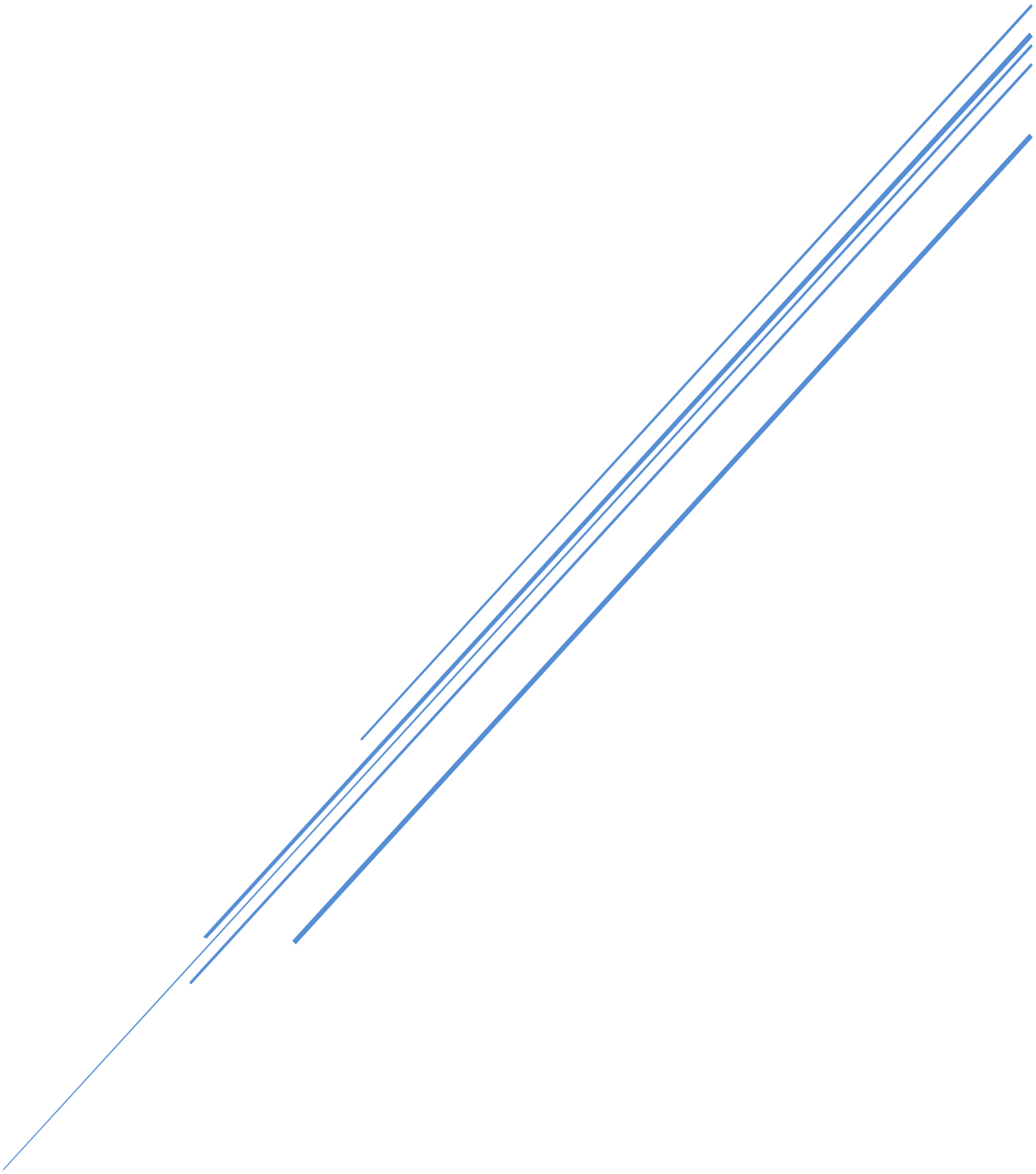
Memoria Práctica Obligatoria



Daniel Hernández Vega 70915236A
Álvaro López Marcos 70911319L

Información del Sistema

- La solución de la práctica ha sido desarrollada en un sistema Debian 9 de 32bits, dada la situación actual optamos por usar un ordenador para a modo de servidor, el cual estaría encendido de manera continua para poder trabajar cualquiera de nosotros en cualquier momento.
- Todo el software utilizado en la realización de la práctica ha sido software gratuito.

