




UD 2. Servidor HTTP

Despliegue de Aplicaciones Web

Angela Borges Cantarino

| | |
|--|---|
| <i>Despliegue de Aplicaciones Web</i> |  |
| UD 2. Servidor HTTP | |
| Práctica 2.2: Administración de Apache II Módulos | |

Índice

| | |
|---|----|
| A) Módulos en Linux..... | 3 |
| A.1) Módulos | 3 |
| A.2) Módulo userdir..... | 5 |
| A.3) Módulo userdir en el servidor de clase..... | 7 |
| B) Control de acceso por IP y nombre de dominio..... | 10 |
| C) Autenticación y autorización Basic y Digest..... | 12 |
| C.1) Autenticación Basic | 13 |
| C.2) Autenticación Digest | 16 |
| D) Ficheros .htaccess (si no sale poner pantallazo de haberlo intentado)..... | 19 |
| E) Ficheros de registros (logs)..... | 22 |
| F) Módulos status e info | 24 |
| G) Webalizer | 30 |
| F) GitHub..... | 35 |

- Crea un fichero que se llame Practica2.2_Apellido1Apellido2_Nombre.pdf .
- Inserta todas las capturas de pantallas por orden explicando cada una de ellas.
- Una vez terminada la práctica, sube el archivo.

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.

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

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?

Extensión `.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?

`IfModule`

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

Contiene archivos con extensión `.so`

Toma capturas de los pasos 1, 2, 3 y 4.

PASO 1

```
angela@servidorLinuxabc:~$ sudo apache2ctl -l
[sudo] password for angela:
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
angela@servidorLinuxabc:~$ _
```

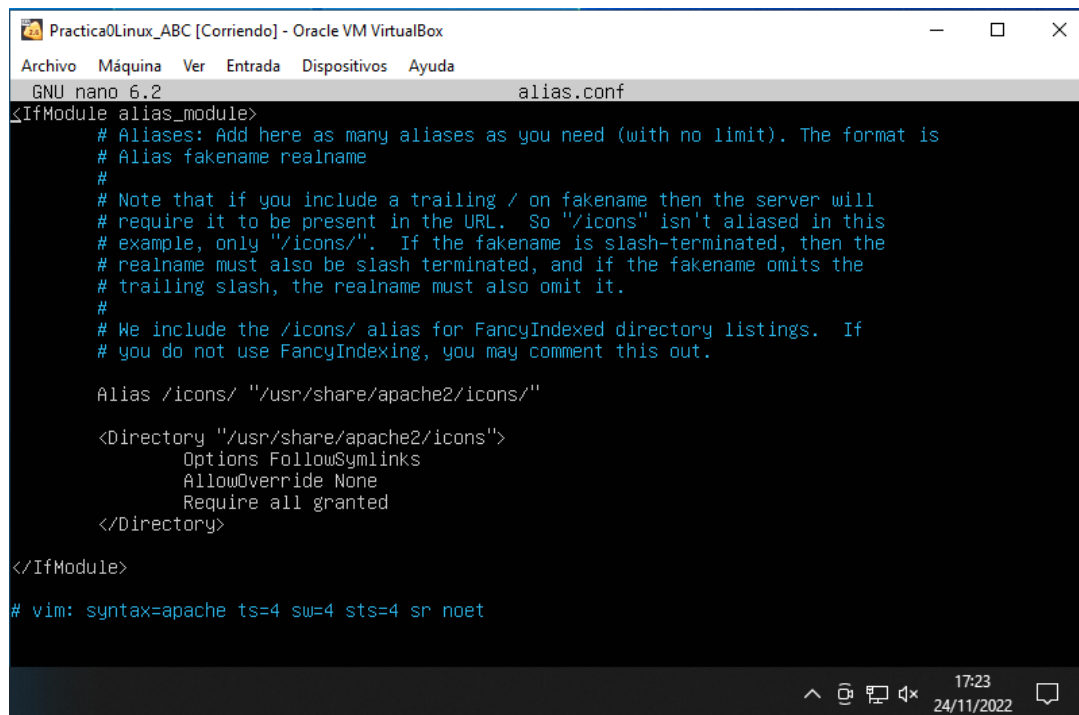
PASO 2

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

PASO 3

```
Practica0Linux_ABC [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 6.2                                mime.load
LoadModule mime_module /usr/lib/apache2/modules/mod_mime.so
```

PASO 4



```
Practica0Linux_ABC [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 6.2 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
```

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?

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

PASO 3) Verifica ahora si el módulo está habilitado.

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?

ROOT

¿Cuál es el subdirectorio que deben crear los usuarios en su carpeta home para poner sus páginas personales?

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

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)

PASO 3

```
angela@servidorLinuxabc:/etc/apache2/mods-enabled$ sudo systemctl restart apache2
angela@servidorLinuxabc:/etc/apache2/mods-enabled$ ls
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  dir.load     mpm_event.load  setenvif.load
auth_basic.load     autoindex.conf  env.load     negotiation.conf status.conf
authn_core.load     autoindex.load  filter.load  negotiation.load status.load
authn_file.load     deflate.conf     mime.conf    reqtimeout.conf userdir.conf
angela@servidorLinuxabc:/etc/apache2/mods-enabled$ _
```

PASO 5

```
Practica0Linux_ABC [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 6.2 /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
```

PASO 7**A.3) Módulo userdir en el servidor de clase**

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

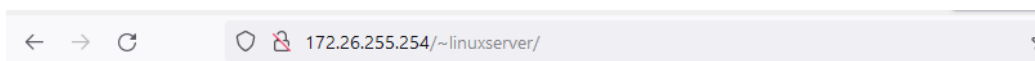
Recordad que es la inicial del primer nombre y el primer apellido.

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

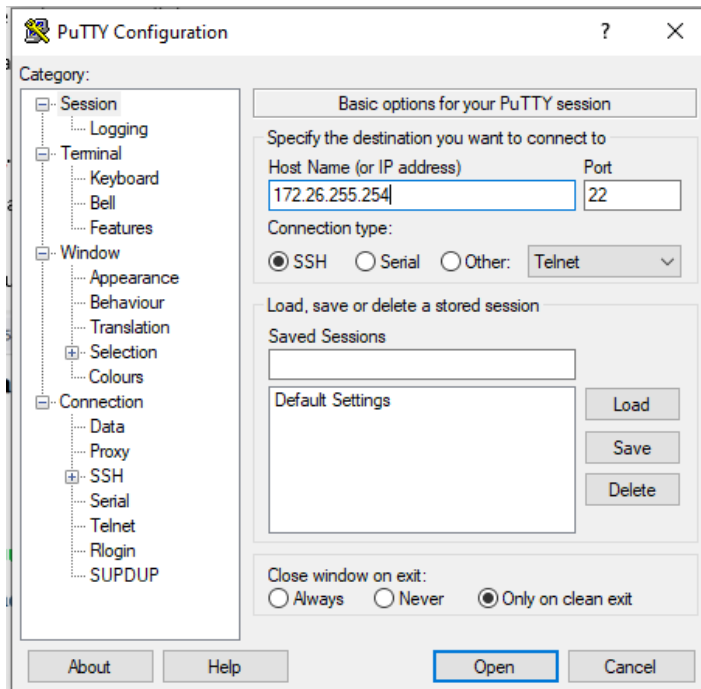
PASO 2) Da los pasos necesarios para qué al acceder a `http://172.26.255.254/~agutierrez` se vea tu página web en el servidor.

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

**Página WEB del usuario LINUXSERVER**

Detalla los pasos seguidos para conseguirlo.

Primero debemos instalar Putty en Windows, accedemos a través de la IP: 172.26.255.254, si lo intentamos a través de nuestro usuario no nos funciona porque no tenemos permisos.



```
172.26.255.254 - PuTTY
login as: aborges
aborges@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 lun 28 nov 2022 16:25:10 UTC

System load:  0.08           Temperature:   34.0 C
Usage of /:   17.3% of 54.22GB Processes:      157
Memory usage: 15%           Users logged in: 2
Swap usage:   0%            IPv4 address for enp2s0: 172.26.255.254

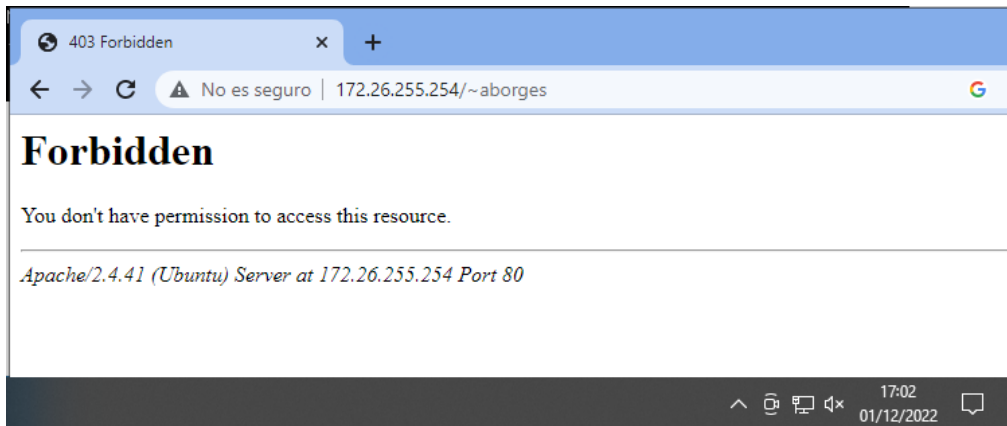
0 updates can be applied immediately.

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Fri Nov 19 17:08:18 2021 from 172.26.0.70
$
```

Debemos un directorio nuevo `public_html`

```
Last login: Mon Nov 28 16:25:11 2022 from 172.26.153.198
$ mkadir public_html
-sh: 1: mkadir: not found
$ mkdir public_html
$ cd public_html
$ nano index.html
$
```

A screenshot of a terminal window showing the execution of commands to create a directory and edit a file. The commands are: `mkadir public_html` (which fails with "not found"), `mkdir public_html` (which succeeds), `cd public_html`, and `nano index.html`. The prompt is a green cursor on a black background. The terminal's status bar at the bottom shows the time as 17:13 on 01/12/2022.

