Anexo 1. Instalación y configuración de aplicaciones y servicios.

Autor: Antonio José Fortis Malagón

Tutor: Antonio Mancheño Bautista

Consultor UOC: Jordi Massager Pla

Índice

1.Introducción
2.Instalación del sistema operativo
3.Instalación y configuración del Servicio HTTP8
3.1.Certificado SSL auto-firmado
3.2.Apache211
3.3.Apache2 + SSL11
3.4.Apache2 + Php515
3.5.Apache2 + Php5 + MySQL15
3.6.Servicio FTP16
3.7.Servicio WebDAV17
4.Instalación y configuración del Servicio de Correo19
4.1.Servicio SMTP (Simple Mail Transfer Protocol)20
4.2.Servicio IMAP (Internet Message Access Protocol)
4.3.Configurar Postfix y Dovecot para SSL
4.4.Servicio WebMail
4.5.Filtros de correo (anti-virus, anti-spam)
5.Servicios de Seguridad
5.1.Ataques por Fuerza Bruta (Fail2Ban)32
5.2.Detección de Rootkits (Rootkit Hunter)
5.3.Auditoría de Seguridad (Debsecan)
6.Instalación Plataforma de Formación (Moodle)
7.Instalación Almacenamiento Virtual (OwnCloud)
8.Configuración del Cortafuegos42
0 Configuración de la Conie de Seguridad

1. Introducción

En este anexo, vamos a detallar el proceso de instalación y configuración de un sistema servidor GNU/Linux, en concreto, se instalará la distribución Debian 6, que ha sido la elegida para instalar y configurar sobre ella los diferentes servicios y aplicaciones que se citan en el proyecto.

Dicha documentación, servirá de base para que el administrador del sistema pueda acceder a ella y consultar todo el procedimiento seguido para la puesta en funcionamiento del servidor. En ella se va a detallar el proceso de instalación del sistema operativo y de cada una de las aplicaciones que ofrecen los diferentes servicios, indicando para cada una de ellas, la configuración que se ha realizado.

Para la instalación del sistema operativo, se ha utilizado **VirtualBox** como máquina virtual, ya que se trata de un software de código abierto que puede ser usado libremente.

2. Instalación del sistema operativo

Lo primero que vamos a hacer, es introducir un DVD que contenga una imagen de Debian 6, y una vez reconocido e iniciado el proceso de instalación, tendremos que indicarle el Lenguaje que deseamos, la Zona de Ubicación y la Distribución del teclado.

El siguiente paso, será asignar un nombre a la máquina, en cuyo caso se ha elegido el nombre **servidor**, tal y como podemos ver en la siguiente captura:

<u>4</u> áquina <u>V</u> er	<u>D</u> ispositivos	Ay <u>u</u> da	
		[1] Configurar la re	d
Por fav	or, introduzo	a el nombre de la màquina.	
El nomb adminis domésti	re de máquina trador de reo ca puede inve	≀es una sola palabra que identific ∣si no sabe qué nombre debería ten ntarse este nombre.	a el sistema en la red. Consulte al er. Si está configurando una red
Nombre	de la máquina	::	
servido	r		
<re< td=""><td>troceder></td><td></td><td><continuar></continuar></td></re<>	troceder>		<continuar></continuar>
Tab≻ mueve;	<espacio> se</espacio>	elecciona; <intro> activa un botón</intro>	
			😫 🚯 🖉 🖶 🥅 🕅 🚳 🔊 Ctrl Derecho

Además, habrá que elegir un nombre de dominio, siendo el elegido mmsierradecadiz.lan

<u>M</u> áqu	uina <u>V</u> er	<u>D</u> ispositivos	Ay <u>u</u> da						
_									
				- [!] Confi	gurar la	red 📙			
	El nom sistem invent nombre	mbre de domin ma. Habitualm cárselo si es e de dominio	io es la par ente es algo tá instaland en todos sus	te de su dir que termina o una red do ordenadores	rección de a por .com oméstica, 3.	Interne , .net, pero ase	t a la der .edu, o .(gúrese de	recha del nomb org. Puede utilizar el m	re de ismo
	Nombre	e de dominio:							
	mmsier	radecadiz.la	n						
	<f< td=""><td>(etroceder></td><td></td><td></td><td></td><td></td><td></td><td><continua< td=""><td>r></td></continua<></td></f<>	(etroceder>						<continua< td=""><td>r></td></continua<>	r>
<tab></tab>	mueve;	<espacio≻ s<="" td=""><td>elecciona; <</td><td>Intro≻ activ</td><td>a un botó</td><td>n</td><td></td><td></td><td></td></espacio≻>	elecciona; <	Intro≻ activ	a un botó	n			
						1	9 📀 🖉 🗗) 📖 🔘 [🚳 🖸 C	trl Derecho

A continuación, debemos de indicar la contraseña de **root**, además de generar un usuario con el cual trabajaremos. En este caso, el usuario elegido será **afortis**, tal y como podemos observar:



Seguidamente, deberemos de configurar la Zona horaria y seleccionar el Particionado de los discos, en cuyo caso se van a utilizar varias particiones tal y como podemos observar:

<u>M</u> áquina <u>V</u> er <u>D</u> ispositivos Ay <u>u</u> da
[!!] Particionado de discos
Éste es un resumen de las particiones y puntos de montaje que tiene configurados actualmente. Seleccione una partición para modificar sus valores (sistema de ficheros, puntos de montaje, etc.), el espacio libre para añadir una partición nueva o un dispositivo para inicializar la tabla de particiones.
Particionado guiado Configurar RAID por software Configurar el Gestor de Volúmenes Lógicos (LVM) Configurar los volúmenes cifrados
SCSI1 (0,0,0) (sda) – 8.6 GB ATA VBOX HARDDISK #1 primaria 349.2 MB B f ext3 / #5 lógica 3.0 GB f ext3 /usr #6 lógica 1.5 GB f ext3 /var #7 lógica 484.4 MB f intercambio intercambio #8 lógica 252.7 MB f ext3 /tmp #9 lógica 3.0 GB f ext3 /home
Deshacer los cambios realizados a las particiones Finalizar el particionado y escribir los cambios en el disco
<retroceder></retroceder>
<f1> para ayuda; <tab> mueve; <espacio> selecciona; <intro> activa un botón</intro></espacio></tab></f1>
Se 🖓 🗗 🗐 🚺 Ctrl Derecho

Una vez que se ha instalado el Sistema Base, debemos de seleccionar los programas que se van a instalar, en cuyo caso, no vamos a marcar ninguno, únicamente el servicio SSH, que nos permitirá conectarnos de forma segura y remota al servidor para administrarlo.

<u>M</u> áquina <u>V</u> er <u>D</u> ispositivos Ayuda
[!] Selección de programas De momento sólo está instalado el sistema básico. Puede escoger la instalación de las
siguientes colecciones predefinidas de programas para adaptar mas la instalacion a sus necesidades.
Elegir los programas a instalar:
 [] Entorno de escritorio gráfico [] Servidor de web [] Servidor de impresoras [] Servidor de DNS [] Servidor de ficheros [] Servidor de correo [] Base de datos SQL [*] Servidor SSH [] Ordenador portátil [] Utilidades estándar del sistema
< <u>Continuar></u>
<tab> mueve; <espacio> selecciona; <intro> activa un botón</intro></espacio></tab>
😂 🕢 🎜 🗐 🕐 Ctrl Derecho 👘

Finalizada la instalación de programas e instalado el Cargador de Arranque GRUB, tendremos el proceso de instalación finalizado.



Lo único que nos queda pendiente para comprobar la correcta instalación, será iniciar el sistema y ver que se carga correctamente.

<u>M</u> áquina <u>V</u> er <u>D</u> ispositivos Ay <u>u</u> da
Checking file systemsfsck from util-linux-ng 2.17.2 /dev/sda9: clean, 15/185104 files, 29118/740096 blocks /dev/sda8: clean, 12/61752 files, 13973/246784 blocks /dev/sda5: clean, 11671/182896 files, 75756/731392 blocks /dev/sda6: clean, 1207/89760 files, 24663/358656 blocks dope
Mounting local filesystemsdone. Activating swapfile swapdone. Cleaning up temporary files Setting kernel variablesdone. Configuring network interfacesdone. Cleaning up temporary files
Setting console screen modes. Skipping font and keymap setup (handled by console–setup). Setting up console font and keymapdone. INIT: Entering runlevel: 2 Using makefile–style concurrent boot in runlevel 2. Starting enhanced syslogd: rsyslogd.
Starting OpenBSD Secure Shell server: sshd. Starting periodic command scheduler: cron.
Deblan GNU/Linux 6.0 servidor ttyl servidor login: _ Servidor login: _

Lo siguiente que vamos a realizar sobre el sistema es actualizarlo a través de Internet, para ello, haremos uso del gestor de paquetes **aptitude**, utilizando para ello los comandos:

- aptitude update: actualiza la lista de paquetes existentes en los repositorios.
- **aptitude safe-upgrade**: una vez actualizada la lista de paquetes, permite instalar todas las actualizaciones disponibles, satisfaciendo todas las dependencias necesarias.

Una vez actualizado el sistema, para poder administrar el sistema de forma remota, se ha instalado el servidor SSH, el cual, es un protocolo de comunicaciones que encripta los datos intercambiados, haciendo imposible la violación de privacidad de la comunicación.

Para añadir un nivel de seguridad más a este servicio, vamos a realizar una modificación en el fichero de configuración del servicio SSH, el cual se encuentra en */etc/ssh/sshd_config* y nos va a permitir desactivar el login como root. Esta modificación, hay que realizarla en la siguiente sección:

```
#[...]
# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes
```

#[...]

De esta forma, para poder conectarnos al sistema, habrá que hacer un login con un usuario normal (en este caso **afortis**), y una vez que nos hemos identificado y accedido, adquirimos los privilegios de **root** según se puede observar en la siguiente imagen:

^

```
<u>Archivo Editar Ver Terminal Ayuda</u>
afortis@afortis-laptop:~$ ssh root@servidor.mmsierradecadiz.lan
root@servidor.mmsierradecadiz.lan's password:
Permission denied, please try again.
root@servidor.mmsierradecadiz.lan's password:
Permission denied, please try again.
root@servidor.mmsierradecadiz.lan's password:
afortis@afortis-laptop:~$ ssh afortis@servidor.mmsierradecadiz.lan
afortis@servidor.mmsierradecadiz.lan's password:
Linux servidor 2.6.32-5-686 #1 SMP Sun Sep 23 09:49:36 UTC 2012 i686
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Feb 5 20:55:15 2013 from 192.168.0.100
afortis@servidor:~$ su - root
Contraseña:
root@servidor:~#
```

3. Instalación y configuración del Servicio HTTP

En este apartado vamos a detallar el proceso de instalación de un Servidor HTTP, junto con una serie de complementos que le añadirán una mayor funcionalidad. El servidor elegido es **Apache2** y los complementos que se le van a añadir son **SSL**, **PHP5** y **MySQL**. Además, para establecer una conexión segura y de confianza vamos a generar un certificado que respalde la identidad del servidor.

3.1. Certificado SSL auto-firmado

Aunque los certificados son generalmente emitidos por entidades certificadoras (Certificate Authority) independientes y de confianza reconocida, para nuestro caso vamos a generar un certificado auto-firmado para una CA (Certificate Authority) creada por nosotros.

