

U.T.1 Administración de servidores web



Configuración

Módulos del Apache: Instalación, configuración y uso

Para añadir un conjunto de utilidades al servidor, simplemente hay que añadirle un módulo, de forma que no es necesario volver a instalar el software.

Los módulos del Apache se pueden clasificar en tres categorías:

- ✓ **Módulos Base:** Módulo con las funciones básicas del Apache.
- ✓ **Módulos Multiproceso:** son los responsables de la unión con los puertos de la máquina, aceptando las peticiones y enviando a los hijos a atender a las peticiones
- ✓ **Módulos Adicionales:** Cualquier otro módulo que le añada una funcionalidad al servidor.

Tipos de Módulos

Módulos Estáticos

Módulos dinámicos:

/etc/apache2/mods-enabled

```
root@maite-VirtualBox:~# apache2ctl -l
Compiled in modules:
  core.c
  mod_log_config.c
  mod_logio.c
  prefork.c
  http_core.c
  mod_so.c
root@maite-VirtualBox:~#
```

```
lrwxrwxrwx 1 root root 30 sep 30 14:04 deflate.load -> ../mods-available/deflate.load
lrwxrwxrwx 1 root root 26 sep 30 14:04 dir.conf -> ../mods-available/dir.conf
lrwxrwxrwx 1 root root 26 sep 30 14:04 dir.load -> ../mods-available/dir.load
lrwxrwxrwx 1 root root 26 sep 30 14:04 env.load -> ../mods-available/env.load
lrwxrwxrwx 1 root root 27 sep 30 14:04 mime.conf -> ../mods-available/mime.conf
lrwxrwxrwx 1 root root 27 sep 30 14:04 mime.load -> ../mods-available/mime.load
lrwxrwxrwx 1 root root 34 sep 30 14:04 negotiation.conf -> ../mods-available/negotiation.conf
lrwxrwxrwx 1 root root 34 sep 30 14:04 negotiation.load -> ../mods-available/negotiation.load
lrwxrwxrwx 1 root root 27 oct 5 00:38 php5.conf -> ../mods-available/php5.conf
lrwxrwxrwx 1 root root 27 oct 5 00:38 php5.load -> ../mods-available/php5.load
lrwxrwxrwx 1 root root 33 sep 30 14:04 reqtimeout.conf -> ../mods-available/reqtimeout.conf
lrwxrwxrwx 1 root root 33 sep 30 14:04 reqtimeout.load -> ../mods-available/reqtimeout.load
lrwxrwxrwx 1 root root 31 sep 30 14:04 setenvif.conf -> ../mods-available/setenvif.conf
lrwxrwxrwx 1 root root 31 sep 30 14:04 setenvif.load -> ../mods-available/setenvif.load
lrwxrwxrwx 1 root root 29 sep 30 14:04 status.conf -> ../mods-available/status.conf
lrwxrwxrwx 1 root root 29 sep 30 14:04 status.load -> ../mods-available/status.load
```

Contenidos de los ficheros .conf y .load

```
root@maite-VirtualBox:~#  
root@maite-VirtualBox:~#  
root@maite-VirtualBox:~# cat /etc/apache2/mods-enabled/dir.load  
LoadModule dir_module /usr/lib/apache2/modules/mod_dir.so  
root@maite-VirtualBox:~#  
root@maite-VirtualBox:~#  
root@maite-VirtualBox:~# cat /etc/apache2/mods-enabled/dir.conf  
<IfModule mod_dir.c>  
  
    DirectoryIndex index.html index.cgi index.pl index.php index.xhtml ind  
ex.htm  
  
</IfModule>  
root@maite-VirtualBox:~#
```