Y añadir la información.



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

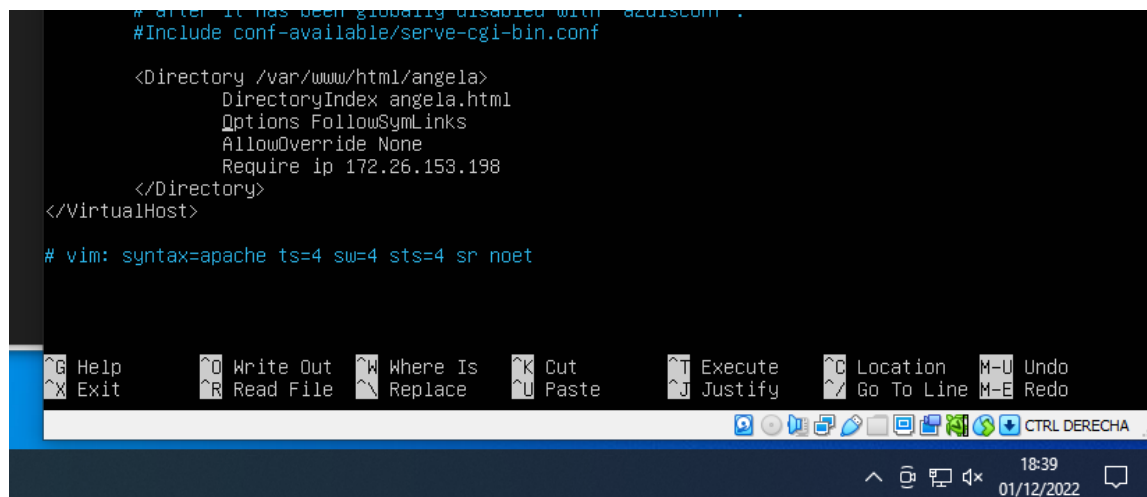
Vamos a controlar el acceso a un recurso de Apache en nuestro servidor Linux para que la máquina física tenga acceso, y la máquina de un compañero no:

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

Si.

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.



```
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf

<Directory /var/www/html/angela>
    DirectoryIndex angela.html
    Options FollowSymLinks
    AllowOverride None
    Require ip 172.26.153.198
</Directory>
</VirtualHost>

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

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).

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



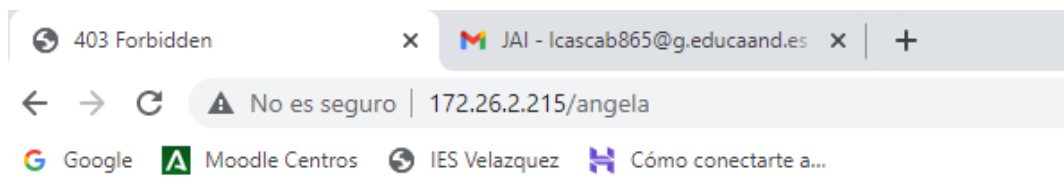
```
angela@servidorLinuxabc:~$ sudo service apache2 restart
angela@servidorLinuxabc:~$ _
```

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



Captura de mi ordenador

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



Forbidden

You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at 172.26.2.215 Port 80

Captura desde el ordenador de Lucia

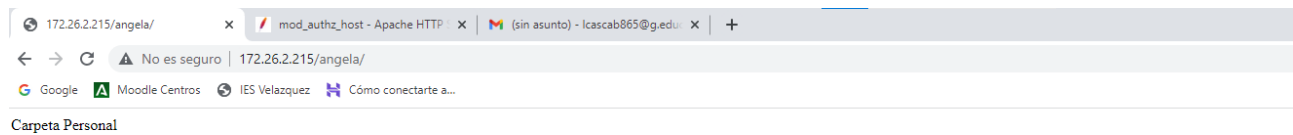
Toma una captura de los pasos 3,4,5 y 6.

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**.

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.



3ª vez que creo este archivo html para el usuario ANGELA BORGES CANTARINO

Toma una captura de los pasos 7 y 9.

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`

```
# 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>

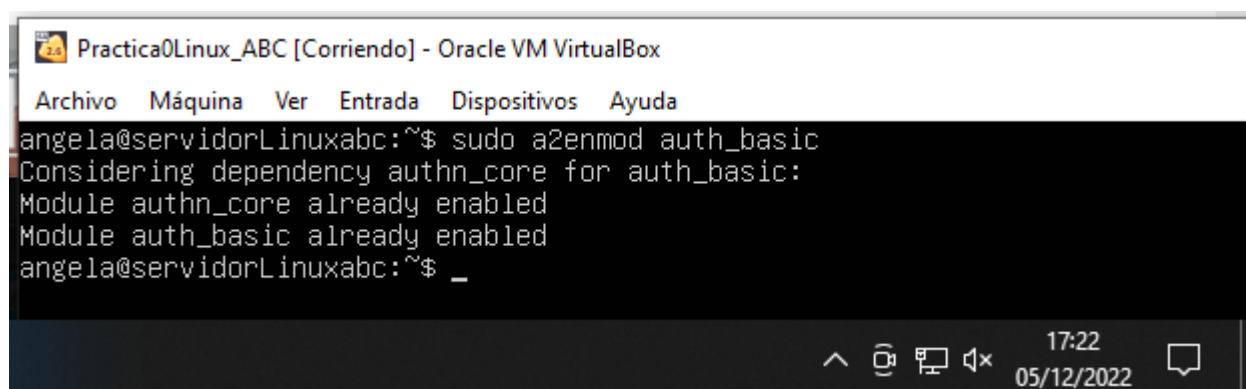
- Definir directivas:
 - `AuthType`: tipo de autorización
 - `AuthName`: nombre de la autorización cuando el cliente reciba el mensaje
 - `AuthDigestProvider`: establecen el método de almacenamiento de las contraseñas del servidor, en nuestro caso se almacenarán en un archivo y por tanto tendrán el valor `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.



```
Practica0Linux_ABC [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
angela@servidorLinuxabc:~$ sudo a2enmod auth_basic
Considering dependency authn_core for auth_basic:
Module authn_core already enabled
Module auth_basic already enabled
angela@servidorLinuxabc:~$ _
```

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.

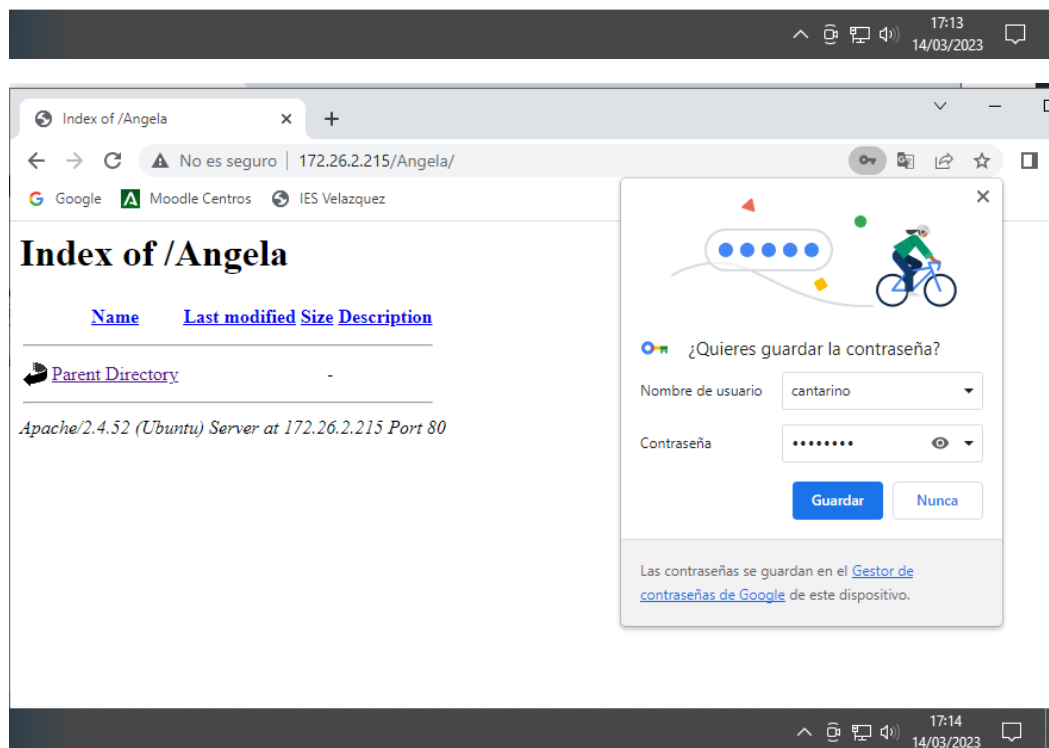
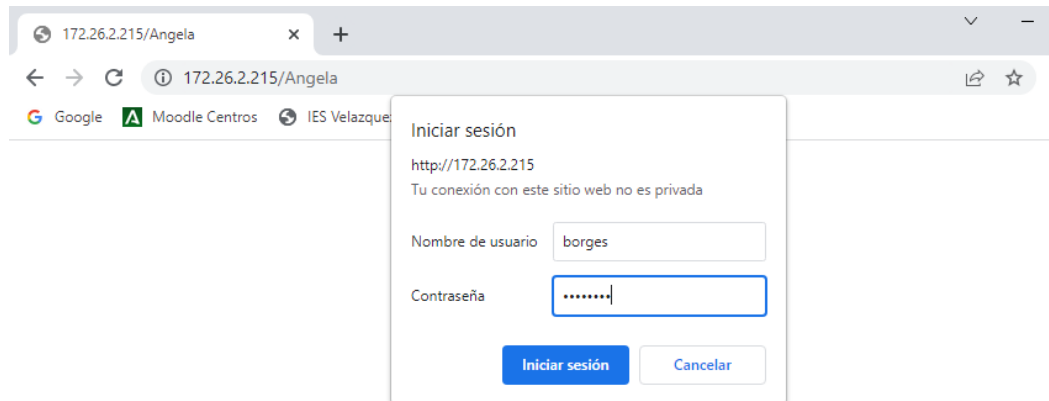
PASO 3) Para usar la autenticación Basic hay que crear un fichero accesible (el fichero que se creará será **/etc/apache2/passwd**) en el que se guardarán los usuarios y contraseñas. Para crear ese fichero se utilizará el comando **htpasswd** (ver cuadro arriba). Añade los usuarios **apellido1** y **apellido2**.