En primer lugar, vamos a generar el certificado de la CA (Certificate Authority) cifrado con una passphrase de 2048 bits y válido durante 365 días utilizando los siguientes comandos:

openssl genrsa -des3 -out caMMSC.key 2048 openssl req -new -x509 -days 365 -key caMMSC.key -out caMMSC.crt

dichos comandos, nos van a pedir una cierta información sobre la CA que paso a mostrar en la siguiente captura:



donde vamos a tener como resultado, el fichero **caMMSC.key** que corresponderá a la llave que usa la CA para firmar los certificados y el fichero **caMMSC.crt** que será el propio certificado de la CA.

A continuación, vamos a generar el certificado del servidor, utilizando para ello una clave de 1024 bits sin cifrar y que será firmado por la CA generada en el apartado anterior. Los comandos utilizados son los siguientes:

openssl genrsa -des3 -out servidorMMSC.key 1024

openssl req -new -key servidorMMSC.key -out servidorMMSC.csr

con la ejecución de dichos comandos, nos solicitará información sobre el servidor, que será la que muestro a continuación:

2	afortis@servidor: ~	• + ×
<u>A</u> rchivo <u>E</u> ditar <u>V</u> er <u>T</u> erminal Ay <u>u</u> da		
<pre>root@servidor:~/certificados# opensol Generating RSA private key, 1024 bit </pre>	. genrsa -des3 -out servidorMMSC.key 1024 long modulus vidorMMSC.key: . req -new -key servidorMMSC.key -out servidorMMSC.csr ey: iformation that will be incorporated .s called a Distinguished Name or a DN. can leave some blank ilt value, .eft blank.	
Country Name (2 letter code) [AU]:ES State or Province Name (full name) [S Locality Name (eg, city) []:Villamart Organization Name (eg, company) [Inte Organizational Unit Name (eg, section Common Name (eg, YOUR name) []:servid Email Address []:afortis@mmsierradeca	Gome-State]:Cádiz sín ernet Widgits Pty Ltd]:Mancomunidad Sierra de Cádiz n) []:Servidor Web Hor.mmsierradecadiz.lan ndiz.lan	
Please enter the following 'extra' at to be sent with your certificate requ A challenge password []: An optional company name []: root@servidor:~/certificados#	tributes uest	Ξ

para posteriormente, firmar el requerimiento anterior (servidorMMSC.csr) con la CA que nos hemos creado. Para ello ejecuto el siguiente comando:

openssl x509 -req -days 365 -in servidorMMSC.csr -CA caMMSC.crt -CAkey caMMSC.key -set_serial 01 -out servidorMMSC.crt

que generará el certificado del servidor firmado por nuestra CA (servidorMMSC.crt) y la clave privada para el servidor (servidorMMSC.key).

Como la clave privada del servidor está encriptada y protegida por una contraseña, ésta debe de escribirse cada vez que se accede al servicio. Si queremos generar la clave de forma que no obliguemos al servidor a pedir la contraseña, debemos de crear una **clave insegura** que se usará para iniciar el servicio y no requerir la clave cada vez.

Los comandos utilizados para generar esta clave a partir de la clave que ya teníamos creada, y crear una copia de seguridad de la clave segura, son los siguientes:

openssl rsa -in servidorMMSC.key -out servidorMMSC.key.insecure

mv servidorMMSC.key servidorMMSC.key.secure

mv servidorMMSC.key.insecure servidorMMSC.key

En este caso, al no pedir la clave al iniciar el servicio, debemos de tener en cuenta que dicha clave será almacenada, por lo tanto, si alguna persona tiene acceso al fichero, podría desencriptar toda la transmisión. Para solucionar este problema, se aconseja hacer que el fichero que contiene la clave (servidorMMSC.key) tenga permiso solamente de lectura por el root, lo cual, lo conseguimos con el comando **chmod 400 servidorMMSC.key**, asegurándonos que es el root el propietario de dicho fichero.

La siguiente captura, muestra las últimas operaciones realizadas para generar el certificado del servidor firmado por nuestra CA, y eliminar la clave de forma que no sea requerida cada vez que se conecte con dicho servidor:

```
Archivo Editar Ver Terminal Ayuda
root@servidor:~/certificados# openssl x509 -req -days 365 -in servidorMMSC.csr -CA caMMSC.crt -CAkA
ey caMMSC.key -set serial 01 -out servidorMMSC.crt
Signature ok
subject=/C=ES/ST=C\xC3\xA1diz/L=Villamart\xC3\xADn/0=Mancomunidad Sierra de C\xC3\xA1diz/0U=Servid
or Web/CN=servidor.mmsierradecadiz.lan/emailAddress=afortis@mmsierradecadiz.lan
Getting CA Private Key
Enter pass phrase for caMMSC.key:
root@servidor:~/certificados# openssl rsa -in servidorMMSC.key -out servidorMMSC.key.insecure
Enter pass phrase for servidorMMSC.key:
unable to load Private Key
946:error:06065064:digital envelope routines:EVP DecryptFinal ex:bad decrypt:evp enc.c:330:
946:error:0906A065:PEM routines:PEM do header:bad decrypt:pem lib.c:428:
root@servidor:~/certificados# openssl rsa -in servidorMMSC.key -out servidorMMSC.key.insecure
Enter pass phrase for servidorMMSC.key:
writing RSA key
root@servidor:~/certificados# mv servidorMMSC.key servidorMMSC.key.secure
root@servidor:~/certificados# mv servidorMMSC.key.insecure servidorMMSC.key
root@servidor:~/certificados# chmod 400 servidorMMSC.key
root@servidor:~/certificados# ls -al
total 32
drwxr-xr-x 2 root root 4096 feb 6 20:18 .
drwx----- 4 root root 4096 feb 6 19:24 ..
-rw-r--r-- 1 root root 1944 feb 6 19:27 caMMSC.crt
-rw-r--r-- 1 root root 1751 feb 6 19:25 caMMSC.key
-rw-r--r-- 1 root root 1294 feb 6 19:56 servidorMMSC.crt
-rw-r--r-- 1 root root 781 feb 6 19:44 servidorMMSC.csr
-r------ 1 root root 891 feb 6 20:17 servidorMMSC.key
-rw-r--r-- 1 root root 963 feb 6 19:42 servidorMMSC.key.secure
root@servidor:~/certificados#
```

A continuación, veremos como arrancar el servidor Apache2 de forma que se pueda acceder tanto con el protocolo HTTP, como con HTTPS, mediante el certificado de servidor que hemos creado y que ha sido firmado por nuestra propia CA (Certificate Authority).

3.2. Apache2

Para instalar **Apache2** vamos a hacer uso de los repositorios, ejecutando como root el siguiente comando:

aptitude install apache2

Una vez que ha sido instalado, para comprobar su funcionamiento, desde el navegador web de una máquina cliente, introducimos el nombre **http://servidor.mmsierradecadiz.lan** y veremos que el servidor web funciona, tal y como se muestra en la siguiente captura.



3.3. Apache2 + SSL

Si deseamos que en nuestro servidor web se puedan establecer conexiones seguras y encriptadas, debemos de activar el soporte SSL. De esta forma, será posible enviar y recibir información importante con la certeza de que ésta no podrá ser interceptada por terceras personas.

Durante la instalación de **Apache2** se crea una configuración para acceso seguro (HTTPS) de forma automática. Esta configuración deberá de ser modificada para incluir los certificados autofirmados generados previamente.

El fichero donde se almacena la configuración y sobre el que vamos a realizar las modificaciones es */etc/apache2/sites-available/default-ssl*, quedando como se muestra a continuación:

[...]

```
#
    SSL Engine Switch:
#
    Enable/Disable SSL for this virtual host.
SSLEngine on
#
    A self-signed (snakeoil) certificate can be created by installing
#
    the ssl-cert package. See
    /usr/share/doc/apache2.2-common/README.Debian.gz for more info.
#
    If both key and certificate are stored in the same file, only the
#
    SSLCertificateFile directive is needed.
#
                      /etc/ssl/certs/servidorMMSC.crt
SSLCertificateFile
SSLCertificateKeyFile /etc/ssl/private/servidorMMSC.key
```

```
# [...]
```

Aunque Apache2 está preparado para servir contenido HTTPS, aún hay que habilitar el módulo SSL y activar el sitio creado. Para ello ejecutaremos los comandos **a2enmod ssl** y **a2ensite default-ssl** respectivamente. Además, para que todos estos cambios surtan efecto, debemos de reiniciar el servicio, usando para ello el comando /etc/init.d/apache2 restart.

En la siguiente captura podemos ver la ejecución de dichos comandos:

				afortis@	servidor	: ~			• •	۲
<u>A</u> rchivo	<u>E</u> ditar	<u>V</u> er	<u>T</u> erminal	Ay <u>u</u> da						
root@ser Enabling See /usr and crea Run '/et root@ser Enabling Run '/et root@ser Restarti root@ser Reloadir root@ser	vidor:- module /share, ite sel c/init vidor:- isite o c/init vidor:- ng web vidor:- g web s vidor:-	-# a2 e ssl /doc/ f-sig .d/ap -# a2 defau .d/ap -# /e serv -# /e serve -# /e	apache2. apache2. ache2 re ensite d llt-ssl. ache2 re tc/init. er: apac tc/init. r config	l 2-common/ ificates. start' to efault-ss load' to d/apache2 he2 w d/apache2 : apache2	/README.D o activat sl activate 2 restart vaiting . 2 reload 2.	ebian.gz e new con e new con	on how t nfigurati figuratio	o configure on! n!	e SSL	

Si queremos verificar el correcto funcionamiento del servicio web seguro (HTTPS), deberemos de insertar en un navegador web la dirección <u>https://servidor.mmsierradecadiz.lan</u> y a continuación nos aparecerá una advertencia en la que se indica que la conexión es no confiable, debido a que dicho certificado (el certificado del servidor) ha sido firmado por una CA (la creada por nosotros) que no está reconocida, por lo tanto deberemos de confiar en ella para seguir adelante.

En la siguiente captura, se muestra la conexión realizada:



Una vez que aceptamos el certificado, tal y como podemos ver en la siguiente imagen

Está a punto de alterar cómo identifica Firef Los bancos, tiendas y otros sitios púl no le pedirán hacer esto.	fox este sitio. Dicos legítimos
Servidor	
Dirección: https://servidor.mmsierradecadiz.la	Obtener certificado
Estado del certificado	
Este sitio intenta identificarse a sí mismo con información no válida.	<u>V</u> er
Identidad desconocida	
No se confía en el certificado porque no ha sido autoridad reconocida usando una firma segura.	verificado por una
✓ Guardar esta exce <u>p</u> ción de manera permanen	te
Confirmar excepción de seguridad	Cancelar

nos podemos conectar al servidor web a través de una conexión segura (HTTPS), lo cual vamos a ver a continuación:



It works!

This is the default web page for this server. The web server software is running but no content has been added, yet. Una vez establecida la conexión con el servidor desde el cliente, podemos observar en el navegador del cliente que el certificado del servidor ha sido añadido, lo cual quedaría reflejado así

dropdav.com	www.dropdav.com:	Permanente	15/10/16	
GTE Corporation		rennanelite	15/10/16	^
a248.e.akamai.net	sn141w.snt141.mail	Permanente	31/08/12	
Digisign Server ID (Enrich)	*	Permanente	17/07/12	
Mancomunidad Sierra de CĂidiz				
servidor.mmsierradecadiz.lan	servidor.mmsierrad	Permanente	06/02/14	
The USERTRUST Network				
addons.mozilla.org	*	Permanente	15/03/14	=
global trustee	*	Permanente	15/03/14	
kuix.de	*	Permanente	17/04/11	
login.live.com	*	Permanente	15/03/14	
login.skype.com	*	Permanente	15/03/14	
		-		

e incluso, podemos llegar a consultarlo para que muestre la información que contiene.

