

# Servidores Web Apache

## Inicio del servidor Apache

### Comando apachectl

El comando **apachectl** es un front end de httpd.

Antes de iniciar el servidor es conveniente chequear la sintaxis usando el comando:

```
apachectl -t
```

```
Syntax OK
```

Otras opciones del comando:

Ver que módulos tiene cargados

```
apachectl -l
```

Compiled in modules:

```
core.c  
prefork.c  
http_core.c  
mod_so.c
```

Ver con que opciones fue compilado

```
apachectl -V
```

### Iniciar

Con el comando: `"service httpd start"` iniciamos el servidor apache.

### Estado

Para ver el estado del servicio utilizamos el comando:

```
"service httpd status"
```

### Detener

Para detener el servicio:

```
"service httpd stop"
```

### Reiniciar

Si se realizan modificaciones en los archivos de configuración se debe reiniciar el servicio con el comando:

```
"service httpd restart"
```

## Configuración Inicial

Nombre del servidor

**ServerName**

Porqué esta viendo la página principal de Apache si en el directorio /var/www/html no hay nada?

Coloque una archivo index.html con un contenido en /var/www/html y actualice el navegador.

Modifique el nombre index.html por archivo.txt, actualice el navegador, por que está viendo la página de apache?

Modifique la configuración para poder ver como página por defecto a: archivo.txt en

**DocumentRoot**

## Acceso con seguridad

Es posible configurar directorios en apache donde solo puedan acceder determinados usuarios autorizados.

Primero veremos como configurar el acceso de los usuarios a sus propios directorios personales, luego a un directorio en particular. Trabajaremos en la configuración de un usuario o de un grupo de usuarios.

### Permitir el acceso al directorio del usuario

El directorio del usuario se encuentra en su propio home, por ejemplo: `/home/solange/www`

Para ir a la página del usuario en el browser se ingresará:  
**`http://www.dominio.com.uy/~solange`**

De esta forma la administración del contenido estará a cargo del usuario.

## Configuración

### Contenidos

El directorio personal del usuario debe contener un subdirectorio: `www` y un archivo `index.html`

```
[solange@server1 ~]$ tree
.
|-- www
    |-- index.html
```

### Permisos en el sistema de archivos

Se debe configurar los directorios para permitir el acceso de lectura en los directorios de los usuarios, ejecutando el comando `chmod`, por ejemplo para el usuario `solange`:

```
chmod 755 solange
```

Ejemplo de los permisos asignados a los usuarios.

```
[solange@server1 home]$ ll
total 20
drwxr-xr-x 5 adrian  adrian  4096 ago 22 13:11 adrian
drwxr-xr-x 5 solange solange 4096 ago 22 12:53 solange
```

## Configuración del archivo httpd.conf

Primero se configura el siguiente módulo **mod\_userdir.c** en el archivo **httpd.conf**

```
<IfModule mod_userdir.c>

    UserDir disable
    UserDir enabled solange
    UserDir /home/*/www

</IfModule>
```

Luego se ingresan las directivas de acceso:

```
<Directory /home/*/www>
    AllowOverride FileInfo AuthConfig Limit
    Options MultiViews Indexes SymLinksIfOwnerMatch
    IncludesNoExec
    <Limit GET POST OPTIONS>
        Order allow,deny
        Allow from all
        AuthType Basic
        AuthName "Restricted Files"
        AuthUserFile /usr/local/apache/passwd/password
        require user solange
    </Limit>
    <LimitExcept GET POST OPTIONS>
        Order deny,allow
        Deny from all
    </LimitExcept>
</Directory>
```

Directiva	Descripción
<b>AuthType Basic</b>	Tipo de autenticación, Basic es la más segura.
<b>AuthName</b>	Es el aviso que vera el usuario al querer entrar en el directorio del usuario
<b>AuthUserFile</b>	Es la ruta al archivo que contiene los usuarios y las contraseñas.
<b>require</b>	Define el tipo de ingreso, las palabras claves pueden ser: <ol style="list-style-type: none"> <li>1. user</li> <li>2. group</li> <li>3. valid-user</li> </ol>
<b>Limit</b>	Establece que opciones podrán utilizarse: GET POST OPTIONS
<b>LimitExcept</b>	Establece que el resto de las opciones que no están listadas serán denegadas, o sea las únicas permitidas serán: GET POST OPTIONS

<b>SymLinksIfOwnerMatch</b>	Solo los enlaces que apunten a un directorio del dueño serán permitidos.
<b>Indexes</b>	Si en el directorio no hay una página index.html se mostrará el contenido.