Configuración

BASE DE DATOS:

nombreUsuario	correo	nombre	apellidos	direccionPostal	esProfesor	clave	confirmacion	eliminar	editar	permisos

- nombreUsuario: guarda el “nick” del usuario;
- correo: guarda el email del usuario.
- nombre: guarda el nombre personal del usuario.
- apellidos: guarda los dos apellidos del usuario.
- direccionPostal: guarda la dirección Postal del usuario.
- esProfesor: almacena 0 ó 1. Si almacena 1 es profesor, si almacena 0 es alumno.
- confirmacion: almacena 0 ó 1. Si almacena 1 el usuario ya está registrado en el sistema linux, si almacena 0 el usuario sólo está registrado en la base de datos.
- eliminar: almacena 0 ó 1. Si almacena 1 el usuario está listo para ser eliminado del sistema, si almacena 0 todavía no está listo para ser eliminado del sistema.
- editar: almacena 0 ó 1. Si almacena 1 el usuario está listo para que su contraseña sea editada del sistema, si almacena 0 todavía no está listo para editar la contraseña del usuario del sistema.
- permisos: almacena 0 ó 1. Si almacena 1 el usuario está listo para que su carpeta personal sea cambiada al usuario correspondiente, si almacena 0 todavía no está listo para que su carpeta personal se modificada de propietario.

SCRIPTS A DESTACAR:

Ubicación de archivos cgi/perl: /usr/lib/cgi-bin
Ubicación de archivos html: /var/www/html

REGISTRO USUARIOS:

Para conseguir el registro de usuarios tanto en la base de datos como en el sistema, hacemos uso de dos scripts perl.

- *RegsitroBDD*:

  En este script leemos los datos que introduce el usuario a través del formulario de registro (usuario, contraseña, nombre, apellidos, correo, dirección Postal y grupo) . Posteriormente hacemos las comprobaciones necesarias para que el formulario sea llenado correctamente, como comprobar que las dos contraseñas son correctas, que no quede ningún campo vacío…E insertamos en la base de datos una nueva fila con todos los datos, poniendo a los registros que se rellenan con 0 ó 1, todos a 0. Finalmente, se le envía un correo con el link de confirmación de cuenta, para que este sea registrado en el sistema.

- *RegistroLinux:*

  Lee los datos que introduce el usuario a través del formulario de registro rellenando los campos; nombre de usuario y contraseña. Comprobamos con la base de datos si los datos introducidos son correctos y si el usuario no está confirmado. Posteriormente comprobamos si es profesor o no, para asignarle en nuestro caso el grupo 1004 de profesor o 1006 de alumno, creamos los directorios personales en la ruta home , con su carpeta apuntes y public_html con sus correspondientes permisos. En este script no le hacemos propietario al usuario de su directorio, lo

veremos más adelante el método usado. Mediante el módulo usermod le damos de alta en el sistema y posteriormente le establecemos las cuotas correspondientes.Finalmente le enviamos al usuario registrado un correo de bienvenida.

EDITAR USUARIOS:

Como en el registro de usuarios hacemos uso de dos scripts perl:

- *editarBDD:*

  Donde se recoge toda la información del formulario que el usuario quiera cambiar. El usuario y contraseña tienen que ser correctos, si es asi actualizamos de la base de datos los campos que el usuario a introducido y ponemos a 1 el campo editar. Finalmente ejecutamos el script editarLinux.

- *editarLinux:*

  Seleccionamos el usuario de la base de datos que tiene el campo editar igual a 1, y mediante el módulo usermod le asignamos la contraseña nueva que se guardó en la base de datos del script editarBDD.
  Para finalmente volviendo a poner el campo editar a 0.

