Actividad 1 – Ficheros de registros (logs)

1. Empezamos iniciando sesión en la maquina “Alias Server” y consultando el fichero de configuración

/etc/apache2/sites-available/000-default.conf

2. ¿Cuál es el fichero de logs de errores (directiva ErrorLog) y cuál es su nivel de prioridad (directiva LogLevel)? (Haz captura de pantalla)

```
# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
```

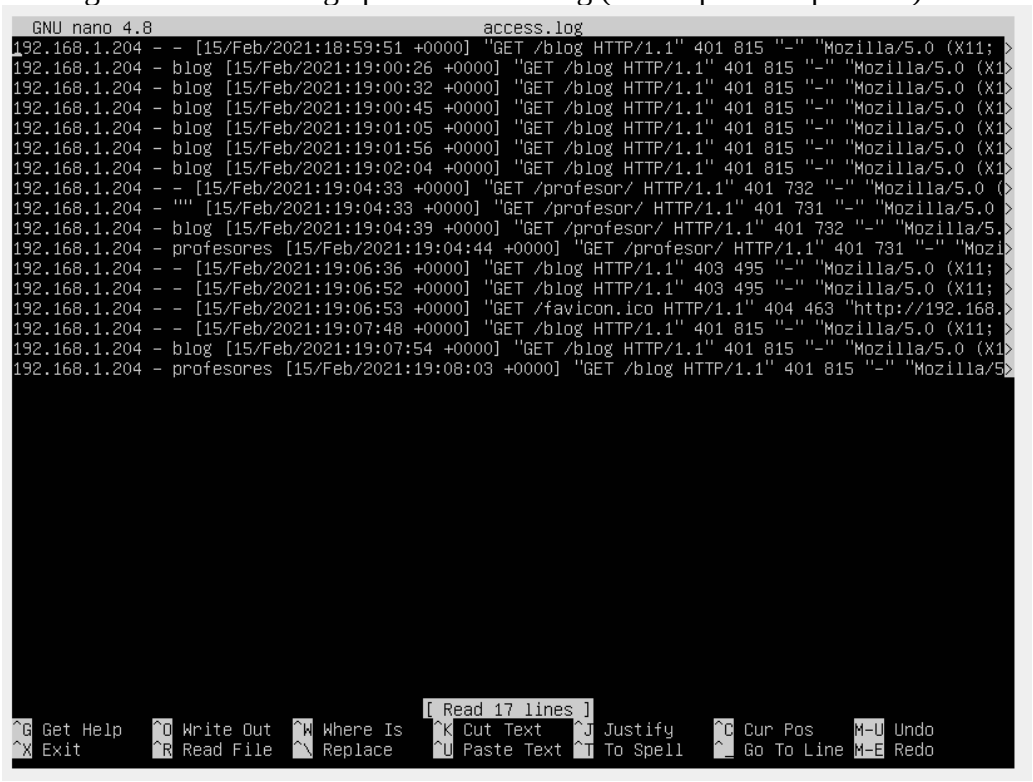
3. ¿Cuál es el fichero de logs de accesos (directiva CustomLog) y cuál es su formato (como no especifica ningún formato con LogFormat se usa el definido para el servidor principal en el fichero / etc/apache2/apache2.conf) (Haz captura de pantalla)

```
# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
```