## Comando htpasswd

Con este comando se crea y administra el archivo especificado en la directiva: **AuthUserFile**.

Como las contraseñas se almacenan cifradas, este archivo no se edita directamente, sino que se crea y se gestionan sus usuarios mediante el comando htpasswd.

### **htpasswd [-c] archivo\_de\_passwords nombre\_usuario**

La opción `-c` se utiliza para crear el archivo cuando se introducen los datos del primer usuario. El programa pedirá la contraseña del usuario y su confirmación. Puede utilizarse también para modificar las contraseñas de usuarios ya incluidos en el archivo.

Ejemplo: creación de la cuenta del usuario solange

```
Htpasswd -c /usr/local/apache/passwd/passwords solange
New password:
Re-type new password:
Updating password for user solange
```

Contenido del archivo con el usuario y la contraseña.

```
[root@server1 httpd]# cat /usr/local/apache/passwd/password
solange:pTCePQJYjAv4I
```

## Permitir el acceso a un grupo de usuarios

Modificamos en la directiva `mod_userdir.c` habilitando el grupo **gente**.

```
<IfModule mod_userdir.c>

#   UserDir disable
   UserDir enabled gente
   UserDir /home/*/www

</IfModule>
```

Modificación de las directivas de acceso:

```
<Directory /home/*/www>
  AllowOverride FileInfo AuthConfig Limit
  Options MultiViews Indexes SymLinksIfOwnerMatch
  IncludesNoExec
  <Limit GET POST OPTIONS>
    Order allow,deny
    Allow from all
    AuthType Basic
    AuthName "Restricted Files"
    AuthUserFile /usr/local/apache/passwd/password
    AuthGroupFile /usr/local/apache/passwd/grupo
    require group gente
  </Limit>
  <LimitExcept GET POST OPTIONS>
    Order deny,allow
    Deny from all
  </LimitExcept>
</Directory>
```

Con la directiva **AuthGroupFile** se define al archivo que tiene el nombre del grupo y los nombres de los usuarios.

Hay que tener en cuenta que los usuarios del grupo deben estar creados en el archivo:  
**/usr/local/apache/passwd/password**

Ejemplo del contenido del archivo **/usr/local/apache/passwd/grupo**

```
gente: solange adrian
```

Los usuarios que podrán acceder a sus directorios serán los que estén contenidos en el grupo, según la directiva: **require group gente**

## valid-user

Otra forma de permitir el acceso a un grupo de usuarios.

```
<IfModule mod_userdir.c>

#   UserDir disable
   UserDir enabled gente
   UserDir /home/*/www

</IfModule>
```

Modificación de las directivas de acceso:

```
<Directory /home/*/www>
  AllowOverride FileInfo AuthConfig Limit
  Options MultiViews Indexes SymLinksIfOwnerMatch
  IncludesNoExec
  <Limit GET POST OPTIONS>
    Order allow,deny
    Allow from all
    AuthType Basic
    AuthName "Restricted Files"
    AuthUserFile /usr/local/apache/passwd/password
    require valid-user
  </Limit>
  <LimitExcept GET POST OPTIONS>
    Order deny,allow
    Deny from all
  </LimitExcept>
</Directory>
```

Con la directiva **require valid-user** definimos que todos los usuarios habilitados están contenidos en el archivo definido en la directiva **AuthUserFile**.





## Acceso por usuario en un directorio

La directiva: `DocumentRoot "/var/www/html"` define el directorio que contendrá los documentos que se ofrecen a los clientes. Podemos crear aquí un subdirectorio y configurarlo para permitir el acceso solo a un grupo de usuarios.