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).

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

```
angela@servidorLinuxabc:/$ sudo service apache2 restart
angela@servidorLinuxabc:/$ _
```

PASO 6) Abre un navegador desde tu máquina física y accede al recurso `/nombreAlumno` como usuario `apellido1`.



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

Este paso no puedo hacerlo pues no tengo a los compañeros en clase.

Toma capturas 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 /amigo).

C.2) Autenticación Digest

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

```
angela@servidorLinuxabc:/$ cd /etc/apache2/mods-enabled/
angela@servidorLinuxabc:/etc/apache2/mods-enabled$ ls
access_compat.load  authz_host.load  dir.load          negotiation.conf  ssl.conf
alias.conf          authz_user.load  env.load          negotiation.load  ssl.load
alias.load          autoindex.conf  filter.load       reqtimeout.conf   status.conf
auth_basic.load     autoindex.load  mime.conf         reqtimeout.load   status.load
authn_core.load     deflate.conf    mime.load         setenvif.conf     userdir.conf
authn_file.load     deflate.load    mpm_event.conf   setenvif.load     userdir.load
authz_core.load     dir.conf        mpm_event.load   socache_shmcb.load

angela@servidorLinuxabc:/etc/apache2/mods-enabled$ sudo a2enmod auth_digest
Considering dependency authn_core for auth_digest:
Module authn_core already enabled
Enabling module auth_digest.
To activate the new configuration, you need to run:
  systemctl restart apache2
angela@servidorLinuxabc:/etc/apache2/mods-enabled$ sudo systemctl restart apache2
angela@servidorLinuxabc:/etc/apache2/mods-enabled$ ls
access_compat.load  authz_core.load  dir.conf          mpm_event.load    socache_shmcb.load
alias.conf          authz_host.load  dir.load          negotiation.conf   ssl.conf
alias.load          authz_user.load  env.load          negotiation.load   ssl.load
auth_basic.load     autoindex.conf  filter.load       reqtimeout.conf    status.conf
auth_digest.load    autoindex.load  mime.conf         reqtimeout.load    status.load
authn_core.load     deflate.conf    mime.load         setenvif.conf      userdir.conf
authn_file.load     deflate.load    mpm_event.conf   setenvif.load      userdir.load
angela@servidorLinuxabc:/etc/apache2/mods-enabled$
```

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.

```
angela@servidorLinuxabc:/var/www/html$ sudo mkdir tareac2
angela@servidorLinuxabc:/var/www/html$ ls
404.html  angela  Angela  ciclos  despliegue.html  fp.html  indice.html  tareac2
angela@servidorLinuxabc:/var/www/html$
```

```
Practica0Linux_ABC [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 6.2                                tareac2.html *
Fichero tareac2 de Angela_
```

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

```
angela@servidorLinuxabc:/$ sudo htdigest -c /etc/apache2/passwd informatica bangela
Adding password for bangela in realm informatica.
New password:
Re-type new password:
angela@servidorLinuxabc:/$ sudo htdigest -c /etc/apache2/passwd informatica cangela
Adding password for cangela in realm informatica.
New password:
Re-type new password:
angela@servidorLinuxabc:/$ _
```

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”.

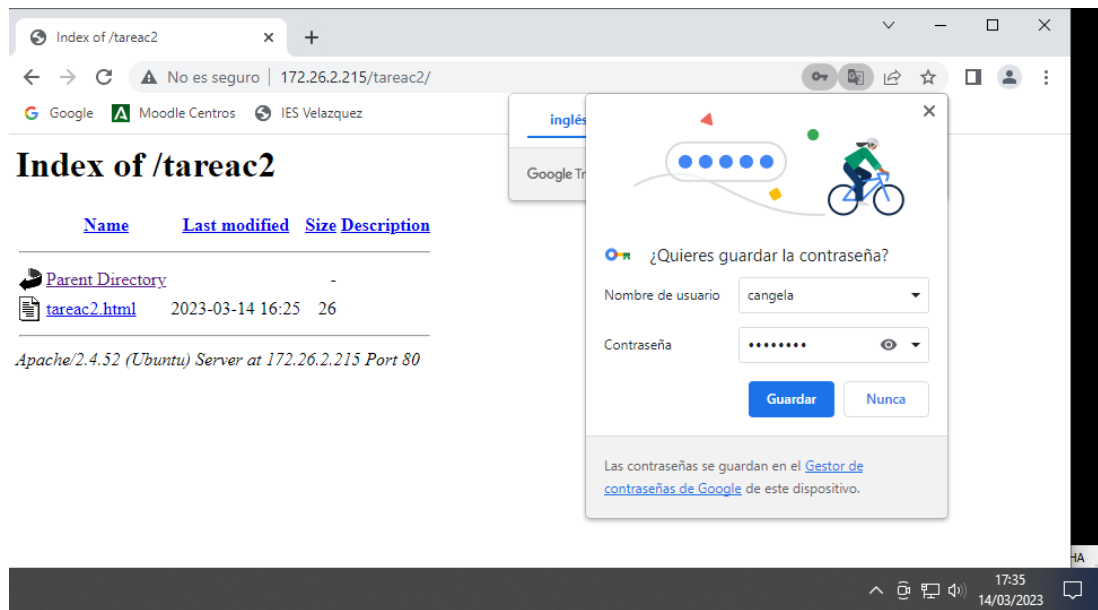
```
</Directory>

<Directory /var/www/html/tareac2>
    Options Indexes FollowSymLinks
    AllowOverride None
    AuthType Digest
    AuthName "informatica"
    AuthUserFile /etc/apache2/passwd
    Require user bangela cangela
</Directory>
```

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

```
angela@servidorLinuxabc:/$ sudo service apache2 restart
angela@servidorLinuxabc:/$
```

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



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

Este paso no puedo hacerlo pues no tengo a los compañeros en clase.

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`.

```
angela@servidorLinuxabc:/$ sudo useradd useraccess
angela@servidorLinuxabc:/$
```

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
```

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

```
angela@servidorLinuxabc:/$ sudo service apache2 restart
angela@servidorLinuxabc:/$ _
```

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

```
servidorLinuxabc login: useraccess
Password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-58-generic x86_64)

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

System information as of mar 14 mar 2023 16:49:31 UTC

System load: 0.34375      Processes:            111
Usage of /:  74.7% of 6.06GB Users logged in:      0
Memory usage: 11%        IPv4 address for enp0s3: 172.26.2.215
Swap usage:  0%

91 updates can be applied immediately.
21 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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

$
```

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

```
Practica0Linux_ABC [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

$ ls
myBlog  myBlog.html
$
```

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).

```

Practica0Linux_ABC [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
$ htdigest -c /home/useraccess/myBlog/.htdigest informatica myUserBlog
Adding password for myUserBlog in realm informatica.
New password:
Re-type new password:
$ _
  
```

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
  
```

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 browser window shows the URL `192.168.1.151/myBlog/`. The page content is:

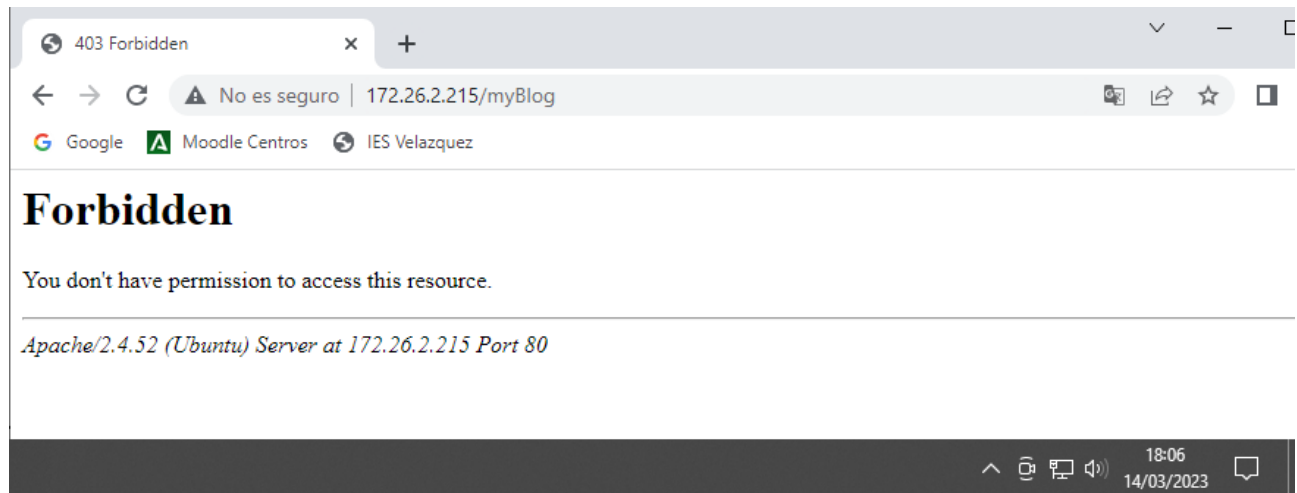
```

Index of /myBlog

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

Below the page content, it says: `Apache/2.4.18 (Ubuntu) Server at 192.168.1.151 Port 80`.

An authentication dialog box is displayed over the page. It contains the text: "Se requiere autenticación", "http://192.168.1.151 necesita un nombre de usuario y una contraseña.", and "Tu conexión con este sitio no es privada." There are input fields for "Nombre de usuario:" and "Contraseña:", and buttons for "Iniciar sesión" and "Cancelar".



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?

Ruta de errores

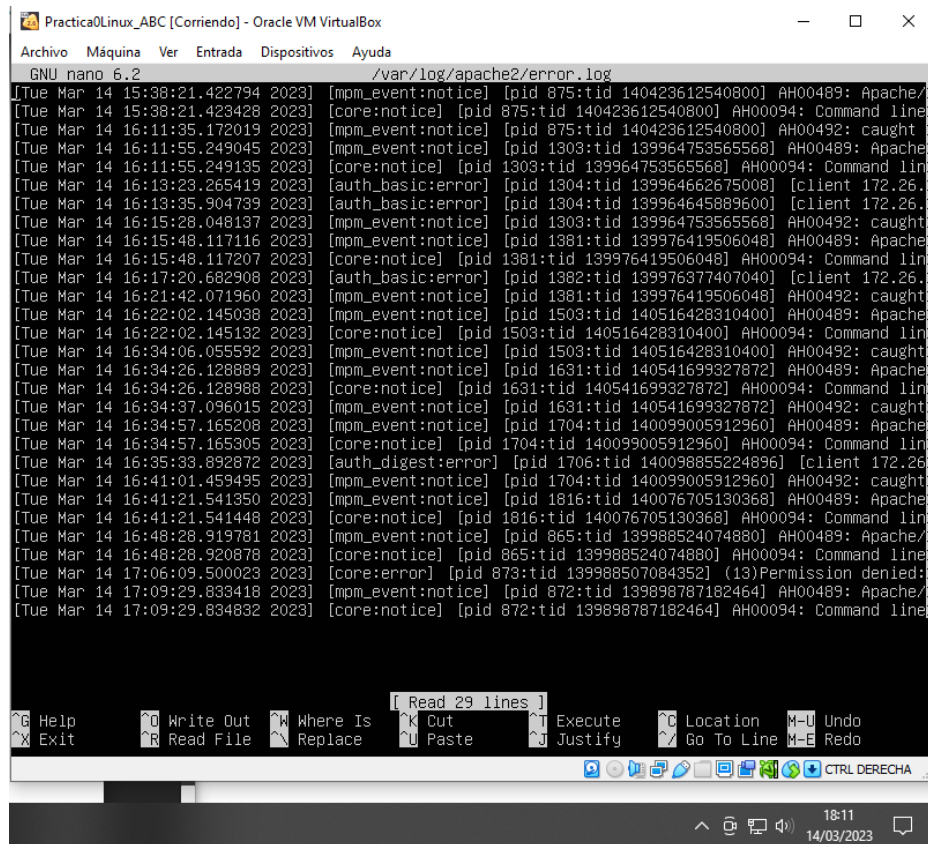
/var/log/apache2/error.log

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

Ruta de accesos

Accesos /var/log/apache2/access.log

PASO 2) Consulta el log de errores



```
GNU nano 6.2 /var/log/apache2/error.log
[Tue Mar 14 15:38:21.422794 2023] [mpm_event:notice] [pid 875:tid 140423612540800] AH00489: Apache/
[Tue Mar 14 15:38:21.423428 2023] [core:notice] [pid 875:tid 140423612540800] AH00094: Command line
[Tue Mar 14 16:11:35.172019 2023] [mpm_event:notice] [pid 875:tid 140423612540800] AH00492: caught
[Tue Mar 14 16:11:55.249045 2023] [mpm_event:notice] [pid 1303:tid 139964753565568] AH00489: Apache
[Tue Mar 14 16:11:55.249135 2023] [core:notice] [pid 1303:tid 139964753565568] AH00094: Command lin
[Tue Mar 14 16:13:23.265419 2023] [auth_basic:error] [pid 1304:tid 139964662675008] [client 172.26.
[Tue Mar 14 16:13:35.904739 2023] [auth_basic:error] [pid 1304:tid 139964645889600] [client 172.26.
[Tue Mar 14 16:15:28.048137 2023] [mpm_event:notice] [pid 1303:tid 139964753565568] AH00492: caught
[Tue Mar 14 16:15:48.117116 2023] [mpm_event:notice] [pid 1381:tid 139976419506048] AH00489: Apache
[Tue Mar 14 16:15:48.117207 2023] [core:notice] [pid 1381:tid 139976419506048] AH00094: Command lin
[Tue Mar 14 16:17:20.682908 2023] [auth_basic:error] [pid 1382:tid 139976377407040] [client 172.26.
[Tue Mar 14 16:21:42.071960 2023] [mpm_event:notice] [pid 1381:tid 139976419506048] AH00492: caught
[Tue Mar 14 16:22:02.145038 2023] [mpm_event:notice] [pid 1503:tid 140516428310400] AH00489: Apache
[Tue Mar 14 16:22:02.145132 2023] [core:notice] [pid 1503:tid 140516428310400] AH00094: Command lin
[Tue Mar 14 16:34:06.055592 2023] [mpm_event:notice] [pid 1503:tid 140516428310400] AH00492: caught
[Tue Mar 14 16:34:26.128889 2023] [mpm_event:notice] [pid 1631:tid 140541699327872] AH00489: Apache
[Tue Mar 14 16:34:26.128988 2023] [core:notice] [pid 1631:tid 140541699327872] AH00094: Command lin
[Tue Mar 14 16:34:37.096015 2023] [mpm_event:notice] [pid 1631:tid 140541699327872] AH00492: caught
[Tue Mar 14 16:34:57.165208 2023] [mpm_event:notice] [pid 1704:tid 140099005912960] AH00489: Apache
[Tue Mar 14 16:34:57.165305 2023] [core:notice] [pid 1704:tid 140099005912960] AH00094: Command lin
[Tue Mar 14 16:35:33.892872 2023] [auth_digest:error] [pid 1706:tid 140098855224896] [client 172.26.
[Tue Mar 14 16:41:01.459495 2023] [mpm_event:notice] [pid 1704:tid 140099005912960] AH00492: caught
[Tue Mar 14 16:41:21.541350 2023] [mpm_event:notice] [pid 1816:tid 140076705130368] AH00489: Apache
[Tue Mar 14 16:41:21.541448 2023] [core:notice] [pid 1816:tid 140076705130368] AH00094: Command lin
[Tue Mar 14 16:48:28.919781 2023] [mpm_event:notice] [pid 865:tid 139988524074880] AH00489: Apache/
[Tue Mar 14 16:48:28.920878 2023] [core:notice] [pid 865:tid 139988524074880] AH00094: Command line
[Tue Mar 14 17:06:09.500023 2023] [core:error] [pid 873:tid 139988507084352] (13)Permission denied:
[Tue Mar 14 17:09:29.833418 2023] [mpm_event:notice] [pid 872:tid 139898787182464] AH00489: Apache/
[Tue Mar 14 17:09:29.834832 2023] [core:notice] [pid 872:tid 139898787182464] AH00094: Command line
```

PASO 3) Consulta el log de accesos

The screenshot shows a terminal window titled 'Practica0Linux_ABC [Corriendo] - Oracle VM VirtualBox'. Inside, the nano text editor is open to the file `/var/log/apache2/access.log`. The log contains numerous entries of HTTP requests, including GET requests for `/Angela`, `/icons/blank.gif`, `/icons/back.gif`, `/favicon.ico`, and `/tareac2/`. The entries include IP addresses, timestamps, status codes, and user agents like 'Mozilla/5.0'. At the bottom of the terminal, there is a status bar with various icons and the system clock showing 18:12 on 14/03/2023.

Toma una captura de los pasos 2 y 3 (del final de cada fichero).

F) Módulos status e info

`status` e `info` son módulos de monitorización. En concreto:

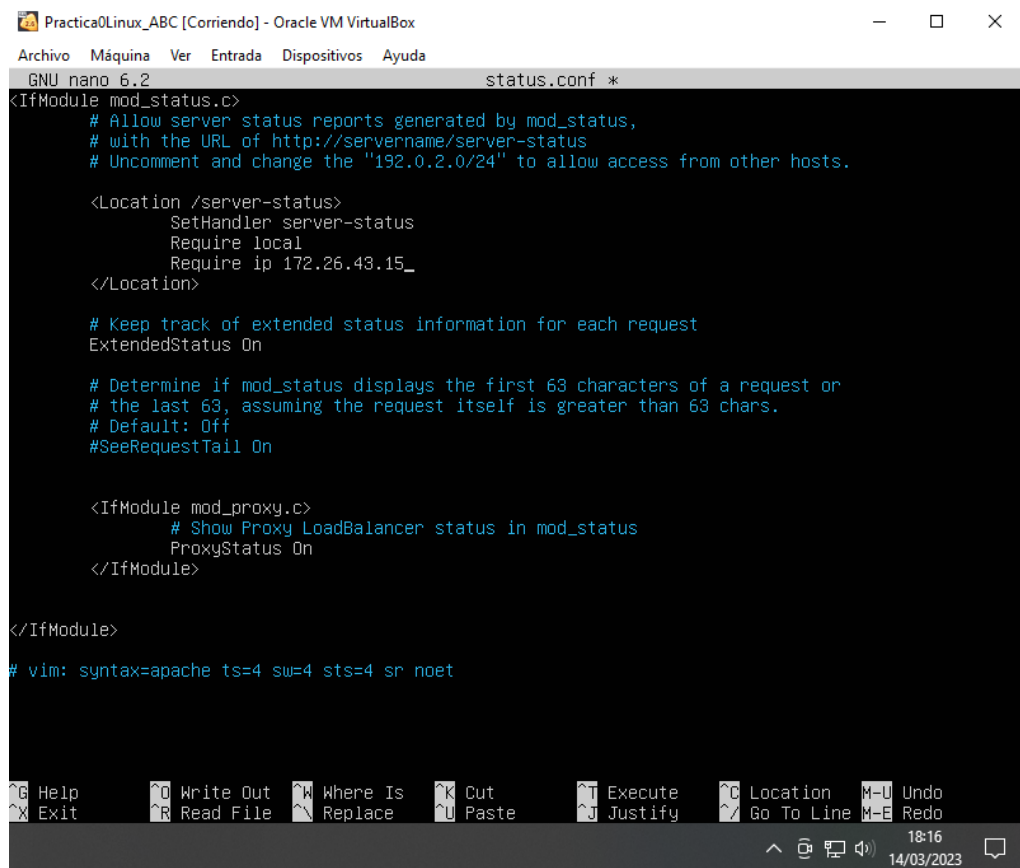
`status` permite monitorizar el rendimiento del servidor Apache (generando un HTML).

`info` proporciona una vista resumida de la configuración del servidor.

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