BAJA USUARIOS:

También hacemos uso de dos scripts:

- *bajaUsuario*:

  Recoge la información del formulario, usuario y contraseña, mediante una sentencia sql seleccionamos los usuarios con ese usuario y contraseña, y posteriormente ponemos a ese el registro eliminar a 1 de ese usuario.
  Finalmente ejecutamos el script bajaLinux

- *bajaLinux*:

  Mediante sql seleccionamos el usuario con el registro eliminar a 1 y mediante el módulo usermod lo eliminamos del sistema y también su carpeta personal.
  Finalmente borramos el usuario de la base de datos.

FICHERO CRONTAB:
Es uno de los demonios o “daemon” (proceso en segundo plano) más importantes y habituales en el sistema. Su ejecución comienza desde el primer instante de arranque.

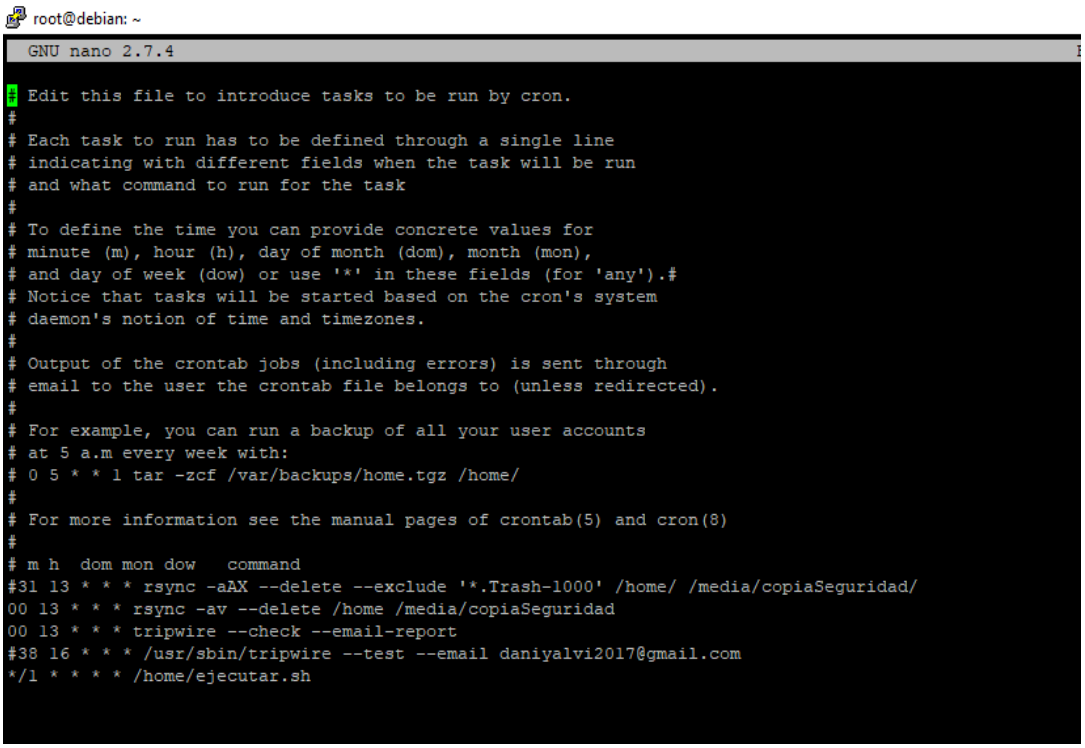
Su función principal es encargarse de lanzar las tareas programadas en fechas específicas y de forma automática y repetitiva. La definición de las tareas se localiza en el archivo /etc/crontab

Lo usamos para:

- Cada minuto de todos los dias, ejecute el script, ejecutar.sh.
  Este script ejecutar.sh nos ejecuta el el fichero perl “usuHom.pl” ubicado en /usr/local/bin/.
    - usuHome.pl: Recoge nombreUsuario y esProfesor de los usuario que tenga el campo permisos a 1 y le asigna el grupo y propietario a la carpeta de dicho usuario.