Módulos disponibles para cargar

- `ls -la /usr/lib/apache2/modules`

```
-rw-r--r-- 1 root root 13660 feb 13 2012 mod_imagemap.so
-rw-r--r-- 1 root root 42332 feb 13 2012 mod_include.so
-rw-r--r-- 1 root root 17928 feb 13 2012 mod_info.so
-rw-r--r-- 1 root root 50520 feb 13 2012 mod_ldap.so
-rw-r--r-- 1 root root 9568 feb 13 2012 mod_log_forensic.so
-rw-r--r-- 1 root root 25952 feb 13 2012 mod_mem_cache.so
-rw-r--r-- 1 root root 22192 feb 13 2012 mod_mime_magic.so
-rw-r--r-- 1 root root 17752 feb 13 2012 mod_mime.so
-rw-r--r-- 1 root root 30048 feb 13 2012 mod_negotiation.so
-rw-r--r-- 1 root root 38240 feb 13 2012 mod_proxy_ajp.so
-rw-r--r-- 1 root root 25956 feb 13 2012 mod_proxy_balancer.so
-rw-r--r-- 1 root root 9520 feb 13 2012 mod_proxy_connect.so
-rw-r--r-- 1 root root 34092 feb 13 2012 mod_proxy_ftp.so
-rw-r--r-- 1 root root 30048 feb 13 2012 mod_proxy_http.so
-rw-r--r-- 1 root root 13696 feb 13 2012 mod_proxy_scgi.so
-rw-r--r-- 1 root root 79196 feb 13 2012 mod_proxy.so
-rw-r--r-- 1 root root 13664 feb 13 2012 mod_reqtimeout.so
-rw-r--r-- 1 root root 62812 feb 13 2012 mod_rewrite.so
-rw-r--r-- 1 root root 9564 feb 13 2012 mod_setenvif.so
-rw-r--r-- 1 root root 9564 feb 13 2012 mod_speling.so
-rw-r--r-- 1 root root 169708 feb 13 2012 mod_ssl.so
-rw-r--r-- 1 root root 21852 feb 13 2012 mod_status.so
-rw-r--r-- 1 root root 13664 feb 13 2012 mod_substitute.so
-rw-r--r-- 1 root root 5468 feb 13 2012 mod_suexec.so
-rw-r--r-- 1 root root 9516 feb 13 2012 mod_unique_id.so
-rw-r--r-- 1 root root 9564 feb 13 2012 mod_userdir.so
-rw-r--r-- 1 root root 9568 feb 13 2012 mod_usertrack.so
-rw-r--r-- 1 root root 9564 feb 13 2012 mod_version.so
-rw-r--r-- 1 root root 9568 feb 13 2012 mod_vhost_alias.so
```

Paquetes disponibles en los repositorios de ubuntu

- apt-cache search libapache2-mod

```
libapache2-mod-upload-progress - upload progress support for the Apache web server
libapache2-mod-uwsgi - uwsgi module for Apache2 (mod_uwsgi)
libapache2-mod-uwsgi-dbg - debugging symbols for Apache2 mod_uwsgi
libapache2-mod-vhost-hash-alias - Fast and efficient way to manage virtual host
libapache2-mod-vhost-ldap - Apache 2 module for Virtual Hosting from LDAP
libapache2-mod-wsgi-py3 - Python 3 WSGI adapter module for Apache
libapache2-mod-xsendfile - Serve large static files efficiently from web applications
libapache2-modsecurity - Tighten web applications security for Apache
libapr-memcache-dev - memcache client library development files
libapr-memcache0 - memcache client library
libocamlnet-ocaml-dev - OCaml application-level Internet libraries - core development libraries
mono-apache-server2 - ASP.NET 2.0 backend for mod_mono2 Apache module
mono-apache-server4 - ASP.NET 1.1 backend for mod_mono Apache module
mono-fastcgi-server2 - ASP.NET 2.0 backend for FastCGI web servers
mono-fastcgi-server4 - ASP.NET 4.0 backend for FastCGI web servers
php5-fpm - server-side, HTML-embedded scripting language (FPM-CGI binary)
libapache2-mod-jk-doc - Documentación del paquete libapache2-mod-jk
libapache2-mod-auth-pam - module for Apache2 which authenticates using PAM
libapache2-mod-auth-sys-group - Module for Apache2 which checks user against system group
libapache2-mod-fcgid-dbg - símbolos de depuración para mod_fcgid
libapache2-mod-neko - Apache module for running server-side Neko programs
libapache2-mod-removeip - Module to remove IP from apache2's logs
mod_proxyindex - Archivos de configuración para mod_proxyindex
```

Módulo userdir

- Determinar si está activado:

```
root@maite-VirtualBox:~#  
root@maite-VirtualBox:~# ls -la /etc/apache2/mods-enabled | grep userdir  
root@maite-VirtualBox:~#  
root@maite-VirtualBox:~# a2enmod userdir  
Enabling module userdir.  
To activate the new configuration, you need to run:  
    service apache2 restart  
root@maite-VirtualBox:~#  
root@maite-VirtualBox:~# ls -la /etc/apache2/mods-enabled | grep userdir  
lrwxrwxrwx 1 root root 30 oct 10 19:34 userdir.conf -> ../mods-available/userdir.conf  
lrwxrwxrwx 1 root root 30 oct 10 19:34 userdir.load -> ../mods-available/userdir.load  
root@maite-VirtualBox:~# service apache2 restart  
* Restarting web server apache2  
apache2: Could not reliably determine the server's fully qualified domain name,  
using 127.0.1.1 for ServerName  
... waiting apache2: Could not reliably determine the server's fully qualified  
domain name, using 127.0.1.1 for ServerName  
[ OK ]  
root@maite-VirtualBox:~#
```

