

**Alumno/a: José Manuel González Peña**

## **PRÁCTICA 5: Servidores Web con autenticación.**

- Tiempo de realización : 2 horas en clase. Documentación en casa.

- Objetivo:

Restringir el acceso a algunos recursos (páginas).

Con

Apache podemos establecer mecanismos de usuario y contraseña, para limitar el acceso. Incluso los usuarios pueden incluirse en grupos y establecer los permisos de acceso a nivel de grupo lo cual puede resultar más cómodo.

¡PERO CUIDADO! la transmisión de información tiene una encriptación muy débil. Aunque en esta primera práctica sobre permisos de acceso aún no lo vamos a aplicar , ten en cuenta que no deberías estar pasando password si no utilizas también

SSL. Cualquier sniffer podrá fácilmente robarte las contraseñas! Lo veremos en la siguiente práctica.

También hay que tener en cuenta que

Apache permite otros métodos más sofisticados de autenticación como son: guardar la contraseña en bases de datos (tipo DB y DBM), en un directorio LDAP e incluso en bases de datos relacionales como MySQL.

- Procedimiento:

Leer el capítulo 5 de la "Guía de supervivencia Apache"

Leer el capítulo "Más Opciones" del Curso de Víctor Fuster.

Aplicar mecanismos de control de acceso sobre alguno de los servidores Web virtuales creados en prácticas anteriores.

1. Enumera las Directivas de Autenticación.

- AuthType
- AuthName
- AuthUserFile
- AuthDigestFile
- AuthGroupFile
- Require
- Allow
- Deny
- Order
- AccessFileName
- AllowOverride