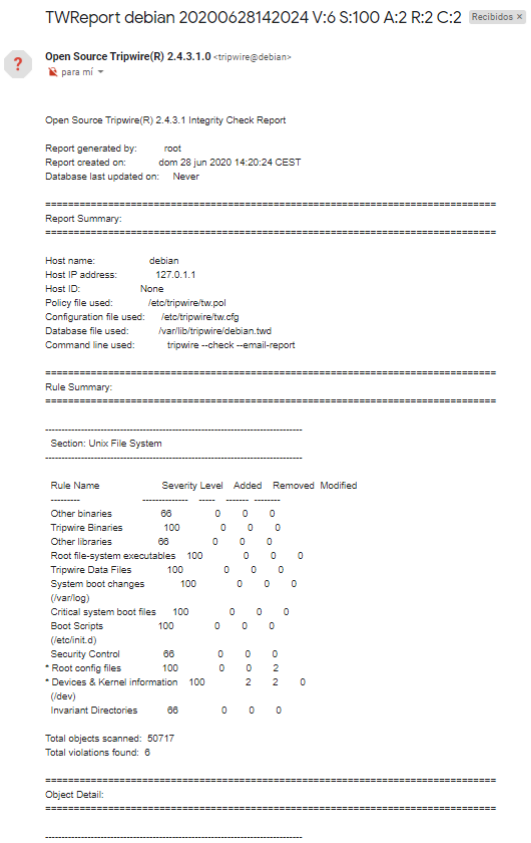
- A las 13:00 haga una copia de seguridad mediante rsync en el directorio /media/copiaSeguridad.

- A las 13:00 envía a nuestro correo un reporte mediante la herramienta tripwire que nos informa de los ficheros que han sido modificados.



TRIPWIRE

Tripwire monitorea rutinariamente la integridad de una gran cantidad de archivos que tienden a ser blanco de los atacantes.
Cada día recibimos via correo un resumen de los archivos modificados en el sistema.



TWReport debian 20200628142024 V:6 S:100 A:2 R:2 C:2 Recibidos ×

Open Source Tripwire(R) 2.4.3.1.0 <tripwire@debian>
para mí

Open Source Tripwire(R) 2.4.3.1 Integrity Check Report

Report generated by: root
Report created on: dom 28 jun 2020 14:20:24 CEST
Database last updated on: Never

Report Summary:

Host name: debian
Host IP address: 127.0.1.1
Host ID: None
Policy file used: /etc/tripwire/tw.pol
Configuration file used: /etc/tripwire/tw.cfg
Database file used: /var/lib/tripwire/debian.twd
Command line used: tripwire --check --email-report

Rule Summary:

Section: Unix File System

Rule Name	Severity Level	Added	Removed	Modified
Other binaries	66	0	0	0
Tripwire Binaries	100	0	0	0
Other libraries	66	0	0	0
Root file-system executables	100	0	0	0
Tripwire Data Files	100	0	0	0
System boot changes (/var/log)	100	0	0	0
Critical system boot files	100	0	0	0
Boot Scripts (/etc/init.d)	100	0	0	0
Security Control	66	0	0	0
* Root config files	100	0	0	2
* Devices & Kernel information (/dev)	100	2	2	0
Invariant Directories	66	0	0	0

Total objects scanned: 50717
Total violations found: 6

Object Detail:

RSYNC

Lo usamos para hacer copias de seguridad de las carpetas personales de los usuarios.
En el fichero crontab lo tenemos programado para que todos los días a las 13:00 se ejecute y copie los archivos a la carpeta /media/copiaSeguridad/

```
root@debian:/media/copiaSeguridad# ls -la
total 12
drwxr-xr-x  3 root       root       4096 jun 30 17:41 .
drwxr-xr-x  5 root       root       4096 jun 30 01:17 ..
drwxr-xr-x 15 scriptuser scriptuser 4096 jun 30 12:38 home
root@debian:/media/copiaSeguridad# cd /home
root@debian:/home# ls
a  admin  apuntes  ejecutar.sh  ew  f  public_html  qq  s  sa  scriptuser  teamspeak  xx  zz
root@debian:/home#
```