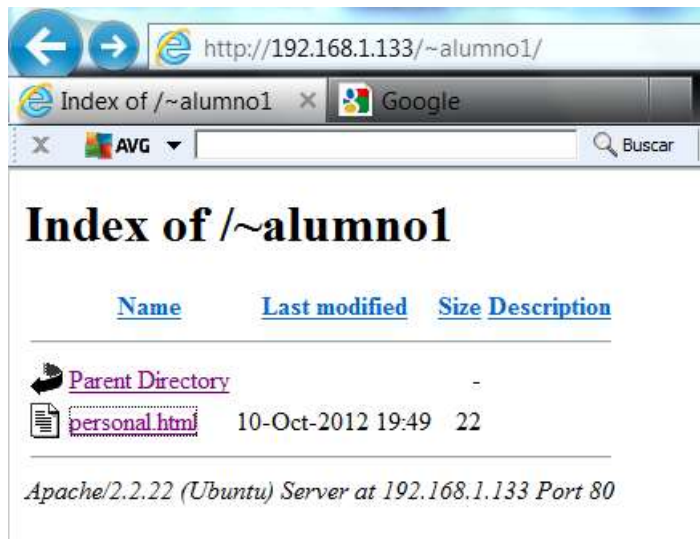
Fichero userdir.conf

- Observar que está habilitado el uso de directorios personales para todos los usuarios, excepto root.

```
root@maite-VirtualBox:~#  
root@maite-VirtualBox:~# cat /etc/apache2/mods-enabled/userdir.conf  
<IfModule mod_userdir.c>  
    UserDir public_html  
    UserDir disabled root  
  
    <Directory /home/*/public_html>  
        AllowOverride FileInfo AuthConfig Limit Indexes  
        Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec  
        <Limit GET POST OPTIONS>  
            Order allow,deny  
            Allow from all  
        </Limit>  
        <LimitExcept GET POST OPTIONS>  
            Order deny,allow  
            Deny from all  
        </LimitExcept>  
    </Directory>  
</IfModule>  
root@maite-VirtualBox:~# _
```


Creación de directorios personales

- public_html es el nombre del directorio que pueden crear los usuarios en su directorio /home para poner sus páginas personales.



Control de acceso por IP

- Crear un directorio secundaria y configurar Apache para que sólo se pueda acceder a él desde la MV de XP.

```
<Directory /var/www/secundaria>  
    Options Indexes FollowSymLinks MultiViews  
    AllowOverride None  
    Order allow,deny  
    allow from 192.168.1.134  
</Directory>
```

Seguridad de Apache. Autenticación y autorización de usuarios

- Cuando un servidor apache recibe una petición de una página web, antes de devolver el resultado, lleva a cabo varias acciones para verificar que la petición está autorizada.

Las distintas acciones que lleva a cabo para verificar la validez de la aplicación, se pueden agrupar en tres tipos: Autenticación, Autorización y Control de Acceso.

Autenticación

- La autenticación, autenticación o **acreditación** es el proceso por el cual se verifica la identidad de una persona. De una forma simple, este proceso se puede llevar a cabo mediante un nombre de usuario y una contraseña, pero se pueden llegar a utilizar otros métodos para validar la identidad de una persona, como mediante el uso de certificados, tarjetas etc

Autenticación Basic a los usuarios alumno1/alumno2 sobre un directorio

- 1/ Comprobar que el módulo auth_basic está habilitado
- 2/ Crear un fichero accesible por Apache en el que se guardarán los usuarios y las contraseñas:
`htpasswd -c /etc/apache2/passwd alumno1`
`htpasswd /etc/apache2/passwd alumno2`
- 3/ En el fichero default permitir el acceso a los dos usuarios al directorio secundaria.

Los valores posibles del tipo de autenticación son: Basic y Digest.
Con Basic, la transferencia de las claves se hará sin cifrar, y con digest se harán cifradas.