4. Consulta el log de errores /var/log/apache2/error.log (Haz captura de pantalla)

```
  GNU nano 4.8                                 error.log
[Mon Feb 15 18:50:36.727893 2021] [mpm_event:notice] [pid 674:tid 140619334835264] AH00489: Apache/
[Mon Feb 15 18:50:36.727985 2021] [core:notice] [pid 674:tid 140619334835264] AH00094: Command line
[Mon Feb 15 18:50:37.874456 2021] [mpm_event:notice] [pid 674:tid 140619334835264] AH00493: SIGUSR1
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.
[Mon Feb 15 18:50:37.877553 2021] [mpm_event:notice] [pid 674:tid 140619334835264] AH00489: Apache/
[Mon Feb 15 18:50:37.877559 2021] [core:notice] [pid 674:tid 140619334835264] AH00094: Command line
[Mon Feb 15 19:00:26.184459 2021] [auth_digest:error] [pid 812:tid 140619200571136] [client 192.168
[Mon Feb 15 19:00:32.800497 2021] [auth_digest:error] [pid 813:tid 140619200571136] [client 192.168
[Mon Feb 15 19:00:45.916250 2021] [auth_digest:error] [pid 812:tid 140619234141952] [client 192.168
[Mon Feb 15 19:01:05.668527 2021] [auth_digest:error] [pid 813:tid 140619183785728] [client 192.168
[Mon Feb 15 19:01:56.986034 2021] [auth_digest:error] [pid 812:tid 140619242534656] [client 192.168
[Mon Feb 15 19:02:04.414055 2021] [auth_digest:error] [pid 813:tid 140619175393024] [client 192.168
[Mon Feb 15 19:04:33.897400 2021] [auth_basic:error] [pid 812:tid 140619125036800] [client 192.168.
[Mon Feb 15 19:04:39.817556 2021] [auth_basic:error] [pid 813:tid 140619158607616] [client 192.168.
[Mon Feb 15 19:04:44.555763 2021] [auth_basic:error] [pid 813:tid 140619234141952] [client 192.168.
[Mon Feb 15 19:06:27.374332 2021] [mpm_event:notice] [pid 674:tid 140619334835264] AH00491: caught
[Mon Feb 15 19:06:27.465717 2021] [mpm_event:notice] [pid 1240:tid 140158668319808] AH00489: Apache
[Mon Feb 15 19:06:27.465880 2021] [core:notice] [pid 1240:tid 140158668319808] AH00094: Command lin
[Mon Feb 15 19:06:36.257601 2021] [authz_core:error] [pid 1242:tid 140158615697152] [client 192.168
[Mon Feb 15 19:06:52.938954 2021] [authz_core:error] [pid 1242:tid 140158531790592] [client 192.168
[Mon Feb 15 19:07:43.018218 2021] [mpm_event:notice] [pid 1240:tid 140158668319808] AH00491: caught
[Mon Feb 15 19:07:43.091947 2021] [mpm_event:notice] [pid 1336:tid 140439373290560] AH00489: Apache
[Mon Feb 15 19:07:43.092021 2021] [core:notice] [pid 1336:tid 140439373290560] AH00094: Command lin
[Mon Feb 15 19:07:54.585355 2021] [auth_digest:error] [pid 1337:tid 140439362631424] [client 192.16
[Mon Feb 15 19:08:03.485723 2021] [auth_digest:error] [pid 1338:tid 140439256561408] [client 192.16
[Mon Feb 15 19:13:26.422902 2021] [mpm_event:notice] [pid 1336:tid 140439373290560] AH00491: caught
[Mon Feb 15 19:13:44.597664 2021] [mpm_event:notice] [pid 668:tid 139693962873920] AH00489: Apache/
[Mon Feb 15 19:13:44.604682 2021] [core:notice] [pid 668:tid 139693962873920] AH00094: Command line
                                [ Read 28 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos   M-U Undo
^X Exit      ^R Read File  ^\ Replace   ^U Paste Text ^T To Spell  ^_ Go To Line M-E Redo
```