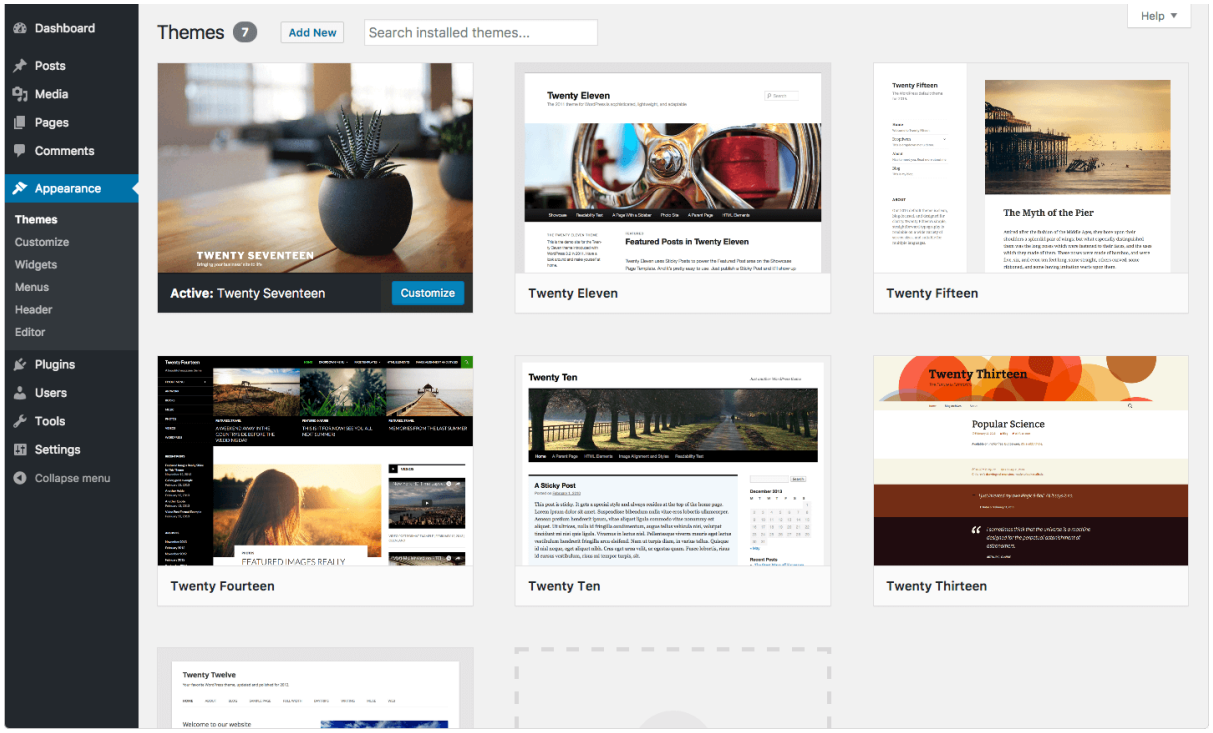
Requisitos del sistema. Servicios que se pueden solicitar por el usuario.

Correo electrónico:

Se ha instalado un servidor de correo electrónico para el envío de correos entre usuarios del servidor local. Además, se ha instalado un webmail, para la gestión de los correos por parte de los usuarios a través del explorador web. Nos hemos decantado por RoundCube.