General Detalles	
No se pudo verificar e	ste certificado por razones desconocidas.
Emitido para Nombre común (CN) Organización (O) Unidad organizativa (OU) Número de serie	servidor.mmsierradecadiz.lan Mancomunidad Sierra de CĀidiz Servidor Web 01
Emitido por Nombre común (CN) Organización (O) Unidad organizativa (OU)	Antonio José Fortis MalagÃ ³ n Mancomunidad Sierra de CĀidiz Servicios InformĀiticos
Validez Emitido el Caduca el	06/02/13 06/02/14
Huellas digitales Huella digital SHA1 Huella digital MD5	24:7C:DB:FC:D2:D4:98:F9:BE:46:0B:E7:EF:62:15:60:4F:AB:7D:6C 18:7B:0E:71:D7:3C:B0:C3:1C:DB:F9:76:09:5B:65:CA
	<u>C</u> errar

3.4. Apache2 + Php5

Para expandir la funcionalidad del servidor web que estamos montando, necesito activar el soporte para php. Dicha activación requiero la instalación de una serie de paquetes y el reinicio del servidor, ejecutando para ello los siguientes comandos:

aptitude install php5 libapache2-mod-php5

para la instalación

/etc/init.d/apache2 restart

para el reinicio del servidor apache2

Para verificar la instalación del soporte **php**, vamos a crear una pequeña página web que muestre las características de la instalación **php**. Esta página se creará en */var/www/phpinfo.php* y su contenido será:

```
<?php
phpinfo();
?>
```

Desde el navegador del cliente, introduciremos <u>http://servidor.mmsierradecadiz.lan/php.info</u> y comprobaremos que se ha instalado correctamente, tal y como vemos en la siguiente captura.



3.5. Apache2 + Php5 + MySQL

Para completar la funcionalidad del servidor web, vamos a activar el soporte **MySQL** del php, instalando para ello los paquetes necesarios y reiniciando de nuevo el servidor.

aptitude install php5-mysql

para la instalación

/etc/init.d/apache2 restart

para el reinicio del servidor apache2

Para verificar la instalación del soporte **MySQL** del php, procederemos de la misma manera que en el caso anterior, es decir, cargaremos el mismo fichero (*phpinfo.php*) en el navegador web de un cliente, introduciendo la dirección <u>https://servidor.mmsierradecadiz.lan/phpinfo.php</u> (en este caso se ha utilizado la conexión segura) y veremos que la instalación ha sido correcta.

Archivo Editar Ver Historial Marcadores H	erramien <u>t</u> as Ay <u>u</u> da						
C phpinfo() +							
+ A https://servidor.mmsierradecadiz.lan/phpi	nfo.php			☆ ~ 😂	₿♥ Google	# 1	
📷 Más visitados 🗸 🛅 Guadalinex 🗸 🛅 Conocimio	ento Libre 🗸 🛅 Software Libre	✓ ■ Redes So	ciales 🗸 🛅 Perio	odicos 🗸 🛅 Televisión 🗸			
	_	m	ysqi				^
	MuCOL Current			emobiled			
	Active Dessistant Links		0	enabled			
	Active Fersistent Links		0				
	Active Links 0						
			oxtornal				
	MYSOL SOCKET		/var/run/mysold/n	avsald sock			
	MYSOL INCLUDE		-l/usr/include/mys	al			
	11002_100		c/usi/iib iiiiysqie				
	Directive	Loca	l Value	Master Value			
	mysql.allow_local_infile On			On			
	mysql.allow_persistent On			On			
	mysql.connect_timeout 60			60			\equiv
	mysql.default_host no value			no value			
	mysql.default_password no value			no value			
	mysql.default_port	no value		no value			
	mysql.default_socket	/var/run/mysql	d/mysqld.sock	/var/run/mysqld/mysqld.sock			
	mysql.default_user	no value		no value			
	mysql.max_links	Unlimited		Unlimited			
	mysql.max_persistent	Unlimited		Unlimited			
	mysql.trace_mode	Off		Off			
			veali				
			y3411				
	Mysqli Suppo	rt		enabled			
	Client API library version		5.1.66				~
				· · · · · ·			_

3.6. Servicio FTP

Como servicio de transferencia de ficheros vamos a utilizar la aplicación **SFTP** (también conocida como **SSH File Transfer Protocol**).

Aunque se trata de un protocolo del nivel de aplicación que proporciona la funcionalidad necesaria para la transferencia y manipulación de ficheros sobre un flujo de datos, es completamente diferente al protocolo FTP (Files Transfer Protocol). SFTP fué construido desde cero y añade la características FTP a SSH, ya que se utiliza conjuntamente con él para proporcionar la seguridad a los datos. Por lo tanto, la seguridad no la provee directamente el protocolo SFTP, sino SSH.

Algunas de las características que podemos destacar de dicho protocolo son:

- SFTP es más seguro que FTP.
- Si dispones de SSH en tu sistema por defecto ya puedes utilizar SFTP, no se necesita configuración adicional de servicios ni otro puerto .
- La transmisión de datos siempre segura encapsulando la conexión mediante SSH .
- El protocolo incluye operaciones para permisos, manipulación de atributos, bloqueo de ficheros y mucho más.
- Se puede utilizar tanto a nivel de línea de comandos como mediante clientes gráficos .
- La mayor parte de los clientes de FTP modernos soportan el protocolo SFTP.

Para la instalación y configuración del servicio, indicar que una vez que tenemos el paquete **openssh-server** (el cual fue añadido durante el proceso de instalación del sistema operativo), dicho servicio ya se encuentra operativo, por lo tanto, lo único que vamos a realizar a continuación, es mostrar una captura donde podemos observar su funcionamiento una vez que ha sido configurado en un cliente FTP, como es el caso de **FileZilla**.

<u>A</u> rchivo <u>E</u> ditar <u>V</u> er	<u>I</u> ransferencia <u>S</u> ervidor <u>M</u> ar	cadores A <u>y</u> uda						
1 1 🛛 🖀 📬 🗱	s 🐰 🏳 🙀 🛷 l 📰 👧 🚰 🚜							
Servidor: sftp://servido	or.m Nombre de <u>u</u> suario: afo	rtis Contra <u>s</u> eña:	Puerto:	Conexión rápida	·			
Estado: Directorio ils Estado: Conectando Respuesta: fzSftp starte Comando: open "afortis Comando: Confiar en ni Comando: Pass: ****** Estado: Connected ti Estado: Connected ti Estado: cd "home/al Respuesta: New director Comando: get "prueba. Estado: Transferenci	AGDO CORRECTAMENTE a servidor.mmsierradecadiz.l. d S@servidor.mmsierradecadiz.l pervidor.mmsierradecadiz.l p servidor.mmsierradecadiz.l. b a descarga de /home/afortis ortis" y is: "/home/afortis/ pueba.txt => local: a de archivo correcta	an an" 22 in //prueba.txt " /home/afortis/prueba.txt						
Sitio local: /home/afort	is/		~	Sitio remoto: /home/afo	rtis			-
✓ ■ afortis ▷ .VirtualBo)X			マ ♀ home Jafortis				
Nombre de archiv Tama	no de Tipo de archivi Ultima	modificaci		Nombre de archivo 🔿	Tamaño de Tipo de a	rcl Ultima modific Permisos	Propietario/	
VirtualBox	Directorio 11/02/1	3 19:48:	<u> </u>	 .bash_history 	731 B Archivo	05/02/13 20:rw	afortis af	
j .aMule	Directorio 19/07/1	0 19:03:		.bash_logout	220 B Archivo	28/08/12 23:rw-rr	afortis af	
adobe 📃	Directorio 11/08/1	0 02:32:		.bashrc	4 KB Archivo	28/08/12 23:rw-rr	afortis af	
📁 .amsn	Directorio 20/07/1	0 02:00:		profile	675 B Archivo	28/08/12 23:rw-rr	afortis af	
.audacity-d	Directorio 07/12/1	1 22:16:		prueba.txt	19 B Plain tex	. 02/02/13 18:rw-rr	root root	
.cache	Directorio 11/02/1	3 19:23:	~					_
45 archivos y 69 directo	prios. Tamaño total: 29 MB			1 archivo seleccionado. 1	famaño total: 19 B			
Servidor/Archivo local	Direcció Archivo remoto	Tamaño Priorida: Es	tado					
Archivos en cola	Transferencias fallidas	Transferencias satisfactorias (2)						
						🔒 Cola: va	ecía 🔹 🖲	

3.7. Servicio WebDAV

El protocolo **WebDAV** (Web-based Distributed Authoring and Versioning) es una extensión del protocolo HTTP que soporta escritura y permite modificar archivos en un servidor web. Esto hace posible no sólo la creación y actualización de contenidos de sitios web de una forma fácil, sino el uso de otras aplicaciones, como la creación de calendarios compartidos, la centralización de los marcadores de Firefox o incluso el acceso a los documentos alojados en el servidor desde un explorador de archivos, con la función de "carpetas compartidas".

Para su instalación debemos de indicar que ya se realizó al instalar el servidor Apache2, ya que con él fueron añadidos los módulos necesarios. Seguidamente, para el proceso de configuración, vamos a realizar los siguientes pasos:

1. Crear el directorio donde se almacenará el contenido, estando dicho directorio en el sistema de ficheros del servidor, y utilizando para ello el comando **mkdir -p /var/www/webdav**.

2. Una vez creado, permitimos que apache sea el propietario de dicho directorio y le asignamos permisos de escritura para el grupo, ejecutando para ello los siguientes comandos chown www-data /var/www/webdav y chmod g+w /var/www/webdav respectivamente.

afortis@servidor: ~	●
<u>Archivo Editar Ver Terminal Ayu</u> da	
root@servidor:~# mkdir -p /var/www/webdav root@servidor:~# chown www-data /var/www/webdav/ root@servidor:~# chmod g+w /var/www/webdav/ root@servidor:~# []	

3. El siguiente paso será añadir la localización de **WebDAV** a la configuración de **Apache2**, además de limitar el acceso a **WebDAV** sólo a los usuarios autorizados. Para ello, vamos a definir en el servidor web una localización protegida (webdav), creando o editando el fichero */etc/apache2/conf.d/webdav* con la siguiente información:

Alias /webdav /var/www/webdav

```
<Location /webdav>
DAV On
AuthType Digest
AuthName "webdav"
AuthUserFile /etc/apache2/webdav.passwd
Require valid-user
</Location>
```

4. Posteriormente, deberemos de activar el módulo **dav_fs** y el de autenticación **auth_digest**, ejecutando para ello los comandos que se muestran a continuación:

afortis@servidor: ~	• • •
<u>Archivo E</u> ditar <u>V</u> er <u>T</u> erminal Ayuda	
<pre>root@servidor:~# a2enmod dav_fs Considering dependency dav for dav_fs: Enabling module dav. Enabling module dav_fs. Run '/etc/init.d/apache2 restart' to activate new configuration! root@servidor:~# a2enmod auth_digest Enabling module auth_digest. Run '/etc/init.d/apache2 restart' to activate new configuration! root@servidor:~#</pre>	

5. Además, debe de crearse el fichero de autorizaciones para el recurso webdav con los usuarios que se han definido y sus respectivas contraseñas. Para la generación de la contraseña, utilizamos el comando htdigest -c /etc/apache2/webdav.passwd webdav afortis , siendo webdav el directorio donde se almacena la información de WebDav y afortis el nombre del usuario creado. Una vez ejecutado dicho comando, se nos pedirá una contraseña por dos veces que se que guardará en el fichero webdav.passwd de forma encriptada.