5. Consulta el log de acceso /var/log/apache2/access.log (Haz captura de pantalla)

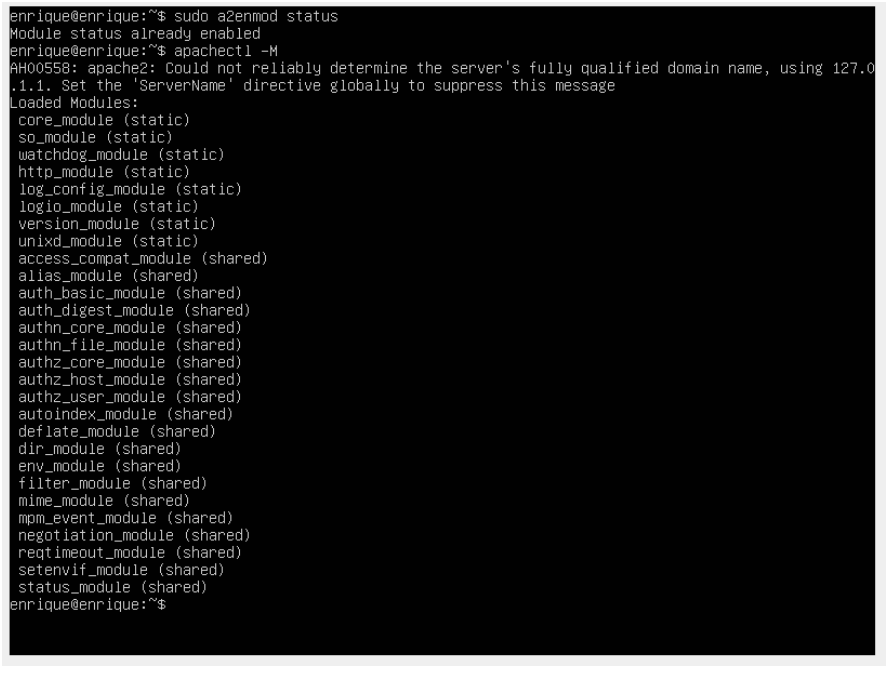


Actividad 2 - Módulos mod_status

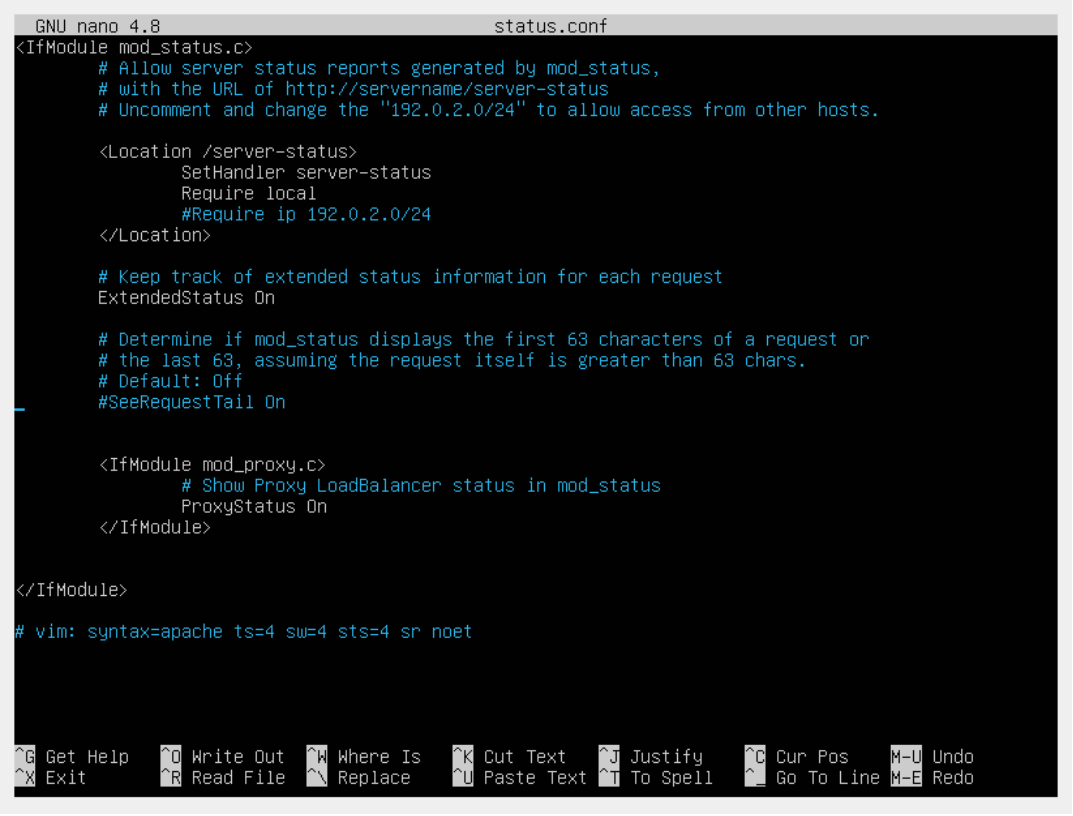
Mod_status permite monitorizar el rendimiento del servidor Apache. Genera un documento en HTML con información sobre el estado actual del servidor.