2. Enumera las Directivas para el control de acceso por IPs.

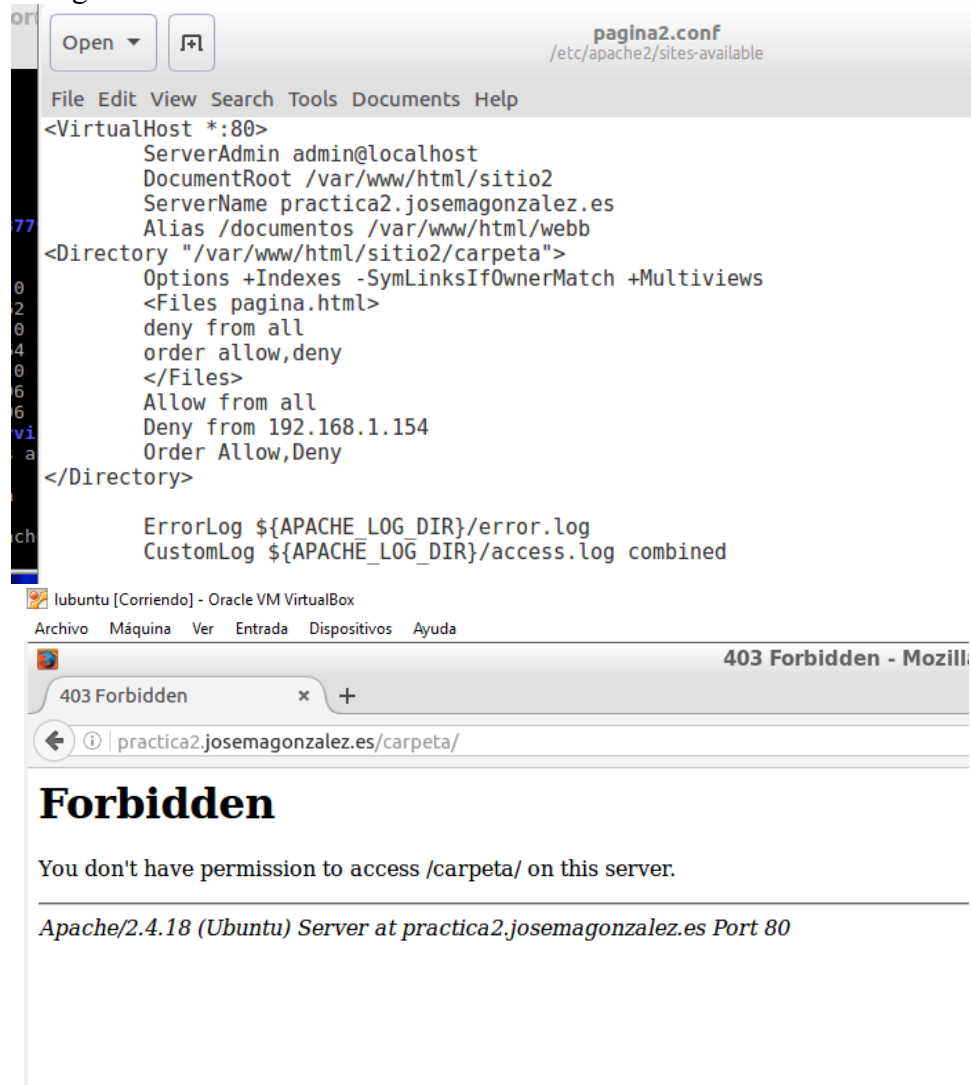
- AuthType
- AuthName
- Require

3. Indica el servidor web que vas a utilizar (IP y nombre) y el cliente (IP y/o nombre)

Servidor web: 192.168.1.152 / http://practica2.josemagonzalez.es/

Cliente: 192.168.1.154

4. Denegar acceso por IP a una de tus máquinas clientes. Debes probar que el cliente inicialmente tenga acceso y luego denegárselo.



The screenshot shows two windows. The top window is a text editor displaying the configuration file `pagina2.conf` for a VirtualHost. The configuration includes a `<Directory>` block for `/var/www/html/sitio2/carpeta/` with the following settings:

```

<Directory "/var/www/html/sitio2/carpeta">
    Options +Indexes -SymLinksIfOwnerMatch +Multiviews
    <Files pagina.html>
        deny from all
        order allow,deny
    </Files>
    Allow from all
    Deny from 192.168.1.154
    Order Allow,Deny
</Directory>

```

The bottom window is a web browser (Mozilla) showing a "403 Forbidden" error. The address bar shows `practica2.josemagonzalez.es/carpeta/`. The page content reads:

**Forbidden**

You don't have permission to access /carpeta/ on this server.

Apache/2.4.18 (Ubuntu) Server at practica2.josemagonzalez.es Port 80

5. Autenticación Digest por usuario (mediante un fichero de cuentas de usuario).

```

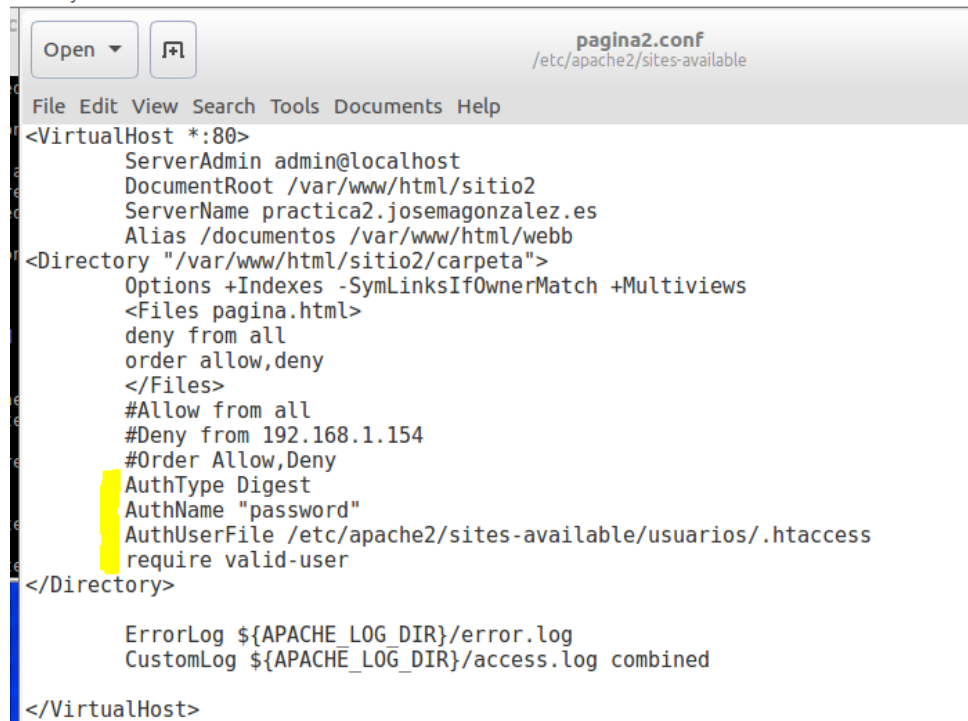
servidor@ubuntu:/$ sudo a2enmod authz_groupfile
[sudo] password for servidor:
Considering dependency authz_core for authz_groupfile:
Module authz_core already enabled
Enabling module authz_groupfile.
To activate the new configuration, you need to run:
    service apache2 restart
servidor@ubuntu:/$ sudo a2enmod auth_digest
Considering dependency authn_core for auth_digest:
Module authn_core already enabled
Enabling module auth_digest.
To activate the new configuration, you need to run:
    service apache2 restart
servidor@ubuntu:/$