```
angela@servidorLinuxabc:~$ cd /etc/apache2/mods-enabled/
angela@servidorLinuxabc:/etc/apache2/mods-enabled$ sudo a2enmod status
Module status already enabled
angela@servidorLinuxabc:/etc/apache2/mods-enabled$
```


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



The screenshot shows a terminal window titled "Practica0Linux_ABC [Corriendo] - Oracle VM VirtualBox". The terminal is running the GNU nano 6.2 editor, editing the file "status.conf". The content of the file is as follows:

```
<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 172.26.43.15_
</Location>

# Keep track of extended status information for each request
ExtendedStatus On

# Determine if mod_status displays the first 63 characters of a request or
# the last 63, assuming the request itself is greater than 63 chars.
# Default: Off
#SeeRequestTail On

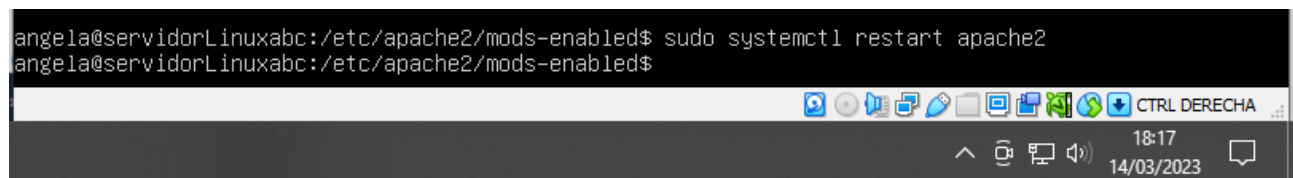
<IfModule mod_proxy.c>
    # Show Proxy LoadBalancer status in mod_status
    ProxyStatus On
</IfModule>

</IfModule>

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

The terminal window also shows a menu bar with options like "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". At the bottom, there is a status bar showing the time "18:16" and the date "14/03/2023".

PASO 3) Reinicia el servidor para aplicar los cambios.



The screenshot shows a terminal window with the following command and output:

```
angela@servidorLinuxabc:/etc/apache2/mods-enabled$ sudo systemctl restart apache2
angela@servidorLinuxabc:/etc/apache2/mods-enabled$
```

The terminal window also shows a menu bar with options like "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". At the bottom, there is a status bar showing the time "18:17" and the date "14/03/2023".

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

Apache Status

No es seguro | 172.26.2.215/server-status

Google Moodle Centros IES Velazquez

Apache Server Status for 172.26.2.215 (via 172.26.2.215)

Server Version: Apache/2.4.52 (Ubuntu) OpenSSL/3.0.2
 Server MPM: event
 Server Built: 2022-06-14T12:30:21

Current Time: Tuesday, 14-Mar-2023 17:18:24 UTC
 Restart Time: Tuesday, 14-Mar-2023 17:17:56 UTC
 Parent Server Config. Generation: 1
 Parent Server MPM Generation: 0
 Server uptime: 27 seconds
 Server load: 0.00 0.01 0.00
 Total accesses: 0 - Total Traffic: 0 kB - Total Duration: 0
 CPU Usage: u0 s0 cu0 cs0
 0 requests/sec - 0 B/second
 1 requests currently being processed, 49 idle workers

| Slot | PID | Stopping | Connections | | Threads | | Async connections | | |
|------|------|----------|-------------|-----------|---------|------|-------------------|------------|---------|
| | | | total | accepting | busy | idle | writing | keep-alive | closing |
| 0 | 1114 | no | 0 | yes | 0 | 25 | 0 | 0 | 0 |
| 1 | 1115 | no | 0 | yes | 1 | 24 | 0 | 0 | 0 |
| Sum | 2 | 0 | 0 | | 1 | 49 | 0 | 0 | 0 |

.....w.....

Scoreboard Key:
 " " Waiting for Connection, "s" Starting up, "r" Reading Request,
 "w" Sending Reply, "k" Keepalive (read), "b" DNS Lookup,
 "c" Closing connection, "L" Logging, "G" Gracefully finishing,
 "I" Idle cleanup of worker, "." Open slot with no current process

| Srv | PID | Acc | M | CPU | SS | Req | Dur | Conn | Child | Slot | Client | Protocol | VHost | Request |
|-----|------|-------|---|------|----|-----|-----|------|-------|------|--------------|----------|-----------------|-----------------------------|
| 1-0 | 1115 | 1/0/0 | W | 0.00 | 0 | 0 | 0 | 0.0 | 0.00 | 0.00 | 172.26.43.15 | http/1.1 | 172.26.2.215:80 | GET /server-status HTTP/1.1 |

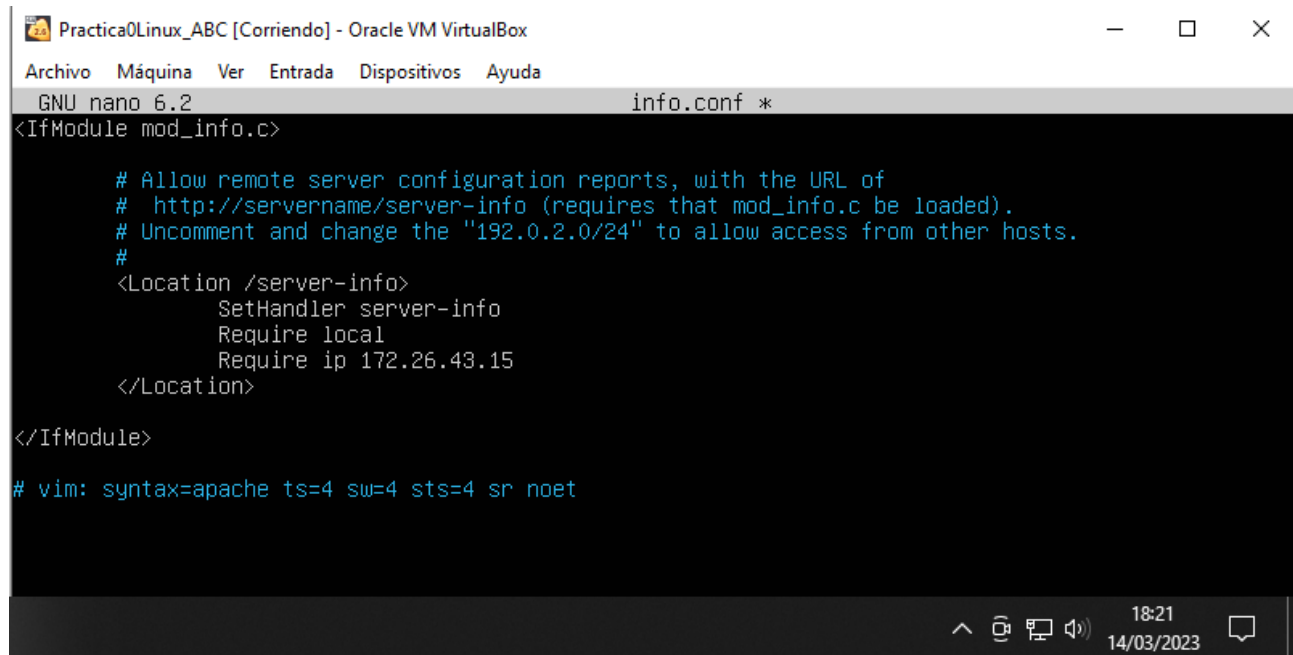
Srv Child Server number - generation
PID OS process ID
Acc Number of accesses this connection / this child / this slot
M Mode of operation
CPU CPU usage, number of seconds
SS Seconds since beginning of most recent request
Req Milliseconds required to process most recent request
Dur Sum of milliseconds required to process all requests
Conn Kilobytes transferred this connection
Child Megabytes transferred this child

Toma una captura de los pasos 2 y 4.