1. Inicia sesión en la maquina “Alias Server” como administrador y habilita el módulo mod_status, si no está habilitado. (Haz captura de pantalla del comando para la activación y comprobación posterior)

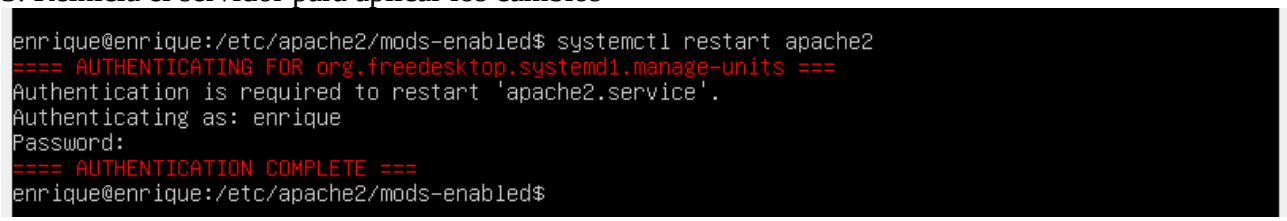
sudo a2enmod status



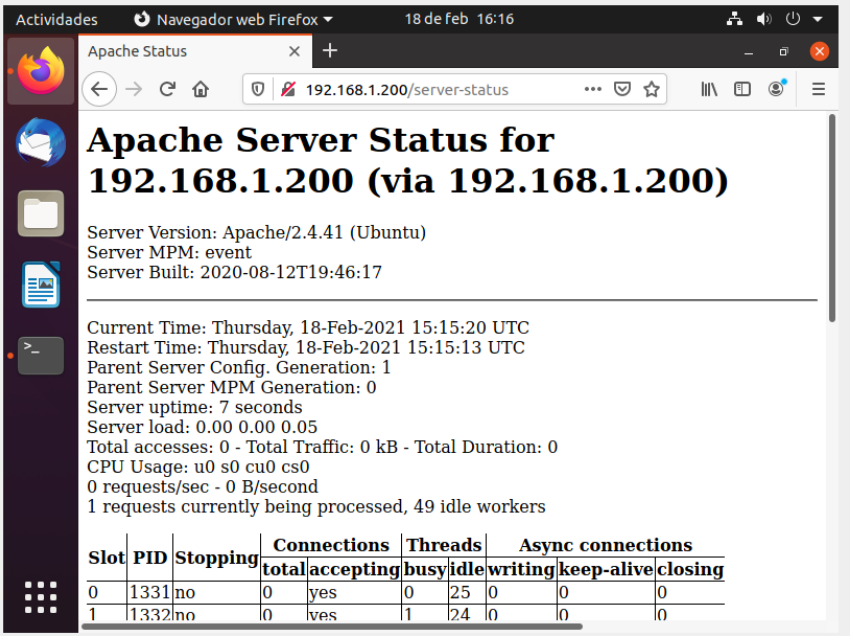
2. Edita el fichero de configuración del módulo /etc/apache2/mods-enabled/status.conf y habilita el acceso a /server-status desde la IP del cliente. (Haz captura de pantalla del fichero de configuración)