```

### 5.1. Autenticación de un usuario concreto.

```
servidor@ubuntu:/etc/apache2/sites-available/usuarios$ sudo htdigest -c .htaccess password usuario
Adding password for usuario in realm password.
New password:
Re-type new password:
servidor@ubuntu:/etc/apache2/sites-available/usuarios$ sudo service apache2 restart
```

ivos Ayuda



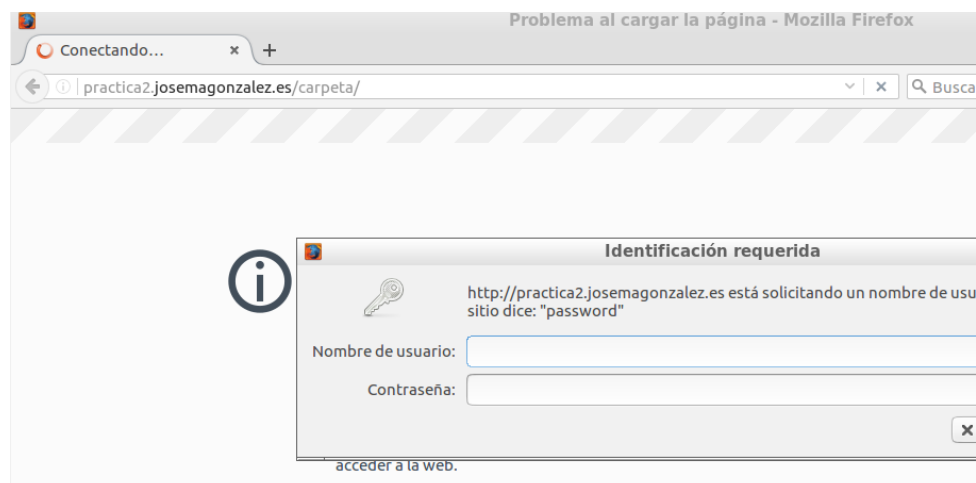
```
pagina2.conf
/etc/apache2/sites-available

File Edit View Search Tools Documents Help

<VirtualHost *:80>
    ServerAdmin admin@localhost
    DocumentRoot /var/www/html/sitio2
    ServerName practica2.josemagonzalez.es
    Alias /documentos /var/www/html/webb
    <Directory "/var/www/html/sitio2/carpeta">
        Options +Indexes -SymLinksIfOwnerMatch +Multiviews
        <Files pagina.html>
            deny from all
            order allow,deny
        </Files>
        #Allow from all
        #Deny from 192.168.1.154
        #Order Allow,Deny
        AuthType Digest
        AuthName "password"
        AuthUserFile /etc/apache2/sites-available/usuarios/.htaccess
        require valid-user
    </Directory>

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

</VirtualHost>
```