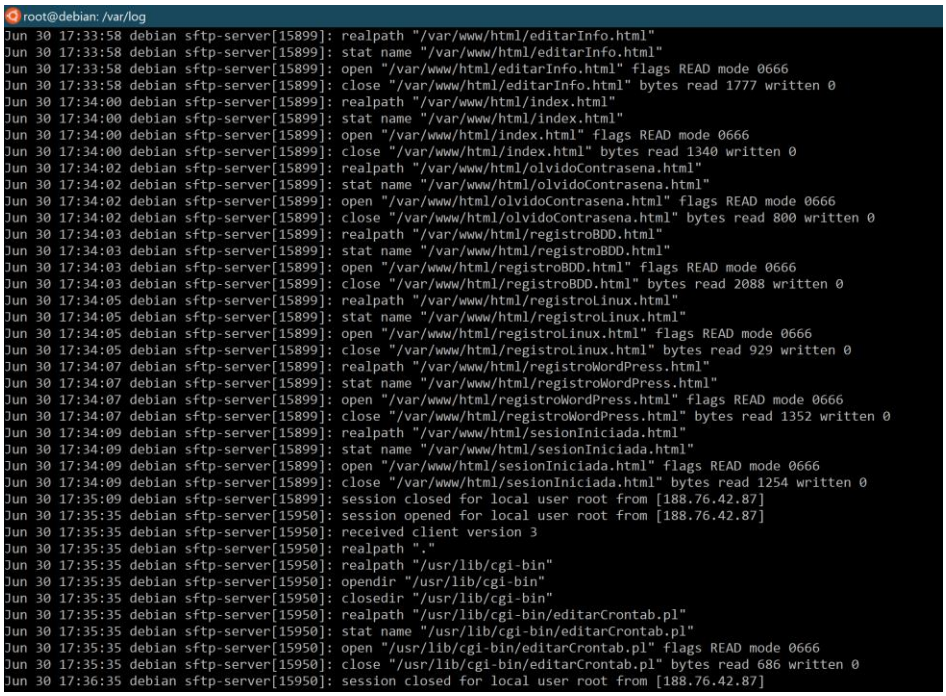
Web personal:

El sistema ofrece a los usuarios la oportunidad de alojar un blog personal, de forma que el sistema pregunta por los datos del usuario y este genera una base de datos para el blog y un directorio con la instalación de su propia herramienta Wordpress.



SFTP:

El sistema ofrece la capacidad de conectarse a este mediante la herramienta sftp ya sea desde una consola o un gestor de transferencias de archivos como puede ser WinSCP. Además, todas las conexiones se registran en un fichero en la ruta /var/log destinado para dicho propósito. El nombre del archivo es sftp-server.log.