3. Reinicia el servidor para aplicar los cambios



4. Desde el cliente, accede a http://IP-SERVER/server-status (Haz captura de pantalla).



Actividad 3 - Módulo mod_info

Mod_info monitoriza el rendimiento del servidor Apache de forma resumida

1. Inicia sesión en la maquina “Alias Server” como administrador y habilita el módulo mod_info, si no está habilitado. (Haz captura de pantalla del comando para la activación y comprobación posterior)

sudo a2enmod info

```
enrique@enrique:/etc/apache2/mods-available$ sudo a2enmod info
Enabling module info.
To activate the new configuration, you need to run:
  systemctl restart apache2
enrique@enrique:/etc/apache2/mods-available$ systemctl restart apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to restart 'apache2.service'.
Authenticating as: enrique
Password:
==== AUTHENTICATION COMPLETE ===
enrique@enrique:/etc/apache2/mods-available$
```

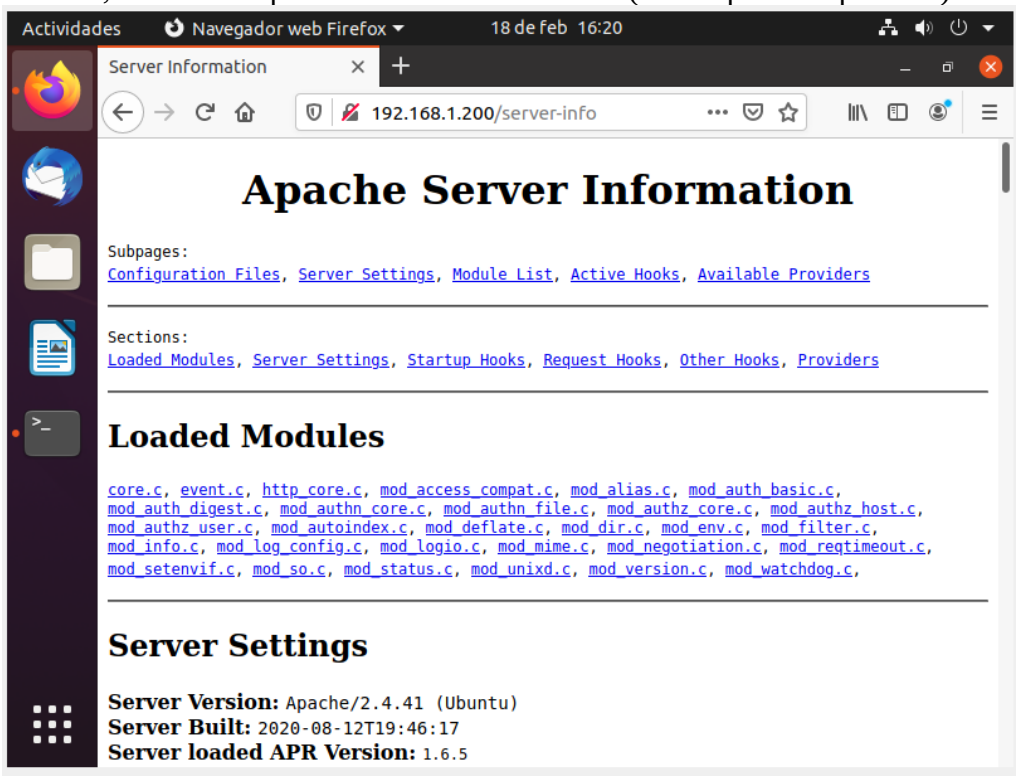
2. Edita el fichero de configuración del módulo /etc/apache2/mods-enabled/info.conf y habilita el acceso a /server-info desde el cliente (Pixel).

```
  GNU nano 4.8                                    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 192.168.1.216_
        </Location>

</IfModule>

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

3. Reinicia el servidor para aplicar los cambios

```
enrique@enrique:/etc/apache2/mods-available$ systemctl restart apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to restart 'apache2.service'.
Authenticating as: enrique
Password:
==== AUTHENTICATION COMPLETE ===
enrique@enrique:/etc/apache2/mods-available$ _
```

4. Desde el cliente, accede a http://IP-SERVER/server-info (Haz captura de pantalla).



Actividad 4 – Webalizer

Webalizer es un programa de análisis estadístico complejo capaz de producir tablas y gráficas sobre quienes están visitando el sitio web.

1. Inicia sesión en la maquina “Alias Server” como administrador

2. Instala el paquete webalizer (actualiza antes el repositorio)

sudo apt-get update

sudo apt-get install webalizer