6. Por último, debemos de recargar el fichero de configuración de Apache con el comando /etc/init.d/apache2 reload para que lea la nueva configuración, y ya nos podemos conectar desde un cliente a <u>http://servidor.mmsierradecadiz.lan/webdav</u> previa autenticación, tal y como podemos ver en la imagen.

ا	4.3.1 Servi	dor WebDAV [Servi Mozilla Firefox bian Server] - Mozilla Firefox		. 6 .
Archivo Editar Ver Historial Marc	adores Herramien <u>t</u> as	Ayuda		
Conectando	4			
servidor.mmsierradecadiz.lan/v	vebdav	~ 3	8 G00	gle 🙀 🐴
🛅 Más visitados 🗸 🛅 Guadalinex 🛩 🛅	Conocimiento Libre 🗸 🛛	🖥 Software Libre 🗸 🛅 Redes Sociales 🗸 🋅 Periodicos 🗸 🛅 Televisión 🗸		
It works!				
This is the default web page for	this server.			
The web server software is run	ning but no content	has been added, yet.		
	۷	Identificación requerida	€ ⊗	
		http://servidor.mmsierradecadiz.lan está solicitando un nombre de usuario y una contraseña. El sitio dice: "webdav"		
	Nombre de usuario:			
	Contraseña:			
		Cancelar	eptar	

Y una vez autenticados, accedemos al contenido de dicho directorio, en este caso un fichero de prueba.



4. Instalación y configuración del Servicio de Correo

El servicio de correo electrónico que hemos instalado, se compone de un **Servicio SMTP** (Postfix), se trata de un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos. Un **Servicio IMAP** (Dovecot), es un protocolo de aplicación de acceso a mensajes electrónicos almacenados en un servidor. Por último, un **Servicio WebMail** (Roundcube) que nos permita consultar nuestros correos electrónicos de manera fácil, práctica y accesible desde cualquier lugar.

4.1. Servicio SMTP (Simple Mail Transfer Protocol)

Como aplicación para este servicio hemos utilizado **Postfix** y el proceso de instalación y configuración ha sido el siguiente:

1. Instalamos los paquetes necesarios mediante el siguiente comando:

aptitude install postfix postfix-tls sasl2-bin

Una vez iniciado el proceso de instalación, nos aparecerá una pantalla indicando que especifiquemos el tipo de configuración para el servidor, tal y como podemos ver en la imagen:

<u>M</u> áquina <u>V</u> er <u>D</u> ispositivos Ay <u>u</u> da
Configuración de paquetes
Postfix Configuration
Escoja el tipo de configuración del servidor de correo que se ajusta mejor a sus necesidades.
Sin configuración: Se debe elegir para mantener la configuración actual intacta. Sitio de Internet:
El correo se envía y recibe directamente utilizando SMTP. Internet con «smarthost»: El correo se recibe directamente utilizando SMTP o ejecutando una herramienta como fectchmail. El correo de salida se envía utilizando
Sólo correo local: El único correo que se entrega es para los usuarios locales. No hay red.
KAceptar>
S 🖓 🖓 🖓 🗐 🚺 🖉 Ctrl Derecho

Como la configuración la vamos a realizar manualmente sobre diferentes ficheros, elegimos la opción **Sin Configuración**, procediendo posteriormente a la edición y modificación de los ficheros necesarios.

<u>M</u> áquina <u>V</u> er <u>D</u> ispositivos Ayuda
Configuración de paquetes
Postfix Configuration Tipo genérico de configuración de correo: Sin configuración Sitio de Internet Internet con «smarthost» Sistema satélite Sólo correo local
<aceptar> <cancelar></cancelar></aceptar>
😂 😳 🧷 🖶 🖸 Ctrl Derecho

2. El primer fichero que vamos a modificar es el fichero **main.cf**, el cual vamos a obtenerlo de /usr/lib/postfix/main.cf y copiarlo en /etc/postfix/main.cf. Una vez realizada la copia, procedemos a editarlo y configurarlo, realizando sobre él las siguientes modificaciones.

```
# línea 59: descomentar
mail owner = postfix
# línea 76: descomentar y especificar el nombre del servidor
myhostname = servidor.mmsierradecadiz.lan
# línea 83: descomentar y especificar el dominio del servidor
mydomain = mmsierradecadiz.lan
# línea 104: descomentar
myorigin = $mydomain
# línea 118: descomentar
inet interfaces = all
# línea 166: descomentar
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
# línea 209: descomentar
local recipient maps = unix:passwd.byname $alias maps
# línea 268: descomentar y especificar la red
mynetworks = 127.0.0/8, 192.168.0.0/24
# línea 388: descomentar
alias maps = hash:/etc/aliases
# línea 399: descomentar
alias_database = hash:/etc/aliases
# línea 421: descomentar ( usar Maildir )
home mailbox = Maildir/
# línea 526: descomentar
header checks = regexp:/etc/postfix/header checks
# añadir: chequea el cuerpo del mensaje
body checks = regexp:/etc/postfix/body checks
# línea 552: comentar la primera línea y añadir la que aparece a
continuación
# smtpd banner = $myhostname ESMTP $mail name (@@DISTRO@@)
smtpd banner = $myhostname ESMTP
# línea 626: añadir
sendmail path = /usr/sbin/postfix
# línea 631: añadir
newaliases_path = /usr/bin/newaliases
# línea 636: añadir
mailq path = /usr/bin/mailq
```

```
# línea 642: añadir
setgid group = postdrop
# línea 646: comentar
# html directory =
# línea 650: comentar
# manpage_directory =
# línea 655: comentar
# sample directory =
# línea 659: comentar
# readme directory =
# añadir al final de fichero para limitar el tamaño de los correos a 10
MBvtes
message size limit = 10485760
# añadir a continuación para limitar el tamaño del buzón a 1 GByte
mailbox_size_limit = 1073741824
# añadir para autenticación SMTP-Auth
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth-client
smtpd_sasl_auth_enable = yes
smtpd sasl security options = noanonymous
smtpd sasl local domain = $myhostname
smtpd client restrictions = permit mynetworks,reject unknown client,permit
smtpd recipient restrictions =
permit mynetworks, permit auth destination, permit sasl authenticated, reject
```

3. El segundo fichero a modificar es el fichero **header_checks**, el cual vamos a editar desde su ubicación actual que es **/etc/postfix/header_checks**, añadiendo sobre él lo siguiente:

```
# rechaza las direcciones de correo que no están especificadas ( vacías )
/^From:.*<#.*@.*>/ REJECT
/^Return-Path:.*<#.*@.*>/ REJECT
```

4. El tercer fichero a modificar es el fichero **body_checks**, el cual vamos a editar desde su ubicación actual que es **/etc/postfix/body_checks**, añadiendo sobre él lo siguiente:

```
# rechaza los mensajes que incluyen la dirección especificada en el cuerpo
# del mensaje
/^(|[^>].*)example.com/ REJECT
```

5. Por último, actualizamos el fichero /etc/aliases de la base de datos con el comando:

newaliases

y reiniciamos el servicio para habilitar los cambios realizados en los ficheros de configuración, ejecutando para ello el siguiente comando.

/etc/init.d/postfix restart

4.2. Servicio IMAP (Internet Message Access Protocol)

Como aplicación para este servicio hemos utilizado **Dovecot** y el proceso de instalación y configuración ha sido el siguiente:

1. Instalamos los paquetes necesarios mediante el siguiente comando:

aptitude install dovecot-common dovecot-imapd

2. A continuación, editamos el fichero de configuración **dovecot.conf** que se encuentra en la ubicación **/etc/dovecot/dovecot.conf** y realizamos sobre él las siguientes modificaciones:

```
# línea 53: descomentar and cambiar ( autenticación con texto plano )
disable plaintext auth = no
# línea 95: descomentar and cambiar ( permite uso de certificados )
ssl = yes
# línea 230: descomentar y añadir
mail location = maildir:~/Maildir
# línea 893: añadir
mechanisms = plain login
# línea 1120: cambiar como viene a continuación
socket listen {
   #master {
         # Master socket provides access to userdb information. It's
typically
      # used to give Dovecot's local delivery agent access to userdb so it
      # can find mailbox locations.
      #path = /var/run/dovecot/auth-master
      #mode = 0600
      # Default user/group is the one who started dovecot-auth (root)
      #user =
      #group =
    #}
    client {
      # The client socket is generally safe to export to everyone. Typical
     # use is to export it to your SMTP server so it can do SMTP AUTH
     # lookups using it.
      #path = /var/run/dovecot/auth-client
      path = /var/spool/postfix/private/auth-client
      mode = 0660
      user = postfix
      group = postfix
      #mode = 0660
   }
 }
}
```

3. Por último, reiniciamos el servicio para habilitar los cambios realizados en el fichero de configuración, ejecutando para ello el siguiente comando.

/etc/init.d/dovecot restart

4.3. Configurar Postfix y Dovecot para SSL

Después de haber configurado los servicios de SMTP e IMAP, vamos a añadirle la opción de usar los **certificados SSL** que habíamos generado anteriormente, añadiendo con ello otro nivel más de seguridad.

Los pasos que hemos seguido para su instalación y configuración han sido:

1. Editamos el fichero /etc/postfix/main.cf, añadiendo la siguiente información:

```
# añadir al final del fichero para configurar Postfix para SSL
smtpd_use_tls = yes
smtpd_tls_cert_file = /etc/ssl/certs/servidorMMSC.crt
smtpd_tls_key_file = /etc/ssl/private/servidorMMSC.key
smtpd tls session cache database = btree:${data directory}/smtpd scache
```

2. Además, también debemos de editar el fichero **/etc/postfix/master.cf** y realizar en él la siguiente modificación:

```
# líneas 17, 18: descomentar
smtps inet n - - - - smtpd
-o smtpd_tls_wrappermode=yes
```

3. También será necesario editar el fichero **/etc/dovecot/dovecot.conf** y realizar en él las siguientes modificaciones:

```
# línea 95: descomentar
ssl = yes
# líneas 100, 101: descomentar y especificar certificado
ssl_cert_file = /etc/ssl/certs/servidorMMSC.crt
ssl_key_file = /etc/ssl/private/servidorMMSC.key
```

4. Por último, reiniciamos los servicios SMTP e IMAP, ejecutando para ellos los comandos:

/etc/init.d/postfix restart

/etc/init.d/dovecot restart

Una vez realizadas dichas configuraciones, podemos configurar un cliente de correo como **Thunderbird** y comprobar que el Servicio de Correo funciona correctamente.