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

```
angela@servidorLinuxabc:/etc/apache2/mods-enabled$ sudo a2enmod info
Enabling module info.
To activate the new configuration, you need to run:
  systemctl restart apache2
angela@servidorLinuxabc:/etc/apache2/mods-enabled$ sudo systemctl restart apache2
angela@servidorLinuxabc:/etc/apache2/mods-enabled$ _
```

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

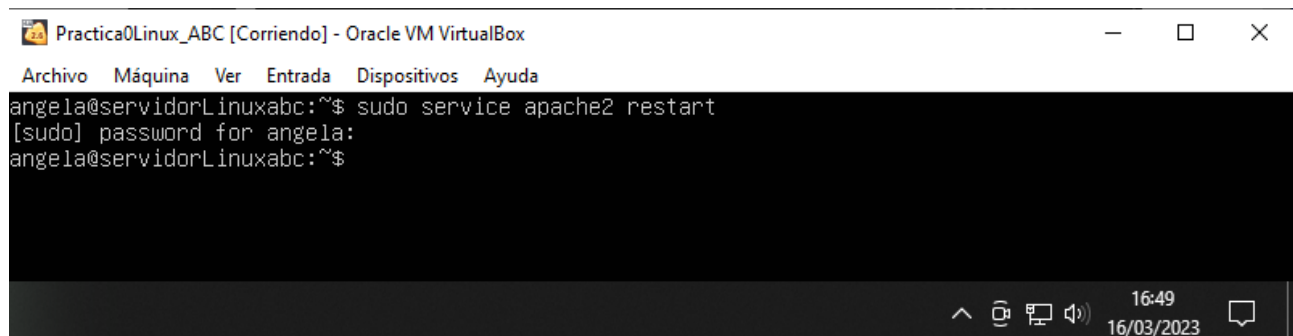


```
Practica0Linux_ABC [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 6.2 info.conf *
<IfModule mod_info.c>

    # 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 172.26.43.15
    </Location>
</IfModule>

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

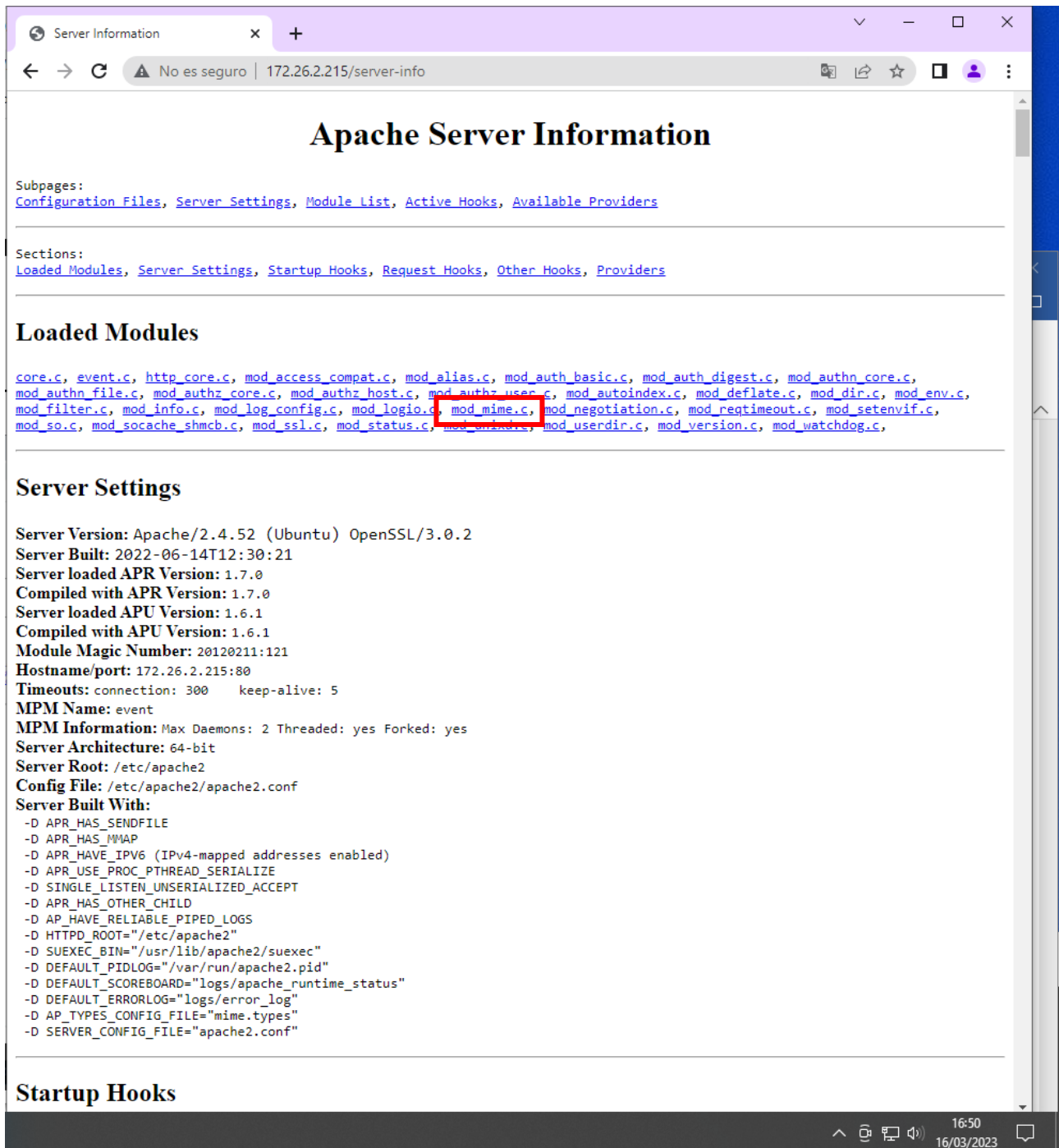
PASO 7) Reinicia el servidor para aplicar los cambios.