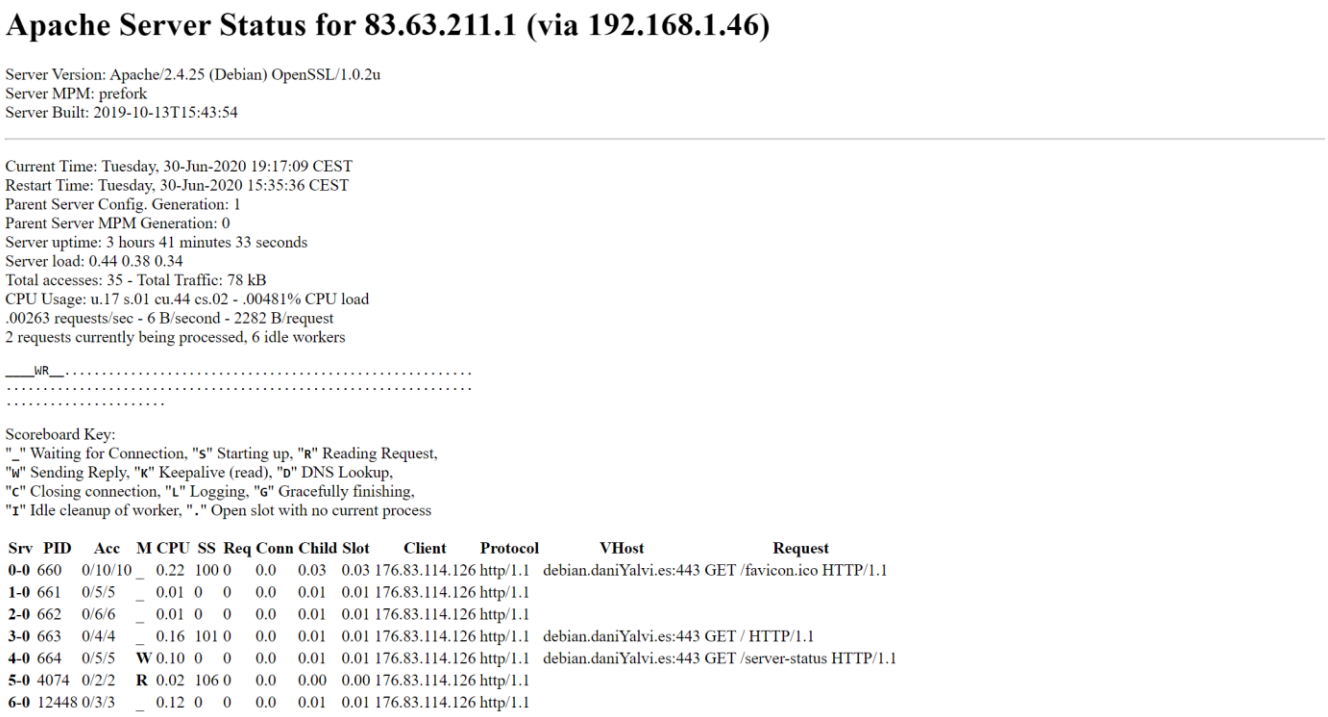


TeamSpeak3:

Se trata de un servidor que permite el chat de voz entre los usuarios. Nuestro problema ha sido que, una vez instalado y configurado el servidor, al iniciarlo, nos daba un exec format error. Investigando un poco llegamos a la conclusión de que nuestro sistema de 32bits no es compatible con dicho servidor y no fuimos capaces de encontrar una versión de este de 32 bits.

Monitorización:

En el servidor web se encuentra disponible en ‘https://localhost/server-status’ que nos informa del estado de los componentes del sistema, como la carga de cpu, las memorias, uso de disco o el tráfico de datos. Además, se informa mediante un correo todas las noches con el resumen de acciones llevadas a cabo en el sistema.



Apache Server Status for 83.63.211.1 (via 192.168.1.46)

Server Version: Apache/2.4.25 (Debian) OpenSSL/1.0.2u
Server MPM: prefork
Server Built: 2019-10-13T15:43:54

Current Time: Tuesday, 30-Jun-2020 19:17:09 CEST
Restart Time: Tuesday, 30-Jun-2020 15:35:36 CEST
Parent Server Config. Generation: 1
Parent Server MPM Generation: 0
Server uptime: 3 hours 41 minutes 33 seconds
Server load: 0.44 0.38 0.34
Total accesses: 35 - Total Traffic: 78 kB
CPU Usage: u.17 s.01 cu.44 cs.02 - .00481% CPU load
.00263 requests/sec - 6 B/second - 2282 B/request
2 requests currently being processed, 6 idle workers

____WR__.....
.....
.....

Scoreboard Key:
"_" Waiting for Connection, "S" Starting up, "R" Reading Request,
"W" Sending Reply, "K" Keepalive (read), "D" 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	Conn	Child	Slot	Client	Protocol	VHost	Request
0-0	660	0/10/10	_	0.22	100	0	0.0	0.03	0.03	176.83.114.126	http/1.1	debian.daniYalvi.es:443	GET /favicon.ico HTTP/1.1
1-0	661	0/5/5	_	0.01	0	0	0.0	0.01	0.01	176.83.114.126	http/1.1		
2-0	662	0/6/6	_	0.01	0	0	0.0	0.01	0.01	176.83.114.126	http/1.1		
3-0	663	0/4/4	_	0.16	101	0	0.0	0.01	0.01	176.83.114.126	http/1.1	debian.daniYalvi.es:443	GET / HTTP/1.1
4-0	664	0/5/5	W	0.10	0	0	0.0	0.01	0.01	176.83.114.126	http/1.1	debian.daniYalvi.es:443	GET /server-status HTTP/1.1
5-0	4074	0/2/2	R	0.02	106	0	0.0	0.00	0.00	176.83.114.126	http/1.1		
6-0	12448	0/3/3	_	0.12	0	0	0.0	0.01	0.01	176.83.114.126	http/1.1		

Moodle:

Ha sido instalado un servidor de moodle. Una plataforma diseñada para la gestión de clases y cursos, el administrador del servidor es el que añade a los miembros de los cursos y del servidor.