<u>S</u> u nombre:	Antonio J	osé Fortis Malagón Su nombre	e, tal y co	mo se muestra	a los de	emás
Dirección de correo:	ortis@m	msierradecadiz.lan				
Contr <u>a</u> seña:						
	✓ <u>R</u> ecord	lar contraseña				
:	Se ha enco	ontrado la siguiente configuració	in sondea	ndo el servidor	suminis	strado
		Nombre del servidor	Puerto	SSL		Identificación
Entrante:	MAP 🗘	Nombre del servidor servidor.mmsierradecadiz.lai	Puerto 993 🗸	SSL SSL/TLS	٢	Identificación Contraseña normal
Entrante:	MAP ᅌ	Nombre del servidor servidor.mmsierradecadiz.lai servidor.mmsierradecadiz	Puerto 993 ~ 465 ~	SSL SSL/TLS SSL/TLS	•	Identificación Contraseña normal 🗘 Contraseña normal 🗘
Entrante: 🗍 Saliente: 🚦 Nombre de usuario:	MAP 🗘	Nombre del servidor servidor.mmsierradecadiz.laı servidor.mmsierradecadiz	Puerto 993 ~ 465 ~	SSL SSL/TLS SSL/TLS	•	Identificación Contraseña normal 🗘 Contraseña normal 🗘
Entrante: 1	MAP ᅌ	Nombre del servidor servidor.mmsierradecadiz.lai servidor.mmsierradecadiz	Puerto 993 ✓ 465 ✓	SSL SSL/TLS SSL/TLS	•	Identificación Contraseña normal 🔅 Contraseña normal 🔅

Una vez realizada la configuración, al acceder al cliente **Thunderbird**, nos pedirá que aceptemos nuestro certificado, tal y como podemos ver en la siguiente captura:

Está a punto de alterar cómo identifica Thunderbird es	te sitio.
Los bancos, tiendas y otros sitios públicos leg no le pedirán hacer esto.	ítimos
Servidor	
Dirección: servidor.mmsierradecadiz.lan:993	ertificado
Estado del certificado	
Este sitio intenta identificarse a sí mismo con información no válida.	<u>V</u> er
Identidad desconocida	
No se confía en el certificado porque no ha sido verificado p autoridad reconocida usando una firma segura.	or una
 Guardar esta excepción de manera permanente 	
Confirmar excepción de seguridad	Cancelar

Por último, junto al usuario <u>afortis@mmsierradecadiz.lan</u>, se ha creado otro usuario en el servidor, llamado <u>usuario@mmsierradecadiz.lan</u> y se ha comprobado el intercambio de correos electrónicos, tal y como podemos comprobar.



4.4. Servicio WebMail

El siguiente paso será configurar un servicio de WebMail, para el cual hemos elegido **RoundCube**, que nos va a permitir consultar nuestro correo electrónico de manera fácil, práctica, confortable y accesible, desde cualquier lugar.

Para su instalación y configuración hemos realizado lo siguiente:

1. Instalamos los paquetes necesarios, mediante el comando:

aptitude install roundcube roundcube-mysql

2. Nos indica si queremos configurar la base de datos que tenemos instalada para roundcube, a lo que respondemos que Sí

<u>M</u> áquina <u>V</u> er <u>D</u> ispositivos Ay <u>u</u> da
Configuración de paquetes
Configuracion de roundcube-core
Es necesario tener una base de datos instalada y configurada para roundcube antes de poder utilizarlo. Puede gestionar esto opcionalmente a través «dbconfig-common».
Si vd. es un administrador de bases de datos avanzado o si la base de datos ya está instalada y configurada quizás quiera realizar esta configuración manualmente, y debería rechazar esta opción. Probablemente podrá encontrar los detalles de las operaciones que debe realizar en «/usr/share/doc/roundcube».
Debería escoger esta opción en cualquier otro caso.
¿Desea configurar la base de datos para roundcube con «dbconfig-common»?
KSÍ> (No>

3. A continuación, nos pide que seleccionemos la base de datos que vamos a utilizar, siendo en nuestro caso mysql, tal y como podemos ver.

<u>M</u> áquina <u>V</u> er <u>D</u> ispositivos Ay <u>u</u> da
Configuración de paquetes
Se puede configurar roundcube para utilizar una base de datos que puede ser de distintos tipo. A continuación se le mostrarán las opciones disponibles.
El tipo de base de datos que se va a utilizar para roundcube:
<mark>mysql</mark> pgsql sqlite
<mark>⟨Aceptar></mark> ⟨Cancelar>
😂 😳 🖉 🖶 🔕 Ctrl Derecho

4. El siguiente paso será especificar la clave de root de MySQL para poder crear la base de datos y el usuario, según podemos ver en la siguiente captura.

<u>M</u> ác	quina	<u>V</u> er	<u>D</u> ispositivos	Ay <u>u</u> da
Cont	figur	ració	ón de paque	tes
	Pro pao	oporo quete	cione la co e utilizará	│ Configuración de roundcube-core │ ntraseña para la cuenta de administración que este para crear la base de datos MySQL y el usuario.
	Cor	ntras	seña del us	uario de administración de la base de datos:
	жж	кжжж	*******	
				< <u>Aceptar></u> <cancelar></cancelar>
				😂 🕑 🖉 🖶 🔟 🚺 Karl Derecho

5. Y por último, asignar una contraseña a la base de datos que se ha creado.

Má	áquina <u>V</u> er <u>D</u> ispositivos Ay <u>u</u> da
Cor	nfiguración de paquetes
	Configuración de roundcube-core Proporcione una contraseña para que roundcube se registre con el servidor de base de datos. Si deja este campo en blanco se generará un contraseña aleatoria.
	Contraseña de aplicación MySQL para roundcube:

	<aceptar> <cancelar></cancelar></aceptar>
	😂 😳 🖉 🖶 🌘 Ctrl Derecho

Una vez instalada la aplicación, debemos de realizar las configuraciones necesarias para ajustar la aplicación a nuestro servidor de correo, para lo cual, tenemos que editar el fichero **/etc/roundcube/main.inc.php** y realizar sobre él las siguientes modificaciones:

```
# línea 66: especifica el servidor IMAP con soporte para SSL
$rcmail_config['default_host'] = 'ssl://servidor.mmsierradecadiz.lan';
# línea 69: especifica el puerto IMAP para el soporte SSL
$rcmail_config['default_port'] = 993;
# línea 87: indica el nombre de dominio
$rcmail_config['mail_domain'] = 'mmsierradecadiz.lan';
```

```
# línea 102: especifica el servidor SMTP con soporte para SSL
$rcmail config['smtp server'] = 'ssl://servidor.mmsierradecadiz.lan';
# línea 105: especifica el puerto SMTP para el soporte SSL
$rcmail config['smtp port'] = 465;
# línea 109: RoundCube usa como usuario SMTP el utilizado en el login
$rcmail_config['smtp_user'] = '%u';
# línea 113: RoundCube usa como password SMTP el utilizado en el login
$rcmail_config['smtp_pass'] = '%p';
# línea 123: establece SMTP HELO host con el nombre de nuestro servidor
$rcmail config['smtp helo host'] = 'servidor.mmsierradecadiz.lan';
# línea 168: establece el lenguaje a español
$rcmail config['language'] = 'es ES';
# línea 180: asigna a UserAgent el mensaje de cabecera en los envíos
$rcmail config['useragent'] = 'RoundCube Webmail/'.RCMAIL VERSION;
# línea 183: indica el título que tendrá la página web de RoundCube
$rcmail_config['product_name'] = 'Servidor Mancomunidad Sierra de Cadiz';
# línea 218: indica la codificación de caracteres por defecto
$rcmail_config['default_charset'] = 'UTF-8';
```

El siguiente fichero a modificar, es **/etc/roundcube/apache.conf**, en el cual sólo vamos a realizar una modificación.

línea 4: descomentarla
Alias /roundcube /var/lib/roundcube

Para que los cambios en los ficheros surtan efecto, habrá que reiniciar el servidor Apache, utilizando para ello el comando que se especifica a continuación.

/etc/init.d/apache2 restart

Una vez reiniciado es servidor Apache, podemos comprobar el funcionamiento del servicio, introduciendo la dirección <u>http://servidor.mmsierradecadiz.lan/roundcube</u>.

			PA 41
https://servidor.mmsierradecadiz.lan/roundcub	e/?_task=logout	ିଙ୍ୟ 🖏 🔣 ସେତ୍ତୋବ	£8 🖆
🛅 Más visitados 🗸 🛅 Guadalinex 🗸 🛅 Conocimiento I	.ibre 🗸 🛅 Software Libre 🔪 🛅 Redes Sociales 🗸 🛅 Periodicos 🗸	Televisión~	
Free webmail for the masses			
	Bienvenido a Servidor Mancomunidad Sierra de Cadiz		
	Nombre de usuario afortis		
	Contraseña •••••••		
	Entrar		

Y una vez que nos hemos identificado, se puede comprobar como se accede a nuestro correo electrónico a través de WebMail.



4.5. Filtros de correo (anti-virus, anti-spam)

Para terminar con el servicio de correo electrónico, vamos a instalar y configurar una serie de filtros que van a añadir seguridad al servicio. Este sistema de filtros va a permitir implementar soluciones anti-virus y anti-spam, tal y como vamos a describir en los siguientes pasos:

1. Instalación de los paquetes necesarios ejecutando el siguiente comando.

aptitude install clamav-daemon amavisd-new spamassassin

2. Editar el fichero /etc/default/spamassassin y realizar sobre él la siguiente modificación.

```
# línea 8: establecer a "1" para habilitar filtro anti-spam
ENABLED=1
```

3. Editar el fichero /etc/amavis/amavisd.conf y realizar sobre él las siguientes modificaciones.

```
# línea 66: descomentar
$MYHOME = '/var/lib/amavis';
# línea 71: especificar nombre de dominio
$mydomain = 'mmsierradecadiz.lan';
# línea 73: descomentar y especificar nombre del servidor
$myhostname = 'servidor.mmsierradecadiz.lan';
# línea 77,78: cambiar
$daemon_user = 'amavis';
$daemon_group = 'amavis';
# línea 626: comentar ( no notifica si un virus es detectado )
#$virus_admin = "virusalert\@$mydomain";
```

```
# linea 1934: descomentar y añadir
['ClamAV-clamd',
    \&ask_daemon, ["CONTSCAN {}\n", "/var/run/clamav/clamd.ctl"],
    qr/\bOK$/m, qr/\bFOUND$/m,
    qr/^.*?: (?!Infected Archive)(.*) FOUND$/m ],
```

4. Editar el fichero /etc/amavis/conf.d/15-content_filter_mode y realizar sobre él las siguientes modificaciones.

5. Editar el fichero /etc/postfix/main.cf y añadir al final la siguiente línea.

```
# Configurar amavis en Postfix
content_filter=smtp-amavis:[127.0.0.1]:10024
```

6. Editar el fichero /etc/postfix/master.cf y añadir al final las siguientes líneas.

```
# Configurar amavis en Postfix
smtp-amavis unix -
                                        -
                                               2 smtp
                                  n
      -o smtp data done timeout=1200
      -o smtp_send_xforward_command=yes
      -o disable dns lookups=yes
127.0.0.1:10025 inet n
                           -
                                 n
                                              - smtpd
                                    -
      -o content filter=
      -o local recipient maps=
      -o relay recipient maps=
      -o smtpd restriction classes=
      -o smtpd client restrictions=
      -o smtpd helo restrictions=
      -o smtpd sender restrictions=
      -o smtpd recipient restrictions=permit mynetworks, reject
      -o mynetworks=127.0.0.0/8
      -o strict rfc821 envelopes=yes
      -o smtpd_error_sleep_time=0
      -o smtpd soft error limit=1001
  -o smtpd hard error limit=1000
Para finalizar, ejecutamos los comandos que se muestran a continuación:
touch /etc/mailname
```

```
chmod -R 775 /var/lib/amavis/tmp
```

usermod -G amavis clamav

Y reiniciamos los servicios que se han visto implicados para recargar las nuevas configuraciones que se han establecido.