### Configuración de un directorio

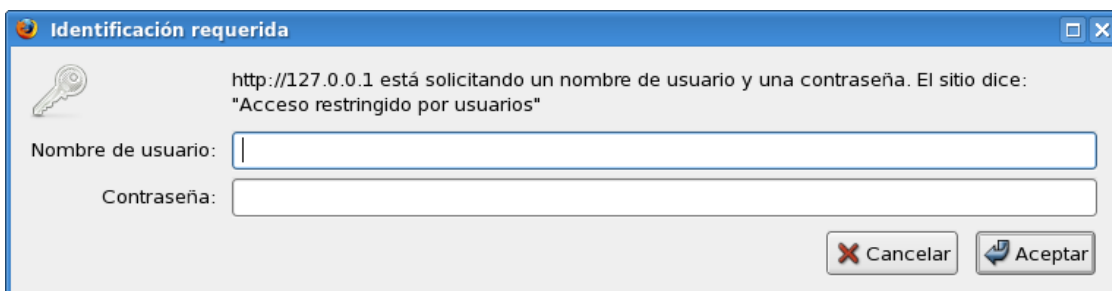
Creamos un directorio en: `/var/www/html/directorio`

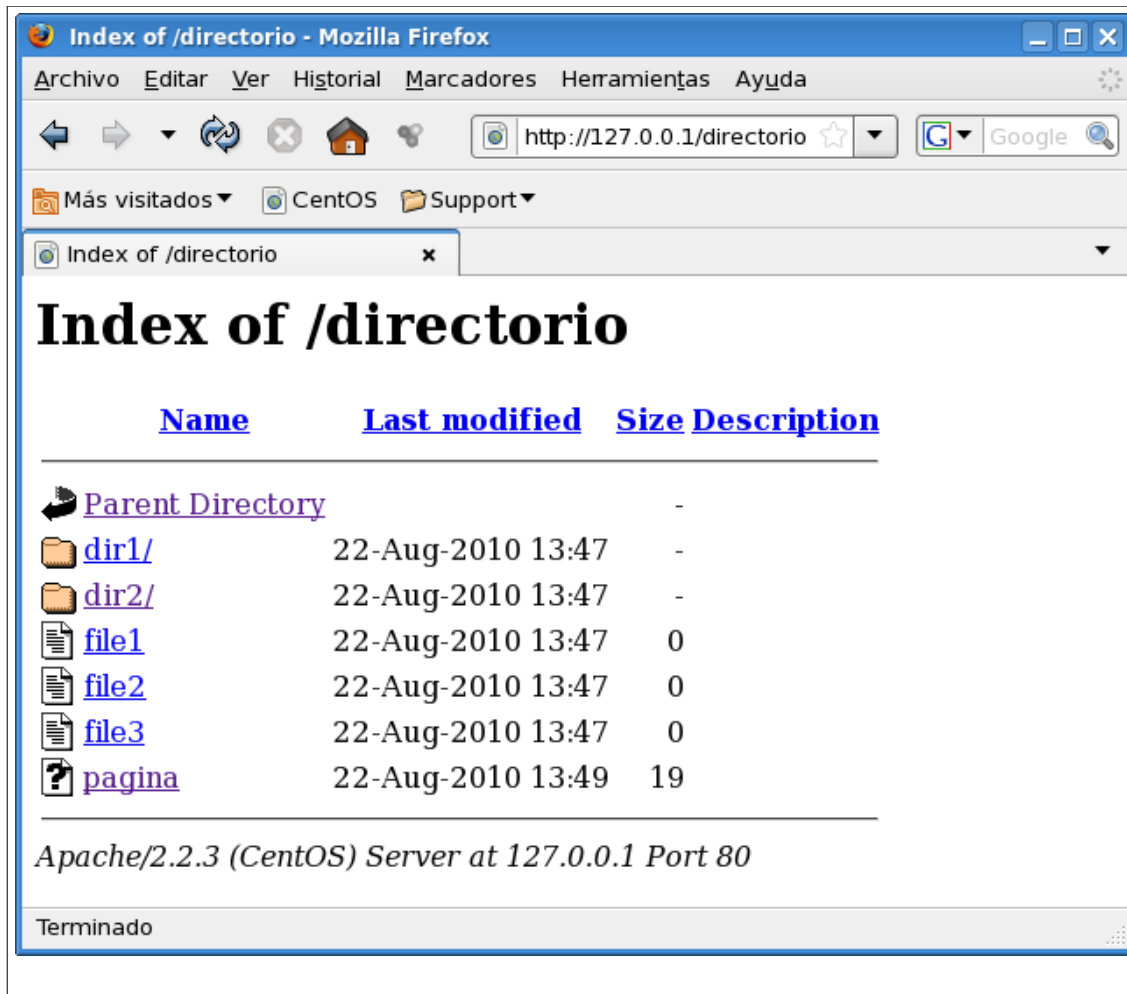
Configuración en el archivo `httpd.conf`

```
<Directory /var/www/html/directorio>
  AllowOverride FileInfo AuthConfig Limit
  Options MultiViews Indexes SymLinksIfOwnerMatch
  IncludesNoExec
  <Limit GET POST OPTIONS>
    Order allow,deny
    Allow from all
    AuthType Basic
    AuthName "Acceso restringido por usuarios"
    AuthUserFile /usr/local/apache/passwd/password
    require valid-user
  </Limit>
  <LimitExcept GET POST OPTIONS>
    Order deny,allow
    Deny from all
  </LimitExcept>
</Directory>
```