Configuración de la Autenticación

- **AuthType:** selecciona el tipo de autenticación de usuarios.
- **AuthName:** especifica un nombre del dominio para el cual se solicita el acceso, este nombre figurará en la pantalla donde se pide la clave.
- **Require:** selecciona los usuarios que pueden acceder a un área determinada

Creación de ficheros con usuario/passwd

```
root@maite-VirtualBox:/etc/apache2# htpasswd -c /etc/apache2/passwd alumno1
New password:
Re-type new password:
Adding password for user alumno1
root@maite-VirtualBox:/etc/apache2#
root@maite-VirtualBox:/etc/apache2# htpasswd /etc/apache2/passwd alumno2
New password:
Re-type new password:
Adding password for user alumno2
root@maite-VirtualBox:/etc/apache2# ls -la pas*
-rw-r--r-- 1 root root 92 oct 10 20:47 passwd
root@maite-VirtualBox:/etc/apache2# cat passwd
alumno1:$apr1$nlw2K9oX$EuKqXW7Xbipe6qhZlshHA1
alumno2:$apr1$U7M7FPhs$1zq7o j4qNPhosviF0THsp/
root@maite-VirtualBox:/etc/apache2#
root@maite-VirtualBox:/etc/apache2#
```

Fichero de configuración

```
<Directory /var/www/secundaria>  
    Options Indexes FollowSymLinks MultiViews  
    AllowOverride None  
    Order allow,deny  
    allow from all  
    AuthType Basic  
    AuthName "Acceso Restringido"  
    AuthUserFile /etc/apache2/passwd  
    Require user alumno1 alumno2  
</Directory>
```


Autenticación HTTP Digest

- 1/ Comprobar que el módulo auth_digest está habilitado y si no lo está habilitarlo.
- 2/ Crear un fichero accesible por Apache en el que se guardarán los usuarios y las contraseñas:
`htdigest -c /etc/apache2/passwd info alumno1`
`htdigest /etc/apache2/passwd info alumno2`
- 3/ En el fichero default permitir el acceso al/los usuarios al directorio fp

Módulo de control de acceso

- El módulo de control de acceso de apache permite controlar el acceso a los diferentes directorios y ficheros del servidor dependiendo del nombre de la máquina o dirección IP del cliente.
- Las directivas que proporciona este módulo se pueden utilizar dentro de los elementos `<Directory>`, y del fichero de configuración `httpd.conf`, o bien dentro de ficheros `.htaccess` ubicados dentro de las carpetas.

Las directivas con las que cuenta el módulo para permitir o denegar el acceso son:

- **Allow:** controla los servidores que tendrán acceso al contenido.
- **Deny:** controla los servidores a los que se denegará el acceso.
- **Order:** determina el orden en el que se leerán los permisos, por ejemplo para leer primero los permitidos y luego los no permitidos se pondrá "Allow,Deny" en este caso si un servidor está en la lista de permitidos, y en la de denegados, el acceso al mismo será denegado, ya que la entrada dentro de la opción Deny sobrescribirá la de la entrada Allow.

Ficheros .htaccess

- Habilitar el uso del fichero de configuración de directorios .htaccess, en el directorio /home/maite/cuaderno para que sea el usuario maite el que pueda controlar como sirve Apache el contenido de dicho directorio.
- Configurar un alias /cuaderno que permita acceder al directorio /home/maite/cuaderno
- Como usuario maite, configura el .htaccess, de forma que sólo se pueda acceder al directorio desde la MV de XP y utilice autenticación digest, para que solo pueda acceder el usuario “virtual” cuaderno.

Pasos

- 1/ Configurar default permitiendo sobrecribir todas las directivas de cuaderno por el fichero .htaccess

```
Alias /cuaderno /home/maite/cuaderno
<Directory /home/maite/cuaderno>
    Options FollowSymLinks MultiViews
    AllowOverride All
    Order allow,deny
    allow from all
</Directory>
```

.htaccess

- 2/ Como usuario maite configura el fichero .htaccess, sobre el fichero /home/maite/cuaderno, para que sólo se pueda acceder desde la MV XP y utilice autenticación http Digest para que sólo pueda acceder el usuario cuaderno

```
maite@maite-VirtualBox:~/cuaderno$  
maite@maite-VirtualBox:~/cuaderno$ cat .htaccess  
Options Indexes  
AuthType Digest  
AuthName "info"  
AuthUserFile /home/maite/.htdigest  
Require user cuaderno  
  
maite@maite-VirtualBox:~/cuaderno$ _
```

Creación de fichero de passwords

- `htdigest -c /home/maite/.htdigest info cuaderno`