/etc/init.d/clamav-daemon restart /etc/init.d/spamassassin start /etc/init.d/postfix restart /etc/init.d/amavis restart

En la siguientes captura podemos ver como quedarían tras su ejecución en el servidor.

```
root@servidor:~# touch /etc/mailname
root@servidor:~# touch /etc/mailname
root@servidor:~# chmod -R 775 /var/lib/amavis/tmp
root@servidor:~# usermod -G amavis clamav
root@servidor:~# /etc/init.d/clamav-daemon restart
Stopping ClamAV daemon: clamd.
Starting ClamAV daemon: clamd .
root@servidor:~# /etc/init.d/spamassassin start
Starting SpamAssassin Mail Filter Daemon: spamd.
root@servidor:~# /etc/init.d/postfix restart
Stopping Postfix Mail Transport Agent: postfix.
Starting Postfix Mail Transport Agent: postfix.
Starting Postfix Mail Transport Agent: postfix.
root@servidor:~# /etc/init.d/amavis restart
Stopping amavisd: amavisd-new.
Starting amavisd: amavisd-new.
root@servidor:~#
```

Junto con el resultado del análisis de un correo electrónico que se ha enviado, donde se puede comprobar que ha sido analizado con dichas herramientas para comprobar la existencia de algún tipo de malware.

```
Archivo Editar Ver Ayuda
     Return-Path: <usuario@mmsierradecadiz.lan>
     X-Original-To: afortis@mmsierradecadiz.lan
     Delivered-To: afortis@mmsierradecadiz.lan
     Received: from localhost (localhost [127.0.0.1])
         by servidor.mmsierradecadiz.lan (Postfix) with ESMTP id 0280D6E33A
         for <afortis@mmsierradecadiz.lan>; Tue, 19 Feb 2013 01:14:49 +0100 (CET)
     X-Virus-Scanned: Debian amavisd-new at mmsierradecadiz.lan
     Received: from servidor.mmsierradecadiz.lan ([127.0.0.1])
         by localhost (servidor.mmsierradecadiz.lan [127.0.0.1]) (amavisd-new, port 10024)
         with ESMTP id KZcamUMbJiqP for <afortis@mmsierradecadiz.lan>;
         Tue, 19 Feb 2013 01:14:45 +0100 (CET)
     Received: from [192.168.0.100] (unknown [192.168.0.100])
         by servidor.mmsierradecadiz.lan (Postfix) with ESMTPSA id 70CC56E337
         for <afortis@mmsierradecadiz.lan>; Tue, 19 Feb 2013 01:14:45 +0100 (CET)
     Message-ID: <5122C3F6.7000402@mmsierradecadiz.lan>
     Date: Tue, 19 Feb 2013 01:14:46 +0100
     From: usuario <usuario@mmsierradecadiz.lan>
     User-Agent: Mozilla/5.0 (X11; Linux i686; rv:17.0) Gecko/20130107 Thunderbird/17.0.2
     MIME-Version: 1.0
     To: afortis@mmsierradecadiz.lan
     Subject: =?ISO-8859-1?Q?Env=EDo_de_un_correo_analizado_con_lo?=
      =?IS0-8859-1?Q?s_filtros=2E?=
     Content-Type: text/plain; charset=ISO-8859-1; format=flowed
     Content-Transfer-Encoding: 8bit
     Vamos a enviar un correo desde el usuario "usuario" al usuario "afortis"
     verificando que se han instalado los filtros Anti-Virus y Anti-Spam en
     el Servidor de Correo.
     Para ello, se visualizarán las propiedades del correo enviado y se podrá
     comprobar que ha sido analizado mendiante dichos filtros.
```

5. Servicios de Seguridad

Dentro de los Servicios de Seguridad que vamos a instalar y configurar en nuestro servidor, se encuentran los siguientes:

- Herramienta para la prevención de Ataques por Fuerza Bruta (Fail2Ban).
- Herramienta para la Detección de Rootkits (Rootkit Hunter).
- Herramienta para Auditoría de Seguridad (Debsecan).

5.1. Ataques por Fuerza Bruta (Fail2Ban)

Fail2Ban es una aplicación que analiza continuamente los ficheros log y bloquea las direcciones Internet, de donde se hayan originado varias tentativas fallidas de acceso con contraseña inválida. Además, es extremadamente eficaz en la prevención de ataques de fuerza bruta y ataques de negación de servicio (DoS).

El procedimiento que he seguido para su instalación y configuración, ha sido el siguiente:

1. Instalación de los paquetes necesarios mediante el comando:

aptitude install fail2ban whois

2. Para realizar las configuraciones necesarias, se aconseja trabajar sobre una copia local del fichero /etc/fail2ban/jail.conf, para lo cual, copiamos dicho fichero con el nombre /etc/fail2ban/jail.local y sobre él realizaremos las siguientes modificaciones.

cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

3. Definimos cuales serán las direcciones IP que no estarán sujetas a las restricciones y especificamos por cuanto tiempo estarán bloqueadas las direcciones de donde provengan las amenazas (600 seg), junto con el número de tentativas permitidas (3 tentativas).

```
ignoreip = 127.0.0.1 192.168.0.0/24
bantime = 600
maxretry = 3
```

4. Indicamos la dirección de correo electrónico que recibirá las alertas.

destemail = afortis@mmsierradecadiz.lan

5. Configuramos las acciones a realizar cuando se detecte un posible ataque. En este caso, la dirección IP del atacante es bloqueada y se envía un correo electrónico al administrador del sistema.

```
# ACTIONS
#
# Default banning action (e.g. iptables, iptables-new,
# iptables-multiport, shorewall, etc) It is used to define
# action_* variables. Can be overriden globally or per
# section within jail.local file
banaction = iptables-multiport
```

```
# email action. Since 0.8.1 upstream fail2ban uses sendmail
# MTA for the mailing. Change mta configuration parameter to mail
# if you want to revert to conventional 'mail'.
mta = postfix
# Default protocol
protocol = tcp
# Action shortcuts. To be used to define action parameter
# The simplest action to take: ban only
action = %(banaction)s[name=%( name )s, port="%(port)s", protocol="%
(protocol)s]
# ban & send an e-mail with whois report to the destemail.
action_mw = %(banaction)s[name=%(__name__)s, port="%(port)s", protocol="%
(protocol)s]
             %(mta)s-whois[name=%( name )s, dest="%(destemail)s",
protocol="%(protocol)s]
# ban & send an e-mail with whois report and relevant log lines
# to the destemail.
action mwl = %(banaction)s[name=%( name )s, port="%(port)s", protocol="%
(protocol)s]
              %(mta)s-whois-lines[name=%(__name__)s, dest="%
(destemail)s", logpath=%(logpath)s]
#Choose default action. To change, just override value of 'action' with
#the interpolation to the chosen action shortcut (e.g.
                                                               action mw,
#action mwl, etc) in jail.local globally (section [DEFAULT]) or per
```

6. Se establecen los parámetros de los diferentes servicios que se desean proteger.

```
# JAILS
# [ ... ]
[ssh]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 6
# [ ... ]
```

#specific section
action = %(action)s

7. Y finalmente, reiniciamos el servicio con el comando que indicamos a continuación.

/etc/init.d/fail2ban restart

5.2. Detección de Rootkits (Rootkit Hunter)

Rootkit Hunter es un sistema de detección de rootkits que alerta por correo electrónico al administrador del sistema, en caso de que detecte alteraciones en el sistema que indiquen la presencia de un rootkit.

El procedimiento que he seguido para su instalación y configuración, ha sido el siguiente:

1. Instalación de los paquetes necesarios mediante el comando:

aptitude install rkhunter

- 2. La configuración predeterminada del paquete **rkhunter** que se encuentra en el fichero /etc/rkhunter.conf suele ser suficiente. Además, el archivo /etc/default/rkhunter define que las actualizaciones de la base de datos tengan una periodicidad semanal, la verificación de rootkits diaria y que los resultados sean enviados por correo electrónico al administrador del sistema.
- 3. Para poder ver su funcionamiento, adjuntamos una captura de pantalla donde se puede observar los resultados obtenidos tras realizar un análisis del sistema al ejecutar el comando **rkhunter –check**.

```
Archivo Editar Ver Terminal Ayuda
                                                                                   ~
[Press <ENTER> to continue]
Checking for rootkits...
 Performing check of known rootkit files and directories
    55808 Trojan - Variant A
                                                               [ Not found ]
   ADM Worm
                                                               [ Not found ]
   AjaKit Rootkit
                                                              [ Not found ]
   Adore Rootkit
                                                              [ Not found ]
                                                              [ Not found ]
   aPa Kit
   Apache Worm
                                                              [ Not found ]
                                                              [ Not found ]
   Ambient (ark) Rootkit
                                                              [ Not found ]
   Balaur Rootkit
                                                              [ Not found ]
    BeastKit Rootkit
    beX2 Rootkit
                                                               [ Not found ]
    BOBKit Rootkit
                                                               [ Not found ]
    cb Rootkit
                                                              [ Not found ]
    CiNIK Worm (Slapper.B variant)
                                                              [ Not found ]
   Danny-Boy's Abuse Kit
                                                               [ Not found ]
                                                               [ Not found ]
   Devil RootKit
   Dica-Kit Rootkit
                                                               [ Not found ]
   Dreams Rootkit
                                                              [ Not found ]
```

5.3. Auditoría de Seguridad (Debsecan)

Debsecan efectúa una evaluación de la seguridad del sistema y relata las vulnerabilidades conocidas y asociadas a los paquetes instalados en el sistema, notificando al administrador del sistema los resultados.

El procedimiento que he seguido para su instalación y configuración, ha sido el siguiente:

1. Instalación de los paquetes necesarios mediante el comando:

aptitude install debsecan

2. Debsecan puede configurarse para ser ejecutado diariamente a través de una tarea programada (cron). De esta forma, sus resultados se enviarán por correo electrónico al administrador del sistema. El comando que debemos de ejecutar es el siguiente.

debsecan-create-cron

3. Un ejemplo de utilización en el que se puede observar el envío de un correo electrónico al administrador del sistema, con los resultados del análisis de seguridad, lo podemos ver en la siguiente captura.



6. Instalación Plataforma de Formación (Moodle)

La plataforma de formación **Moodle**, es un Sistema de Gestión de Cursos de Código Abierto (Open Source Course Management System, CMS), conocido también como Sistema de Gestión del Aprendizaje (Learning Management System, LMS) cuyo objetivo es facilitar a los educadores una herramienta para crear sitios web dinámicos en línea para sus estudiantes. Para su instalación, es necesario un Servidor Web con soporte para PHP y MySQL, el cual ya lo tenemos disponible, por lo tanto, vamos a detallar los pasos que hemos seguido para su instalación:

1. Nos descargamos de su <u>página web</u> la última versión estable disponible, que en este caso era **moodle-2.4.1.tgz** y procedemos a descomprimirlo en el directorio /var/www, utilizando para ello el siguiente comando.

tar xzvf moodle-2.4.1.tgz -C /var/www

2. El siguiente paso, será crear el directorio **moodledata** y hacerlo accesible al Servidor Web, para ello, ejecutamos los siguientes comandos.

mkdir /var/moodledata

chown www-data /var/moodledata

chown www-data /var/www/moodle

3. A continuación, debemos de crear la base de datos que utilizará Moodle (moodle), para ello, como administrador de MySQL, ejecutamos los comandos que se muestran en la siguiente captura.

~

```
Archivo Editar Ver Terminal Ayuda
root@servidor:~# mysql -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 38
Server version: 5.1.66-0+squeezel (Debian)
Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> CREATE DATABASE moodle DEFAULT CHARACTER SET utf8 COLLATE utf8 unicode ci;
Query OK, 1 row affected (0.03 sec)
mysql> GRANT ALL PRIVILEGES ON moodle.* TO 'moodle'@'localhost' IDENTIFIED BY 'moodle';
Query OK, 0 rows affected (0.02 sec)
mysql> exit
Bye
root@servidor:~#
```

4. Una vez realizadas dichas operaciones, procedemos a reiniciar el Servidor Web para que todos los cambios realizados surtan efecto.