```
Practica0Linux_ABC [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
angela@servidorLinuxabc:~$ sudo service apache2 restart
[sudo] password for angela:
angela@servidorLinuxabc:~$
```

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?



Server Information

No es seguro | 172.26.2.215/server-info

Apache Server Information

Subpages:
[Configuration Files](#), [Server Settings](#), [Module List](#), [Active Hooks](#), [Available Providers](#)

Sections:
[Loaded Modules](#), [Server Settings](#), [Startup Hooks](#), [Request Hooks](#), [Other Hooks](#), [Providers](#)

Loaded Modules

[core.c](#), [event.c](#), [http_core.c](#), [mod_access_compat.c](#), [mod_alias.c](#), [mod_auth_basic.c](#), [mod_auth_digest.c](#), [mod_authn_core.c](#), [mod_authn_file.c](#), [mod_authz_core.c](#), [mod_authz_host.c](#), [mod_authz_user.c](#), [mod_autoindex.c](#), [mod_deflate.c](#), [mod_dir.c](#), [mod_env.c](#), [mod_filter.c](#), [mod_info.c](#), [mod_log_config.c](#), [mod_logio.c](#), [mod_mime.c](#), [mod_negotiation.c](#), [mod_reqtimeout.c](#), [mod_setenvif.c](#), [mod_so.c](#), [mod_socache_shmcb.c](#), [mod_ssl.c](#), [mod_status.c](#), [mod_strerror.c](#), [mod_userdir.c](#), [mod_version.c](#), [mod_watchdog.c](#)

Server Settings

Server Version: Apache/2.4.52 (Ubuntu) OpenSSL/3.0.2
Server Built: 2022-06-14T12:30:21
Server loaded APR Version: 1.7.0
Compiled with APR Version: 1.7.0
Server loaded APU Version: 1.6.1
Compiled with APU Version: 1.6.1
Module Magic Number: 20120211:121
Hostname/port: 172.26.2.215:80
Timeouts: connection: 300 keep-alive: 5
MPM Name: event
MPM Information: Max Daemons: 2 Threaded: yes Forked: yes
Server Architecture: 64-bit
Server Root: /etc/apache2
Config File: /etc/apache2/apache2.conf
Server Built With:
-D APR_HAS_SENDFILE
-D APR_HAS_MMAP
-D APR_HAVE_IPV6 (IPv4-mapped addresses enabled)
-D APR_USE_PROC_PTHREAD_SERIALIZE
-D SINGLE_LISTEN_UNSERIALIZED_ACCEPT
-D APR_HAS_OTHER_CHILD
-D AP_HAVE_RELIABLE_PIPED_LOGS
-D HTTPD_ROOT="/etc/apache2"
-D SUEXEC_BIN="/usr/lib/apache2/suexec"
-D DEFAULT_PIDLOG="/var/run/apache2.pid"
-D DEFAULT_SCOREBOARD="logs/apache_runtime_status"
-D DEFAULT_ERRORLOG="logs/error_log"
-D AP_TYPES_CONFIG_FILE="mime.types"
-D SERVER_CONFIG_FILE="apache2.conf"

Startup Hooks

Module Name: [mod_mime.c](#)

Content handlers: none

Configuration Phase Participation: Create Directory Config, Merge Directory Configs

Request Phase Participation: Check Type

Module Directives:

AddCharset - a charset (e.g., iso-2022-jp), followed by one or more file extensions
 AddEncoding - an encoding (e.g., gzip), followed by one or more file extensions
 AddHandler - a handler name followed by one or more file extensions
 AddInputFilter - input filter name (or ; delimited names) followed by one or more file extensions
 AddLanguage - a language (e.g., fr), followed by one or more file extensions
 AddOutputFilter - output filter name (or ; delimited names) followed by one or more file extensions
 AddType - a mime type followed by one or more file extensions
 DefaultLanguage - language to use for documents with no other language file extension
 MultiViewsMatch - NegotiatedOnly (default), Handlers and/or Filters, or Any
 RemoveCharset - one or more file extensions
 RemoveEncoding - one or more file extensions
 RemoveHandler - one or more file extensions
 RemoveInputFilter - one or more file extensions
 RemoveLanguage - one or more file extensions
 RemoveOutputFilter - one or more file extensions
 RemoveType - one or more file extensions
 TypesConfig - the MIME types config file
 ModMimeUsePathInfo - Set to 'yes' to allow mod_mime to use path info for type checking

Current Configuration:

In file: /etc/apache2/mods-enabled/mime.conf
 7: TypesConfig /etc/mime.types
 27: AddType application/x-compress .Z
 28: AddType application/x-gzip .gz .tgz
 29: AddType application/x-bzip2 .bz2
 69: AddLanguage am .amh
 70: AddLanguage ar .ara
 71: AddLanguage be .be
 72: AddLanguage bg .bg
 73: AddLanguage bn .bn
 74: AddLanguage br .br
 75: AddLanguage bs .bs

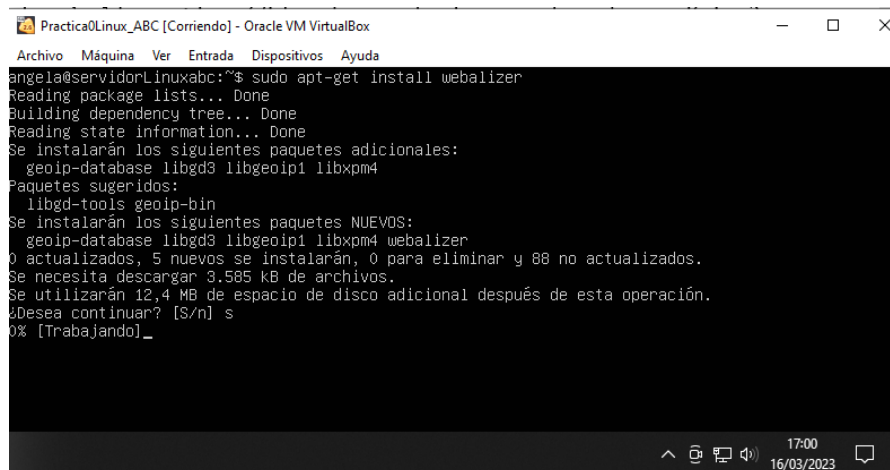
177: AddCharset UTF-16LE .utf16le
 196: AddCharset UTF-16LE .utf16le
 197: AddCharset UTF-32 .utf32
 198: AddCharset UTF-32BE .utf32be
 199: AddCharset UTF-32LE .utf32le
 200: AddCharset euc-cn .euc-cn
 201: AddCharset euc-gb .euc-gb
 202: AddCharset euc-jp .euc-jp

Toma una captura de los pasos 6 y 8.

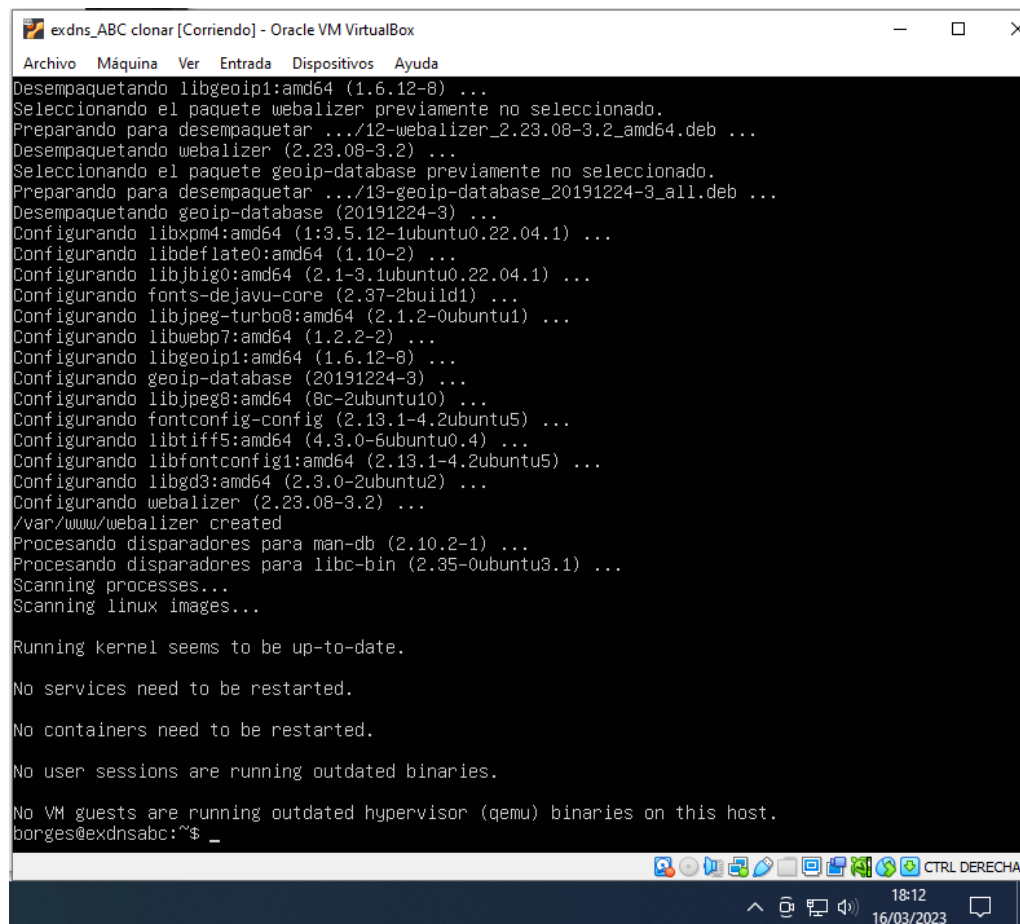
G) Webalizer

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).



```
Practica0Linux_ABC [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
angela@servidorLinuxabc:~$ sudo apt-get install webalizer
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Se instalarán los siguientes paquetes adicionales:
  geoip-database libgd3 libgeoip1 libxpm4
Paquetes sugeridos:
  libgd-tools geoip-bin
Se instalarán los siguientes paquetes NUEVOS:
  geoip-database libgd3 libgeoip1 libxpm4 webalizer
0 actualizados, 5 nuevos se instalarán, 0 para eliminar y 88 no actualizados.
Se necesita descargar 3.585 kB de archivos.
Se utilizarán 12,4 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
0% [Trabajando]
```



```
exdns_ABC clonar [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Desempaquetando libgeoip1:amd64 (1.6.12-8) ...
Seleccionando el paquete webalizer previamente no seleccionado.
Preparando para desempaquetar .../12-webalizer_2.23.08-3.2_amd64.deb ...
Desempaquetando webalizer (2.23.08-3.2) ...
Seleccionando el paquete geoip-database previamente no seleccionado.
Preparando para desempaquetar .../13-geoip-database_20191224-3_all.deb ...
Desempaquetando geoip-database (20191224-3) ...
Configurando libxpm4:amd64 (1:3.5.12-1ubuntu0.22.04.1) ...
Configurando libdeflate0:amd64 (1.10-2) ...
Configurando libjbig0:amd64 (2.1-3.1ubuntu0.22.04.1) ...
Configurando fonts-dejavu-core (2.37-2build1) ...
Configurando libjpeg-turbo8:amd64 (2.1.2-0ubuntu1) ...
Configurando libwebp7:amd64 (1.2.2-2) ...
Configurando libgeoip1:amd64 (1.6.12-8) ...
Configurando geoip-database (20191224-3) ...
Configurando libjpeg8:amd64 (8c-2ubuntu10) ...
Configurando fontconfig-config (2.13.1-4.2ubuntu5) ...
Configurando libtiff5:amd64 (4.3.0-6ubuntu0.4) ...
Configurando libfontconfig1:amd64 (2.13.1-4.2ubuntu5) ...
Configurando libgd3:amd64 (2.3.0-2ubuntu2) ...
Configurando webalizer (2.23.08-3.2) ...
/var/www/webalizer created
Procesando disparadores para man-db (2.10.2-1) ...
Procesando disparadores para libc-bin (2.35-0ubuntu3.1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
borges@exdnsabc:~$
```

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.