```
enrique@enrique:~$ sudo apt-get install webalizer
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  fontconfig-config fonts-dejavu-core geoip-database libfontconfig1 libgd3 libgeoip1
  libjpeg-turbo8 libjpeg8 libtiff5 libwebp6 libxpm4
Suggested packages:
  libgd-tools geoip-bin
The following NEW packages will be installed:
  fontconfig-config fonts-dejavu-core geoip-database libfontconfig1 libgd3 libgeoip1
  libjpeg-turbo8 libjpeg8 libtiff5 libwebp6 libxpm4 webalizer
0 upgraded, 13 newly installed, 0 to remove and 121 not upgraded.
Need to get 5205 kB of archives.
After this operation, 17.6 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

3. Consulta el fichero de configuración /etc/webalizer/webalizer.conf y observa que se analizará el fichero de logs de accesos del servidor virtual por defecto. Quita la extensión .1, e indica /var/www/html/webalizer como directorio de salida.

OutputDir /var/www/html/webalizer

```
  GNU nano 4.8                                webalizer.conf
# at least one space or tab between the keyword and its value.
#
# As of version 0.98, 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 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

# 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

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  M-
^X Exit      ^R Read File  ^\ Replace   ^U Paste Text ^T To Spell ^_ Go To Line M-
```

5. Crea el directorio /var/ www/html/webalizer

```
enrique@enrique:~$ cd /var/www/html
enrique@enrique:/var/www/html$ ll
total 44
drwxr-xr-x 5 root root  4096 Feb 11 15:19 ./
drwxr-xr-x 4 root root  4096 Feb 18 15:30 ../
-rw-r--r-- 1 root root   173 Feb  1 21:54 404.html
drwxr-xr-x 2 root root  4096 Feb 11 15:19 carpetaprivada/
drwxr-xr-x 2 root root  4096 Feb  1 20:13 ciclos/
-rw-r--r-- 1 root root   125 Feb  1 20:15 despliegue.html
-rw-r--r-- 1 root root   112 Feb  1 19:57 fp.html
-rw-r--r-- 1 root root 10918 Jan 18 11:56 indice.html
drwxr-xr-x 2 root root  4096 Feb  6 18:10 profesor/
enrique@enrique:/var/www/html$ sudo mkdir webalizer
enrique@enrique:/var/www/html$ ll
total 48
drwxr-xr-x 6 root root  4096 Feb 18 15:36 ./
drwxr-xr-x 4 root root  4096 Feb 18 15:30 ../
-rw-r--r-- 1 root root   173 Feb  1 21:54 404.html
drwxr-xr-x 2 root root  4096 Feb 11 15:19 carpetaprivada/
drwxr-xr-x 2 root root  4096 Feb  1 20:13 ciclos/
-rw-r--r-- 1 root root   125 Feb  1 20:15 despliegue.html
-rw-r--r-- 1 root root   112 Feb  1 19:57 fp.html
-rw-r--r-- 1 root root 10918 Jan 18 11:56 indice.html
drwxr-xr-x 2 root root  4096 Feb  6 18:10 profesor/
drwxr-xr-x 2 root root  4096 Feb 18 15:36 webalizer/
enrique@enrique:/var/www/html$ _
```

6. Lanza el programa para que lea el fichero de log y genere el documento html con las estadísticas.

sudo webalizer (Haz captura de pantalla)

```
enrique@enrique:/var/www/html$ sudo webalizer
Webalizer V2.23-08 (Linux 5.4.0-62-generic x86_64) locale: /var/www/webalizer
Using logfile /var/log/apache2/access.log.1 (clf)
Creating output in /var/www/webalizer
Hostname for reports is 'enrique'
History file not found...
Generating report for February 2021
Saving history information...
Generating summary report
31 records in 1 seconds, 31/sec
enrique@enrique:/var/www/html$ _
```

7. Desde el cliente, accede a http://IP-SERVER/webalizer/index.html (Haz captura de pantalla).