/etc/init.d/apache2 restart

Una vez finalizada la primera parte de la instalación, para finalizar el proceso, debemos de acceder desde un navegador a la dirección donde está ubicada la plataforma **Moodle** (<u>http://servidor.mmsierradecadiz.lan/moodle</u>) y continuar con los siguientes pasos.

5. En primer lugar, debemos de seleccionar el idioma en el que deseamos que se muestren las opciones de la plataforma, en nuestro caso, **Español-España (es_es)**.

Archivo Editar Ver Historial Ma	cadores Herramien <u>t</u> as Ay <u>u</u> da			
nstalación - Moodle 2.4.1 (Buil	ф			
ervidor.mmsierradecadiz.lar	/moodle/install.php	the state of the	Soogle	👘 🐴
🛅 Más visitados 🗸 🛅 Guadalinex 🗸	🖥 Conocimiento Libre 🗸 🛅 Software Libre 🗸 🛅 Redes Sociales 🗸 📳	🖥 Periodicos 🛩 🛅 Televisión 🛩		
Instalación				
Idioma				
	Seleccionar io	dioma		
	Por favor, seleccione un idioma para el proceso de instalac defecto del sitio, si bien puede cambiarse más adelante.	ión. Este idioma se usará también com	o idioma por	
	ldioma Español - España (es_es)	0		
	Siguie	ente »		
moodle				

6. El siguiente paso, será definir los directorios que vamos a utilizar, los cuales ya vienen definidos, pero que se pueden modificar.

	中			
Servidor.mmsierrad	ecadiz.lan/moodle/install.php	☆ ~ 0	8 v Google	# 1
Más visitados 🗸 🛅 Guad	lalinex 🗸 🛅 Conocimiento Libre 🗸 🛅 Software Libre 🗸 🛅 Redes Sociale	es 🗸 🛅 Periodicos 🗸 🛅 Televisión 🗸		
	 Dirección Web Dirección web completa para acceder a Moodle. I direcciones. Si su sitio tiene varias direcciones pi todas ellas, excepto en ésta. Si su sitio web es ac escriba aquí la dirección pública y configure su D utilizar la dirección pública. Directorio Moodle Ruta completa del directorio de instalación de Mo Directorio de Datos Usted necesita un espacio donde Moodle puede poder LEER y ESCRIBIR el usuario del servidor no debe poderse acceder a esta carpeta directarm no existe. 	No es posible acceder a Moodle utilizando n úblicas debe configurar redirecciones perma ccesible tanto desde una intranet como desd INS para que los usuarios de su intranet pue podle. guardar los archivos subidos. En este direct web (por lo general 'nobody', 'apache' o 'ww nente a través de la web. El instalador tratará	múltiples Inentes en le Internet, edan también orio debe w-data'), pero à de crearla si	
	Dirección Web http://sepuidor.mmslerradaradiz.la	n/moorlle		
	Directorio Meedlo (http://www.face.adl.			
	Directorio Moodie [/var/www/moodie			
	Directorio de Datos //var/moodledata			

7. Una vez definidos los directorios, se hacen las **comprobaciones en el Servidor Web** para ver si se cumplen todos los requisitos, siendo dicha comprobación satisfactoria en este caso.

nstalación		· 夺			
Servido	mmsierrade	cadiz.lan/moodle/admin/index.php?lang=es_es&agreelicense=1	్లా 🖉	<mark>8</mark> ∨ Google	<u>8</u> 9
1ás visitado:	s 🗸 🛅 Guada	linex 🕆 🛅 Conocimiento Libre 🗸 🛅 Software Libre 🗸 🋅 Redes Sociales 🗸 🋅 Periodicos 🗸 🛅	Televisión∽		
		Comprobaciones del servidor			
Nombre	Información	Informe			Estado
unicode		(i) debe estar instalado/activado			OK
database	mysql	() versión 5.1.33 es obligatoria y está ejecutando 5.1.66.0.1			OK
php		() versión 5.3.2 es obligatoria y está ejecutando 5.3.3.7.14			OK
pcreunicode		() debería estar instalado y activado para conseguir los mejores resultados			OK
hp_extension	iconv	() debe estar instalado/activado			OK
hp_extension	mbstring	() debería estar instalado y activado para conseguir los mejores resultados			OK
hp_extension	curl	() debe estar instalado/activado			OK
hp_extension	openssl	🕕 debería estar instalado y activado para conseguir los mejores resultados			OK
hp_extension	tokenizer	() debería estar instalado y activado para conseguir los mejores resultados			<mark>ok</mark>
hp_extension	xmlrpc	() debería estar instalado y activado para conseguir los mejores resultados			OK
hp_extension	soap	(i) debería estar instalado y activado para conseguir los mejores resultados			OK
hp_extension	ctype	(i) debe estar instalado/activado			OK
hp_extension	zip	(i) debe estar instalado/activado			OK
hp_extension	gd	(i) debería estar instalado y activado para conseguir los mejores resultados			OK
hp_extension	simplexml	(i) debe estar instalado/activado			OK
hp_extension	spl	(i) debe estar instalado/activado			OK
hp_extension	pcre	(i) debe estar instalado/activado			OK
hp_extension	dom	(i) debe estar instalado/activado			OK
hp_extension	xml	(i) debe estar instalado/activado			<mark>OK</mark>
hp_extension	intl	debería estar instalado y activado para conseguir los mejores resultados			<u>ok</u>
hp_extension	json	(i) debe estar instalado/activado			<mark>OK</mark>
hp_extension	hash	(i) debe estar instalado/activado			<mark>ok</mark>
php_setting	memory_limit	(i) detectado ajuste recomendado			OK
php_setting	safe_mode	() detectado ajuste recomendado			<mark>ok</mark>
php_setting	file_uploads	 detectado ajuste recomendado 			<mark>OK</mark>

8. Por último, una vez que se ha dado de alta un usuario, podemos ver como quedaría la aplicación ya instalada y preparada para su personalización.

<u>A</u> rchivo <u>E</u> ditar <u>V</u> er Hi <u>s</u> tor	ial <u>M</u> arcadores Herramien <u>t</u> as Ay <u>u</u> da								
fn Mancomunidad de Munici	pios d 🕹								
e Servidor.mmsierraded	cadiz.lan/moodle/	☆ ✔ 🕄	8 Google					ŝ	
🖥 Más visitados 🗸 🛅 Guadal	inex 🕆 🛅 Conocimiento Libre 🗸 🛅 Software Libre 🗸 🛅 Redes Sociales 🗸 🛅 Periodicos 🗸 🛅 Televisión 🗸								
Mancomunidad de	Municipios de la Sierra de Cádiz	Uste	ed se ha identificado c	omo Anto	onio Jo: Español	sé Fortis M I - España	lalagói (es_es) (<mark>Sali</mark> r) ≎	
Navegación 🗆 🗉	Cursos disponibles			Porta Man	al Moo	odle de l nidad de	a		
Página Principal Área personal	No hay cursos en esta categoría			Muni Cádi	icipios z	s de la S	ierra	de	
Páginas del sitio Mi perfil Currono	(Agregar un nuevo curso)			Cale	endar	io		- <	
P Cursos				Dom	fe Lun N	ebrero 20 _{Aar Mié} J	013 lue Vie	Sáb	
Ajustes de la página principal Activar edición Editar ajustes Usuarios Filtos Copia de seguridad Restaurar Banco de preguntas Ajustes de mi perfil Administración del sitio Buscar				3 10 17 24	4 11 18 25 1	5 6 12 13 19 20 26 27	1 7 8 14 15 21 22 28	2 9 9 16 23	
	Usted se ha identificado <u>como Antonio José Fortis Malagón (Salir)</u>								*

7. Instalación Almacenamiento Virtual (OwnCloud)

El sistema de Almacenamiento Virtual **OwnCloud**, es un software que proporciona un área de almacenamiento independiente de la ubicación de los datos (almacenamiento en la nube). Se creó como una aplicación basada en Software Libre que fuese una alternativa a los proveedores de cloud comerciales, por lo tanto, OwnCloud puede ser instalado en un servidor privado sin ningún tipo de coste adicional.

Para su instalación, es necesario un Servidor Web con soporte para PHP y MySQL, el cual ya lo tenemos disponible, por lo tanto, vamos a detallar los pasos que hemos seguido para su instalación:

1. Nos descargamos de su <u>página web</u> la última versión estable disponible, que en este caso era **owncloud-latest.tar.bz2** y procedemos a descomprimirlo en el directorio /var/www, utilizando para ello el siguiente comando.

tar -xvf owncloud-latest.tar.bz2 -C /var/www

2. El siguiente paso, será hacer dicho directorio accesible al Servidor Web, para ello, ejecutamos el siguiente comando.

chown -R www-data:www-data /var/www/owncloud

3. A continuación, debemos de crear la base de datos que utilizará OwnClud (owncloud), para ello, como administrador de MySQL, ejecutamos los comandos que se muestran en la siguiente captura.

~

```
Archivo Editar Ver Terminal Ayuda
root@servidor:~# mysql -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 129
Server version: 5.1.66-0+squeezel (Debian)
Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> CREATE DATABASE owncloud DEFAULT CHARACTER SET utf8 COLLATE utf8 unicode ci;
Query OK, 1 row affected (0.01 sec)
mysql> GRANT ALL PRIVILEGES ON owncloud.* TO 'owncloud'@'localhost' IDENTIFIED BY 'owncloud';
Query OK, 0 rows affected (0.02 sec)
mvsal> exit
Bye
root@servidor:~#
```

4. Una vez realizadas dichas operaciones, procedemos a reiniciar el Servidor Web para que todos los cambios realizados surtan efecto.

/etc/init.d/apache2 restart

Una vez finalizada la primera parte de la instalación, para finalizar el proceso, debemos de acceder desde un navegador a la dirección donde está ubicada la plataforma **OwnClud** (<u>http://servidor.mmsierradecadiz.lan/owncloud</u>) y continuar con los siguientes pasos.

5. En primer lugar, debemos de crear una cuenta de administrador y especificar el directorio de almacenamiento y la base de datos que hemos creado para la aplicación.



6. A continuación, una vez finalizado el proceso de instalación, se dará de alta un usuario, a través del cual accederemos a la aplicación.

Archivo Editar Ver Historial Marcadores Herramientas Ayuda			
OwnCloud		े 🗸 🛃 🔲 🖌 Google	&
Más visitados ~ 🛅 Guadalinex ~ 🗎 Conocimiento Libre ~ 🛅 Software Lil	bre 🗸 🛅 Redes Sociales 🗸 🛅 Periodicos 🗸 🛅 Televis	sión~	
	own(loud		
	afortis		
	••••••		
	recuérdame Entrar		
	ownCloud - servicios web bajo tu control		

7. Una vez que nos hemos identificado, podemos subir información a la plataforma, tal y como se puede ver, siendo accesible dicha información desde cualquier lugar.

