
PASO 4) Desde tu máquina física conéctate al recurso server-status

```
ruiz_jimenez@ServidorLinuxmrj: ~  
3 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your  
Internet connection or proxy settings  
  
Last login: Wed Dec  7 13:39:52 2022  
ruiz_jimenez@ServidorLinuxmrj:~$ sudo service apache2 status  
[sudo] password for ruiz_jimenez:  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese  
   Active: active (running) since Wed 2022-12-07 13:43:30 UTC; 5min ago  
     Docs: https://httpd.apache.org/docs/2.4/  
  Process: 3133 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SU  
 Main PID: 3137 (apache2)  
    Tasks: 55 (limit: 1030)  
   Memory: 5.0M  
      CPU: 48ms  
   CGroup: /system.slice/apache2.service  
           └─3137 /usr/sbin/apache2 -k start  
             └─3138 /usr/sbin/apache2 -k start  
               └─3139 /usr/sbin/apache2 -k start  
  
dic 07 13:43:30 ServidorLinuxmrj systemd[1]: apache2.service: Deactivated succe  
dic 07 13:43:30 ServidorLinuxmrj systemd[1]: Stopped The Apache HTTP Server.  
dic 07 13:43:30 ServidorLinuxmrj systemd[1]: Starting The Apache HTTP Server...  
dic 07 13:43:30 ServidorLinuxmrj apachectl[3136]: AH00558: apache2: Could not r  
dic 07 13:43:30 ServidorLinuxmrj systemd[1]: Started The Apache HTTP Server.
```

Toma una captura de los pasos 2 y 4.