Ingreso en el browser: <http://www.dominio.com.uy/directorio>

En todos los directorios con acceso protegido en el browser el usuario deberá ingresar su nombre y contraseña, como se muestra en la siguiente figura.





The screenshot shows a Mozilla Firefox browser window with the title "Index of /directorio". The address bar displays "http://127.0.0.1/directorio". The browser interface includes a menu bar with "Archivo", "Editar", "Ver", "Historial", "Marcadores", "Herramientas", and "Ayuda". Below the menu bar is a toolbar with navigation icons and a search bar containing "Google". The browser's "Más visitados" (Most Visited) section shows "CentOS" and "Support". The main content area displays the "Index of /directorio" page, which features a table with columns for "Name", "Last modified", "Size", and "Description". The table lists several items: "Parent Directory", "dir1/", "dir2/", "file1", "file2", "file3", and "pagina". Below the table, the text "Apache/2.2.3 (CentOS) Server at 127.0.0.1 Port 80" is visible. The status bar at the bottom of the browser window shows "Terminado".

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">dir1/</a>	22-Aug-2010 13:47	-	
 <a href="#">dir2/</a>	22-Aug-2010 13:47	-	
 <a href="#">file1</a>	22-Aug-2010 13:47	0	
 <a href="#">file2</a>	22-Aug-2010 13:47	0	
 <a href="#">file3</a>	22-Aug-2010 13:47	0	
 <a href="#">pagina</a>	22-Aug-2010 13:49	19	

Apache/2.2.3 (CentOS) Server at 127.0.0.1 Port 80

Terminado

## Configuración de dominios virtuales

Existen tres formas de crear hosts virtuales en un mismo equipo:

1. Mismo hosts con diferentes direcciones IP.
2. Diferente nombre con la misma dirección IP,
3. Ejecutar varias instancias del servidor con diferentes archivos de configuración. Esta opción sobrecarga el servidor, pero facilita la administración si debe realizar modificaciones en los archivos de configuración.

### Sección virtual hosts

Las configuraciones se realizan en esta sección del archivo http.conf.

#### Configuración por dirección IP

En este caso tenemos un servidor con mas de una tarjeta de red, cada una con una dirección IP, configuramos cada uno de los servidores web en una de estas direcciones.

Para configurar dominios virtuales primero se debe descomentar la línea: **"NameVirtualHost \*:80#" para que apache trabaje con ellos.** Luego ingresar los valores de cada uno, según se define en la siguiente tabla.

<b>&lt;VirtualHost IP:80&gt;</b>	Dirección IP y puerto
<b>ServerAdmin</b>	Dirección de correo del encargado del servidor
<b>DocumentRoot</b>	Directorio que contiene las páginas web
<b>ServerName</b>	nombre con el cual será conocido y accedido desde el web
<b>&lt;/VirtualHost&gt;</b>	Fin de la definición

Ejemplo de configuración por diferentes direcciones IP.

```
NameVirtualHost *:80#

<VirtualHost 20.20.142.198:80>
    ServerAdmin webmaster@example.com
    DocumentRoot /virtual/uno/www
    ServerName www.uno.com.uy
</VirtualHost>

<VirtualHost 20.20.142.199:80>
    ServerAdmin webmaster@example.com
    DocumentRoot /virtual/dos/www
    ServerName www.dos.com.uy
```

```
</VirtualHost>
```

### Configuración por nombre

Para poder ofrecer servicios de Hosting a muchos dominios se utiliza una misma dirección IP con diferentes nombres, como se muestra en el ejemplo.