<u>A</u> rchivo <u>E</u> ditar <u>V</u> er	Hi <u>s</u> torial <u>M</u> arcadores Herramien <u>t</u> as Ay <u>u</u> da			
Archivos ownCloud	(afortis) 🕀			
🖉 🖉 🔒 https://serv	ridor.mmsierradecadiz.lan/owncloud/	☆ ∽ 😂	<mark>8</mark> ∨ Google	r 🛔 🔔
🛅 Más visitados 🗸 🛅 G	uadalinex 🕆 🛅 Conocimiento Libre 🕆 🛅 Software Libre 🕆 🛅 Redes Sociales 🗸 🛅 Periodicos 🗸 🛅 Televisión 🗸			
Cloud			٩	ს (
Archivos	Nuevo 🕇			
J Música	Nombre		Tamaño	Modificado
4 Contactos	E linuxMint.pdf		3.8	hace 17 minutos
🛱 Calandaria	owncloud1.png		0.1	hace 16 minutos
	wncloud2.png		0.1	hace 16 minutos
Imágenes	J u2 .ogg		5.6	hace 13 minutos
0				

8. Por último, también es posible configurar OwnCloud a través de WebDAV de forma que nos aparezca como una unidad en nuestro sistema, y de esta forma, sea más fácil acceder a nuestra información.

<u>Archivo</u> <u>E</u> ditar <u>V</u> er	Ir Marcadores Ayuda			
Atrás 🗸 🌩 Adela	ante 🗸 🛧 🔕 😂 [🛅 📃 🔍 100% 🔍	Vista de icono 💲 🛱	
Lugares 🗸 🛛 💥	davs owncloud	remote.php webdav		
 afortis Escritorio Sistema de arch Red windowsVista WebDAV en Papelera Documentos Música Imágenes Vídeos Descargas 	linuxMint.pdf	owncloud1.png	owncloud2.png	J u2.ogg
	4 elementos			

8. Configuración del Cortafuegos

El siguiente servicio que vamos a configurar en nuestro servidor es un cortafuegos, el cual, bloqueará los accesos no autorizados, permitiendo al mismo tiempo, comunicaciones seguras.

Para implementar dicho servicio, se ha hecho uso de **iptables**, el cual, es un componente del framework Netfilter, disponible para el núcleo Linux y que permite interceptar y manipular paquetes de red.

A continuación, se adjunta el código del script que se ha creado junto con los comentarios que explican su funcionamiento.

#!/bin/sh ## SCRIPT de IPTABLES para el Servidor de la Mancomunidad ## Script con Política por defecto Denegar echo -n Aplicando Reglas de Firewall... ## FLUSH de reglas iptables -F iptables -X iptables -Z iptables -t nat -F ## Establecemos politica por defecto: DROP iptables - P INPUT DROP iptables -P OUTPUT DROP iptables - P FORWARD DROP ## Empezamos a abrir, porque ahora esta TODO denegado. ## Debemos decir de manera explicita qué es lo que queremos abrir. # Operar en localhost sin limitaciones iptables - A INPUT - i lo - j ACCEPT iptables -A OUTPUT -o lo -j ACCEPT # A nuestra IP le dejamos todo iptables - A INPUT - s 192.168.0.101 - j ACCEPT iptables -A OUTPUT -d 192.168.0.101 -j ACCEPT #Permitimos conectarnos a nuestra máquina por SSH y tranferencia de ficheros #por sFTP iptables -A INPUT -p tcp -m tcp --sport 22 -m state --state RELATED, ESTABLISHED -j ACCEPT iptables -A OUTPUT -p tcp -m tcp --dport 22 -j ACCEPT # Uno de los servicios que ofrece nuestra máguina es Servidor Web, por tanto, # todo paquete entrante se acepta para ese puerto y los salientes vinculados se aceptan. iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT iptables -A OUTPUT -p tcp -m tcp --sport 80 -m state --state RELATED, ESTABLISHED -j ACCEPT

Completamos el Servidor Web para ofrecer además conexiones seguras (Servicio HTTPS) iptables -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT iptables -A OUTPUT -p tcp -m tcp --sport 443 -m state --state RELATED, ESTABLISHED - j ACCEPT #Otro de los servicios ofrecidos por nuestra máquina es Servidor de Correo, #permitiendo el envío y la recepción de los mismos a través de SMTP e IMAP para #los trabajadores iptables -A INPUT -p tcp -m iprange --src-range 192.168.0.102-192.168.0.254 -d 192.168.0.101 -- dport 25 -j ACCEPT iptables -A OUTPUT -p tcp -m iprange --dst-range 192.168.0.102-192.168.0.254 -s 192.168.0.101 --sport 25 -j ACCEPT iptables -A INPUT -p tcp -m iprange --src-range 192.168.0.102-192.168.0.254 -d 192.168.0.101 -- dport 143 - j ACCEPT iptables -A OUTPUT -p tcp -m iprange --dst-range 192.168.0.102-192.168.0.254 -s 192.168.0.101 -- sport 143 - j ACCEPT #También se permite el uso de los servicios de correo electrónico, de manera #segura sobre SSL iptables -A INPUT -p tcp -m iprange --src-range 192.168.0.102-192.168.0.254 -d 192.168.0.101 -- dport 465 -j ACCEPT iptables -A OUTPUT -p tcp -m iprange --dst-range 192.168.0.102-192.168.0.254 -s 192.168.0.101 --sport 465 -j ACCEPT iptables -A INPUT -p tcp -m iprange --src-range 192.168.0.102-192.168.0.254 -d 192.168.0.101 -- dport 993 -j ACCEPT iptables -A OUTPUT -p tcp -m iprange --dst-range 192.168.0.102-192.168.0.254 -s 192.168.0.101 -- sport 993 -j ACCEPT # Permitimos que la maquina también pueda salir a la web iptables -A INPUT -p tcp -m tcp --sport 80 -m state --state RELATED, ESTABLISHED -j ACCEPT iptables -A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT # Y pueda consultar webs seguras iptables -A INPUT -p tcp -m tcp --sport 443 -m state --state RELATED, ESTABLISHED -j ACCEPT iptables -A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT # Permitimos la consulta a un primer DNS iptables -A INPUT -s 80.58.61.250 -p udp -m udp --sport 53 -j ACCEPT iptables -A OUTPUT -d 80.58.61.250 -p udp -m udp --dport 53 -j ACCEPT # Permitimos la consulta a un segundo DNS iptables -A INPUT -s 80.58.61.254 -p udp -m udp --sport 53 -j ACCEPT iptables -A OUTPUT -d 80.58.61.254 -p udp -m udp --dport 53 -j ACCEPT echo " OK . Verifique que lo que se aplica con: iptables -L -n" # Fin del script

9. Configuración de la Copia de Seguridad

Por último, también se ha decidido implementar un servicio de copias de seguridad, el cual, copiará los ficheros de configuración de los diferentes servicios, junto con las bases de datos y demás directorios que se estimen oportunos y se especifiquen.

A continuación, se adjunta el código del script que se ha creado junto con los comentarios que explican su funcionamiento.

```
#!/bin/sh
```

```
#
#Script que realiza copia de seguridad de las configuraciones que contienen los
#diferentes servicios instalados en el servidor, junto con las bases de datos
#que existen en el sistema.
#Una vez realizada la copia, comprime dicha información y envía un e-mail al
#administrador indicando que la copia de seguridad se ha realizado
#correctamente.
NAME="backup"
                                             # Nombre script.
#Descripción: Script de backup de ficheros de configuracón, datos y Bases de
#Datos.
: ${DATE:=$(date +'%Y-%m-%d')}
                                             # Variable para Fecha.
: ${TIME:=$(date +'%R')}
                                             # Variable para Hora.
: ${WORK DIR:=/seguridad/backups/$DATE} # Directorio de trabajo actual.
: ${LOG FILE:=/seguridad/backups/$DATE/record.log} # Archivo de log.
                                             # Email de Administrador
: ${ADMIN1:=afortis@mmsierradecadiz.lan}
: ${LINE:="------"}
: ${DB PASS:=administrador}
                                                   # Password de MySQL.
# Creando directorio donde se trabajará, si es que no existe.
if [ ! -d "`dirname $LOG_FILE`" ] ; then mkdir -p "`dirname $LOG_FILE`"; fi
# Cambiando a directorio donde trabajaremos.
cd $WORK DIR
# Copiando /ETC/ hacia directorio de trabajo actual.
cp -Rv /etc/ $WORK_DIR > $LOG_FILE
echo $LINE >> $LOG FILE
# Creando carpeta para logs.
mkdir $WORK DIR/logs
# Copiando LOGs.
cp /var/log/apache2/ $WORK_DIR/logs/ -Rv >> $LOG_FILE && echo $LINE >> $LOG_FILE
cp /var/log/aptitud* $WORK_DIR/logs/ -v >> $LOG_FILE && echo $LINE >> $LOG_FILE
cp /var/log/auth* $WORK_DIR/logs/ -v >> $LOG_FILE && echo $LINE >> $LOG_FILE
cp /var/log/daemon* $WORK_DIR/logs/ -v >> $LOG_FILE && echo $LINE >> $LOG_FILE
cp /var/log/dmes* $WORK_DIR/logs/ -v >> $LOG_FILE && echo $LINE >> $LOG_FILE
cp /var/log/kern* $WORK_DIR/logs/ -v >> $LOG_FILE && echo $LINE >> $LOG_FILE
cp /var/log/mail* $WORK_DIR/logs/ -v >> $LOG_FILE && echo $LINE >> $LOG_FILE
cp /var/log/message* $WORK DIR/logs/ -v >> $LOG FILE && echo $LINE >> $LOG FILE
cp /var/log/mysql/ $WORK_DIR/logs/ -Rv >> $LOG_FILE && echo $LINE >> $LOG FILE
cp /var/log/mysql.* $WORK DIR/logs/ -v >> $LOG FILE && echo $LINE >> $LOG FILE
cp /var/log/sys* $WORK DIR/logs/ -v >> $LOG FILE && echo $LINE >> $LOG FILE
```

Creando carpeta para Bases de Datos. mkdir \$WORK DIR/dbs # Exportando DBs. mysqldump --opt -hlocalhost -uroot -p"\$DB_PASS" information_schema > "\$WORK_DIR/dbs/information_schema.sql" mysqldump --opt -hlocalhost -uroot -p"\$DB_PASS" moodle > "\$WORK DIR/dbs/moodle.sql" mysqldump --opt -hlocalhost -uroot -p"\$DB_PASS" mysql > "\$WORK DIR/dbs/mysql.sql" mysqldump --opt -hlocalhost -uroot -p"\$DB_PASS" owncloud > "\$WORK DIR/dbs/owncloud.sql" mysqldump --opt -hlocalhost -uroot -p"\$DB PASS" roundcube > "\$WORK DIR/dbs/roundcube.sql" # Creando carpeta para otros datos del sistema. mkdir \$WORK DIR/datos # Uso de la utilidad Rsync para copiar otros datos del sistema. # El fichero lista directorios contiene los directorios a copiar. rsync -av --delete --prune-empty-dirs --include-from=lista directorios.txt / \$WORK DIR/datos # Saliendo un nivel más arriba (/seguridad/backups/). cd .. # Comprimiendo directorio de trabajo actual. tar czvf "\$DATE.tar.gz" "\$DATE" # Preparando información para enviar por email. touch data.info echo "El archivo \$DATE.rar tiene un tamaño de:" > data.info du -bsh \$DATE.rar >> data.info echo \$LINE >> data.info cat \$LOG FILE >> data.info tar czvf data.info.tar.gz data.info # Eliminando directorio una vez comprimido. rm -R "\$WORK DIR" # Enviando emails a administradores. mail -s "[ScriptBackup] | Status de Backup." \$ADMIN1 < data.info.tar.gz</pre> echo " echo " ## BACKUP REALIZADO! ##" echo " # Fin del script.