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.



```
ubuntu_server (Limpia + internet) [Corriendo] - Oracle VM VirtualBox
GNU nano 6.2 /etc/apache2/mods-enabled/info.conf *
<IfModule mod_info.c>

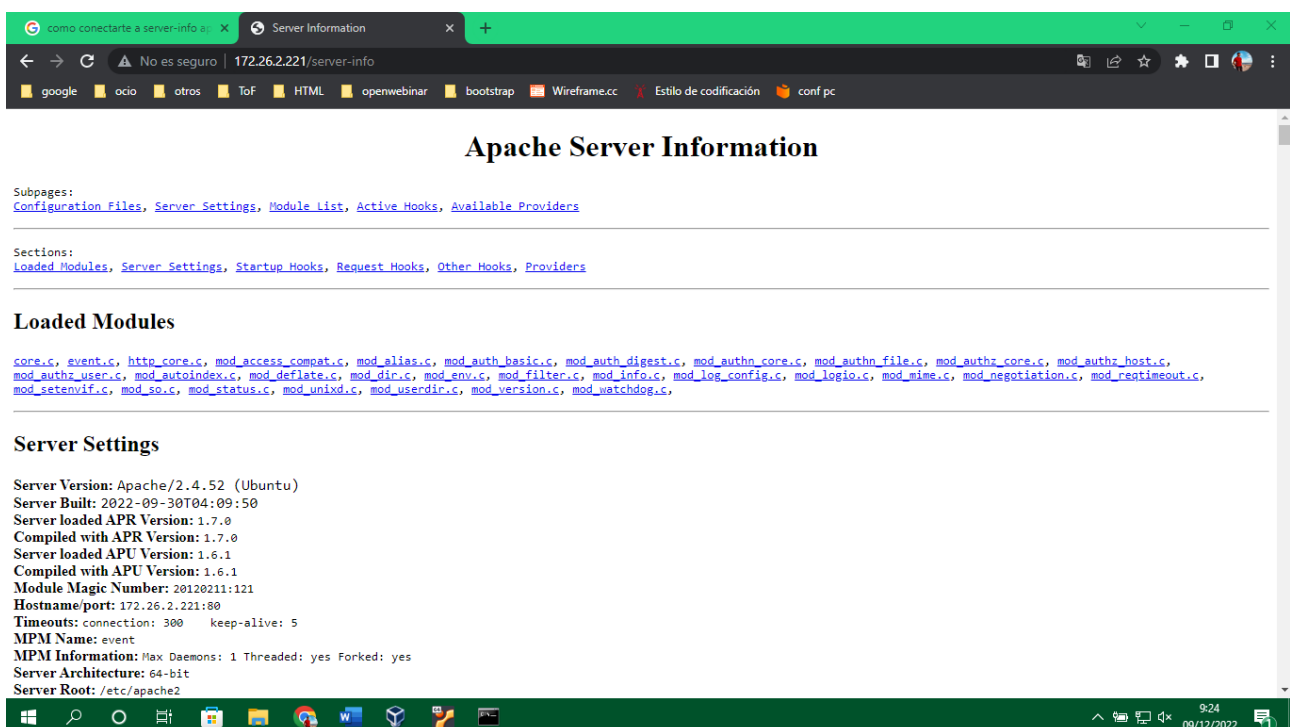
# Allow remote server configuration reports, with the URL of
# http://servername/server-info (requires that mod_info.c be loaded).
# Uncomment and change the "192.0.2.0/24" to allow access from other hosts.
#
<Location /server-info>
    SetHandler server-info
    Require local
    Require ip 172.26.58.171/16
</Location>

</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

PASO 7) Reinicia el servidor para aplicar los cambios.

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





Unión Europea

Fondo Social Europeo
"El FSE invierte en tu futuro"

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?

Si esta cargado el mod_mime y también tiene el UTF-32

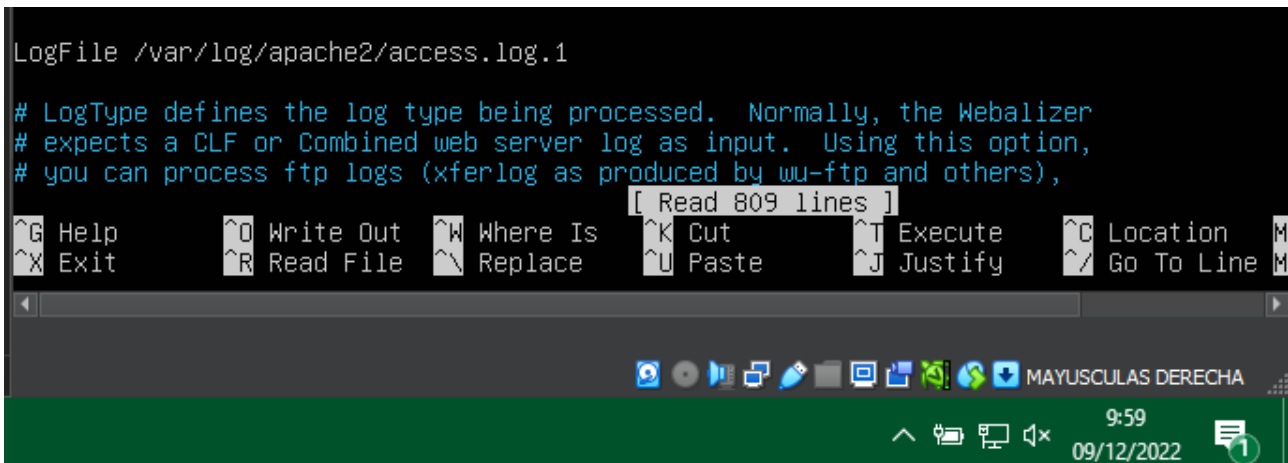
Toma una captura de los pasos 6 y 8.

G) Webalizer

Otra forma de monitorizar nuestro servidor apache es mediante aplicaciones analizadoras de logs, como es el caso de **Webalizer**. Esta aplicación se puede instalar en nuestro servidor y a partir de los archivos logs te crea unas estadísticas que puedes consultar en formato html.

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? ¿es correcta la ruta y el nombre del fichero? Si no es así, modifícala.



```
LogFile /var/log/apache2/access.log.1

# LogType defines the log type being processed.  Normally, the Webalizer
# expects a CLF or Combined web server log as input.  Using this option,
# you can process ftp logs (xferlog as produced by wu-ftp and others),
```

[Read 809 lines]

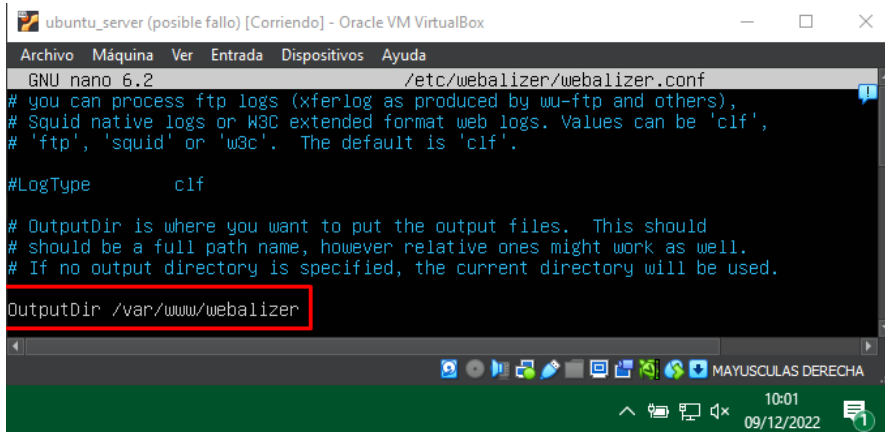
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location ^M
^X Exit ^R Read File ^_ Replace ^U Paste ^J Justify ^_ Go To Line ^M

MAYUSCULAS DERECHA

9:59 09/12/2022

Recoge el log de esta ruta, si es correcta

PASO 3) La instalación también implica la creación del recurso que se servirá desde el navegador, ¿Dónde está este fichero? ¿Es correcta la ubicación para servirlo? **Si no es así, muévelo a la ubicación correcta.**