Ejemplo configuración de varios dominios utilizando la misma dirección IP.

```
NameVirtualHost *:80#  
  
<VirtualHost *:80>  
    ServerAdmin webmaster@example.com  
    DocumentRoot /virtual/uno/www  
    ServerName www.uno.com.uy  
</VirtualHost>  
  
<VirtualHost *:80>  
    ServerAdmin webmaster@example.com  
    DocumentRoot /virtual/dos/www  
    ServerName www.dos.com.uy  
</VirtualHost>
```

Realizar la configuración en archivos separados permite automatizar la administración de los dominios, para esto en el archivo httpd.conf declaramos que incluimos un directorio con archivos de extensión “conf” de la siguiente forma:

```
NameVirtualHost *:80
```

```
Include virtuales/*.conf
```

Creamos el directorio donde se encuentra: `ServerRoot "/etc/httpd"`

```
[root@server1 httpd]# ll
total 20
drwxr-xr-x 2 root root 4096 ago 28 10:12 conf
drwxr-xr-x 2 root root 4096 ago 26 18:19 conf.d
lrwxrwxrwx 1 root root 19 ago 26 18:19 logs ->
../../var/log/httpd
lrwxrwxrwx 1 root root 27 ago 26 18:19 modules ->
../../usr/lib/httpd/modules
lrwxrwxrwx 1 root root 13 ago 26 18:19 run -> ../../var/run
drwxr-xr-x 2 root root 4096 ago 28 09:58 virtuales
```

en el directorio virtuales creamos un archivo por cada dominio

```
[root@server1 virtuales]# ll
total 8
-rw-r--r-- 1 root root 142 ago 28 09:57 www.dos.com.uy.conf
-rw-r--r-- 1 root root 142 ago 28 09:58 www.uno.com.uy.conf
```

Contenido de los archivos

```
[root@server1 virtuales]# cat www.uno.com.uy.conf
<VirtualHost *:80>
    ServerAdmin webmaster@example.com
    DocumentRoot /virtual/uno/www
    ServerName www.uno.com.uy
</VirtualHost>
```

```
[root@server1 virtuales]# cat www.dos.com.uy.conf
<VirtualHost *:80>
    ServerAdmin webmaster@example.com
    DocumentRoot /virtual/dos/www
    ServerName www.dos.com.uy
</VirtualHost>
```

De esta forma para eliminar un dominio simplemente se borra el archivo, y para dar el alta se crea el archivo con el contenido y nombre apropiado.

## Configuración DNS

Los hosts virtuales deben configurarse apropiadamente en el DNS.  
Ejemplo para servidores virtuales por nombre con la misma dirección IP

### Archivo `named.rfc1912`

Configuración del archivo `named.rfc1912`

```
zone "dominio.com.uy" IN {
    type master;
    file "named.dominio";
};
zone "142.20.20.in-addr.arpa" IN {
    type master ;
    file "rev.dominio";
};
zone "uno.com.uy" IN {
    type master;
    file "named.uno.com.uy";
};
zone "dos.com.uy" IN {
    type master;
    file "named.dos.com.uy";
};
```

## Archivos de zona

Configuración del archivo de zona: named.uno.com.uy

```
$TTL 172800
@ IN SOA uno.com.uy. root.localhost. (
                                3
                                10800
                                7200
                                1296000
                                172800 )
;
    IN NS      ns1.dominio.com.uy.
www.uno.com.uy. IN A      20.20.142.199
```

Configuración del archivo de zona: named.dos.com.uy

```
$TTL 172800
@ IN SOA dos.com.uy. root.localhost. (
                                3
                                10800
                                7200
                                1296000
                                172800 )
;
      IN  NS      ns1.dominio.com.uy.
www.dos.com.uy. IN A 20.20.142.199
```