```

default          login.defs        protocols        update-manager
deluser.conf     logrotate.conf   python3          update-motd.d
depmod.d         logrotate.d      python3.10       update-notifier
dhcp            lvm              rc0.d            UPower
dpkg            machine-id       rc1.d            usb_modeswitch.conf
e2scrub.conf     magic            rc2.d            usb_modeswitch.d
environment      magic.mime       rc3.d            vim
ethertypes       mailcap          rc4.d            vmware-tools
fonts           mailcap.order    rc5.d            vtrngb
fstab            manpath.config  rc6.d            webalizer
fuse.conf        mdadm           rc8.d            wget
fwupd           mime.types      resolv.conf      X11
gai.conf         mke2fs.conf     rmt              xattr.conf
groff            ModemManager    rpc              xdg
group            modprobe.d      rsyslog.conf     zsh_command_not_found
group-          modules         screenrc
grub.d           modules-load.d  security
gshadow
borges@exdnsabc:/etc$ _

```

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.**

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:

```

borges@exdnsabc:/var/www$ ls
html webalizer
borges@exdnsabc:/var/www$ _

```

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

```

borges@exdnsabc:/$ sudo mv /var/www/webalizer/ /var/www/html/
borges@exdnsabc:/$ ls
bin  dev  home  lib32  libx32  media  opt  root  sbin  srv  sys  usr
boot  etc  lib  lib64  lost+found  mnt  proc  run  snap  swap.img  tmp  var
borges@exdnsabc:/$ cd /var/www/
borges@exdnsabc:/var/www$ ls
html
borges@exdnsabc:/var/www$

```

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

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

```

GNU nano 4.8 /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 "COPYING" 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 STDIN. 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 (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/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

```

exdns_ABC clonar [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

GNU nano 6.2 /etc/webalizer/webalizer.conf

```

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),
# 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

# 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

# Incremental processing allows multiple partial log files to be used
# instead of one huge one. Useful for large sites that have to rotate
# their log files more than once a month. The Webalizer will save its
# internal state before exiting, and restore it the next time run, in
# order to continue processing where it left off. This mode also causes
# The Webalizer to scan for and ignore duplicate records (records already
# processed by a previous run). See the README file for additional

```

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

[Icons] CTRL DERECHA

18:20
 16/03/2023


```
# 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

# Incremental processing allows multiple partial log files to be used
# instead of one huge one. Useful for large sites that have to rotate
# their log files more than once a month. The Webalizer will save its
# internal state before exiting, and restore it the next time run, in
# order to continue processing where it left off. This mode also causes
# The Webalizer to scan for and ignore duplicate records (records already
# processed by a previous run). See the README file for additional
```

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

CTRL DERECHA

18:21
16/03/2023

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.

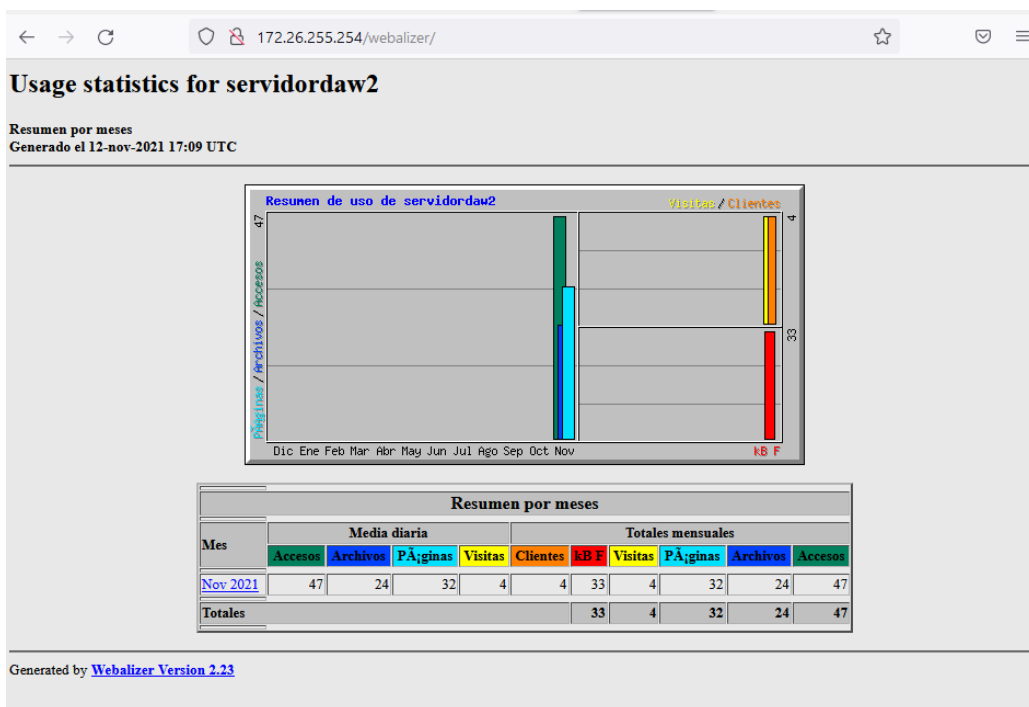
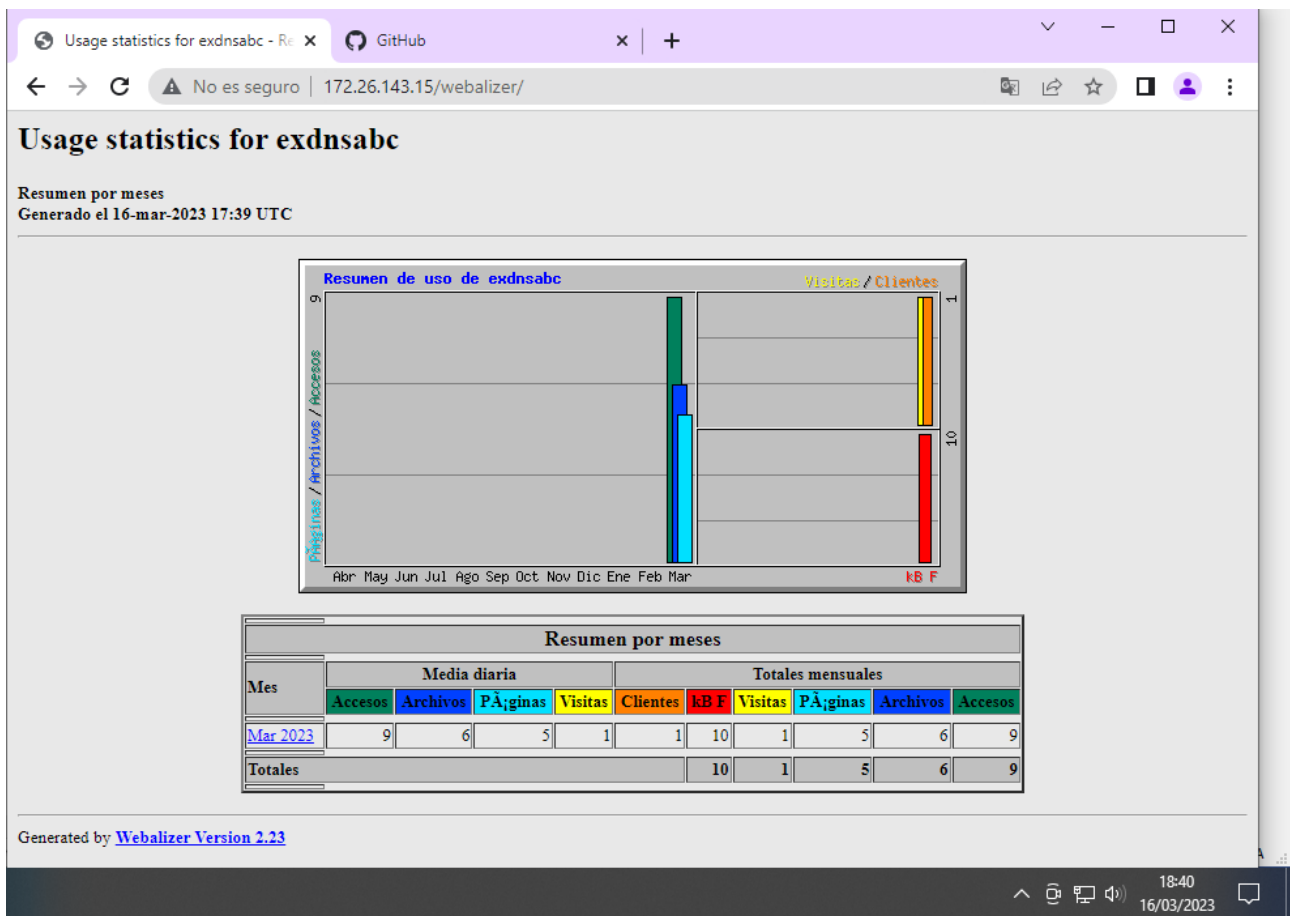
sudo webalizer

```
exdns_ABC clonar [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d3:76:e4 brd ff:ff:ff:ff:ff:ff
    inet 172.26.143.15/16 brd 172.26.255.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed3:76e4/64 scope link
        valid_lft forever preferred_lft forever
borges@exdnsabc:~$ sudo webalizer
[sudo] password for borges:
Webalizer V2.23-08 (Linux 5.15.0-58-generic x86_64) locale: #2#NV
Error: No puedo abrir histórico /var/log/apache2/access.log.1
borges@exdnsabc:~$ cd /var/www/html/
borges@exdnsabc:/var/www/html$ ls
index.html  webalizer
borges@exdnsabc:/var/www/html$ cd webalizer/
borges@exdnsabc:/var/www/html/webalizer$ ls
borges@exdnsabc:/var/www/html/webalizer$ cd /var/log/apache2/
borges@exdnsabc:/var/log/apache2$ ls
access.log  error.log  other_vhosts_access.log
borges@exdnsabc:/var/log/apache2$ cp access.log access.log.1
cp: cannot create regular file 'access.log.1': Permission denied
borges@exdnsabc:/var/log/apache2$ sudo cp access.log access.log.1
borges@exdnsabc:/var/log/apache2$ sudo webalizer
Webalizer V2.23-08 (Linux 5.15.0-58-generic x86_64) locale: ##*U
Utilizando histórico /var/log/apache2/access.log.1 (Clf)
Creando informe en /var/www/html/webalizer
El nombre de máquina en el informe es 'exdnsabc'
No encuentro el archivo histórico...
Generando informe de Marzo 2023
Guardando información de archivo...
Generando informe resumido
9 registros en 1 segundos, 9/sec
borges@exdnsabc:/var/log/apache2$ _
```

18:40
16/03/2023

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.

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