```
ubuntu_server (posible fallo) [Corriendo] - Oracle VM VirtualBox
GNU nano 6.2 /etc/webalizer/webalizer.conf
# you can process ftp logs (xferlog as produced by wu-ftp and others),
# Squid native logs or W3C extended format web logs. Values can be 'clf',
# 'ftp', 'squid' or 'w3c'. The default is 'clf'.

#LogType      clf

# OutputDir is where you want to put the output files. This should
# should be a full path name, however relative ones might work as well.
# If no output directory is specified, the current directory will be used.

OutputDir /var/www/webalizer
```

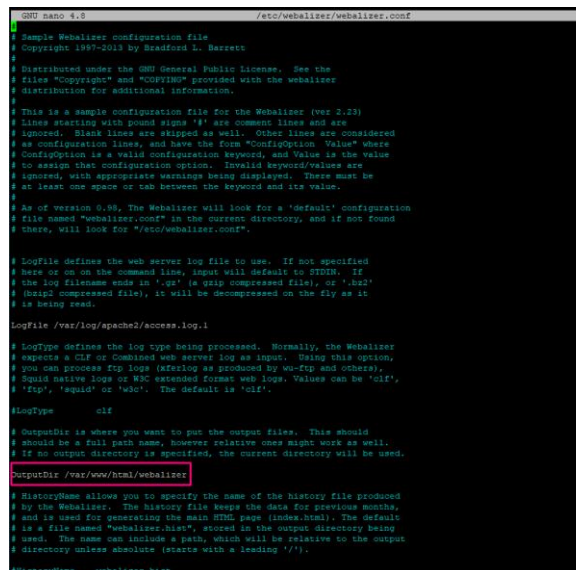
Tenemos que moverlo para que coincida con la ruta `/var/www/html/`

Podemos notar que una vez se descargó Webalizer **la ruta por defecto donde queda almacenado es `/var/www/webalizer`** y este parámetro **debemos moverlo a la ruta `/var/www/html`** para que la sincronización entre Apache y Webalizer sea correcta. Para realizar este proceso simplemente ejecutamos lo siguiente:

```
sudo mv /var/www/webalizer /var/www/html/
```

A continuación, vamos a **editar el archivo de configuración de Webalizer** introduce la siguiente instrucción:

```
sudo nano /etc/webalizer/webalizer.conf
```



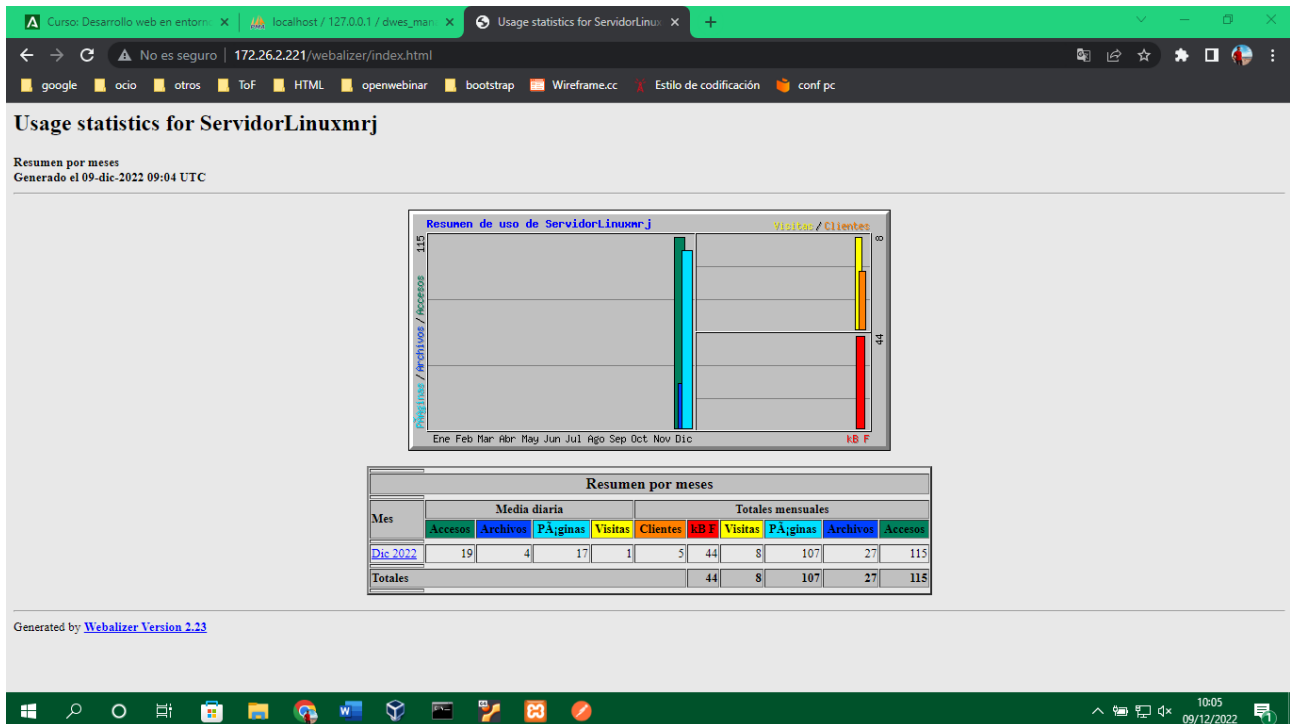
```
GNU nano 6.2 /etc/webalizer/webalizer.conf
# Sample Webalizer configuration file
# Copyright 1997-2013 by Bradford L. Barrett
# Distributed under the GNU General Public License. See the
# files "COPYRIGHT" and "README" provided with the webalizer
# distribution for additional information.
#
# This is a sample configuration file for the Webalizer (ver 2.23)
# Lines starting with pound signs '#' are comment lines and are
# ignored. Blank lines are skipped as well. Other lines are considered
# as configuration lines, and have the form "ConfigOption Value" where
# ConfigOption is a valid configuration keyword, and Value is the value
# to assign that configuration option. Invalid keyword/values are
# ignored, with appropriate warnings being displayed. There must be
# at least one space or tab between the keyword and its value.
#
# As of version 0.99, The Webalizer will look for a 'default' configuration
# file named "webalizer.conf" in the current directory, and if not found
# there, will look for "/etc/webalizer.conf".
#
# Logfile defines the web server log file to use. If not specified
# here or on the command line, input will default to STDERR. If
# the log filename ends in ".gz" (a gzip compressed file), or ".bz2"
# (bzip2 compressed file), it will be decompressed on the fly as it
# is being read.
#
# Logfile /var/log/apache2/access.log.1
#
# LogType defines the log type being processed. Normally, the Webalizer
# expects a CLF or Combined web server log as input. Using this option,
# you can process ftp logs (extracted as produced by wu-ftp and others),
# Squid native logs or W3C extended format web logs. Values can be 'clf',
# 'ftp', 'squid' or 'w3c'. The default is 'clf'.
#
#LogType      clf
#
# OutputDir is where you want to put the output files. This should
# should be a full path name, however relative ones might work as well.
# If no output directory is specified, the current directory will be used.
#
#OutputDir /var/www/html/webalizer
#
# HistoryName allows you to specify the name of the history file produced
# by the Webalizer. The history file keeps the data for previous months,
# and is used for generating the main HTML page (index.html). The default
# is a file named "webalizer.hist", stored in the output directory being
# used. The name can include a path, which will be relative to the output
# directory unless absolute (starts with a leading '/').
#
#HistoryName  webalizer.hist
```



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.



Toma una captura de los pasos 2 y 5.

F) GitHub

Sube el documento al repositorio llamado Despliegue a la carpeta correspondiente.

<https://github.com/ManuelRuJi/Despliegue-git>

Toma capturas de pantalla de los comandos utilizados y del repositorio de la página Web.