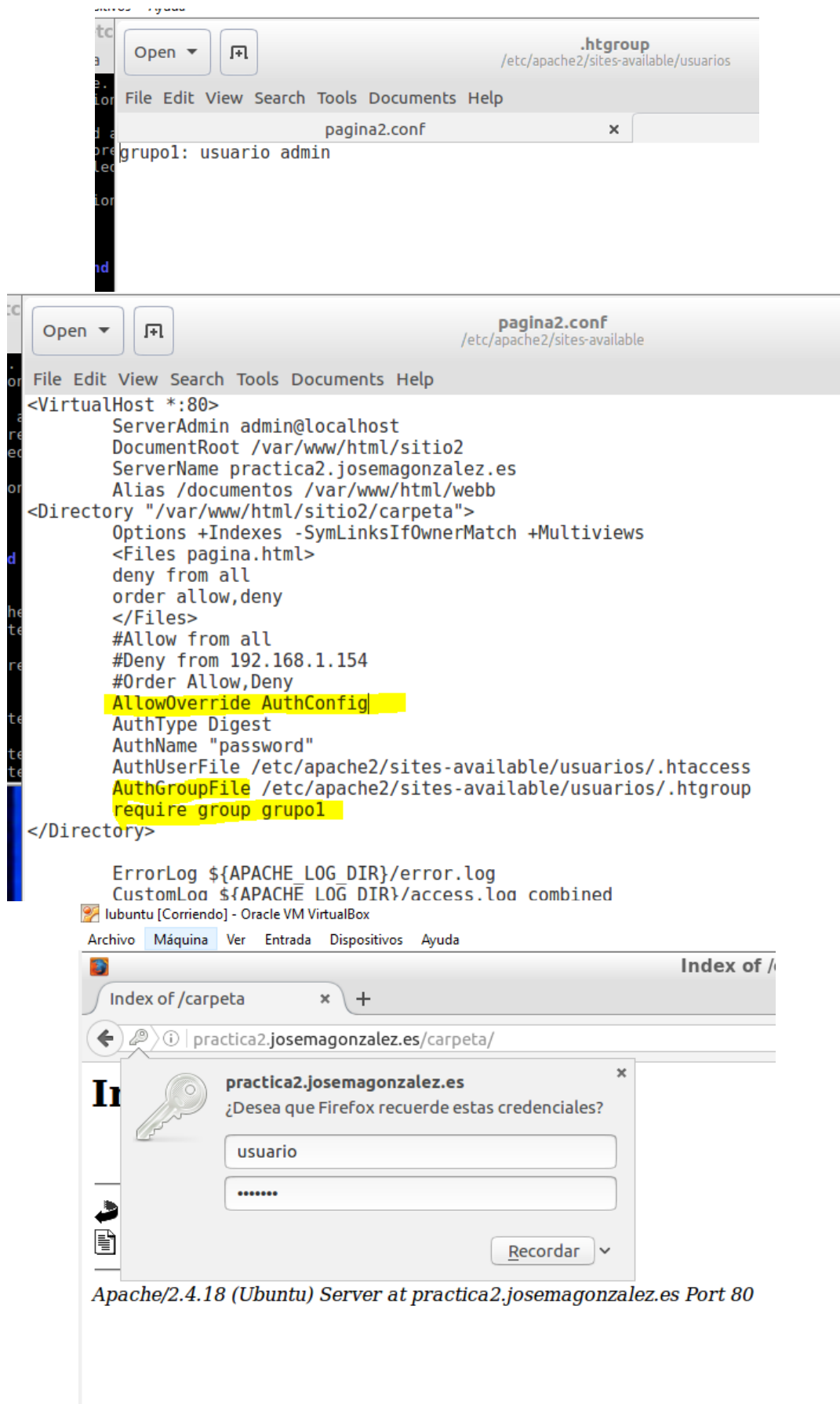
### 5.2. Autenticación de un grupo (llámalo grupo[tuapellido])

Nota: desde la versión Apache 2.0 la directiva para Digest es AuthUserFile en lugar de AuthDigestFile (que es como se indica en la Guía de supervivencia de Apache)

Nota 2: Para la autenticación por grupo hay que crear un fichero de texto en el que introduzcamos en texto plano los nombres de aquellos usuarios de Digest que forman el grupo. Después usar :

AuthGroupFile ruta\_del\_fichero\_grupo

Require group fichero\_grupo



The image shows a sequence of steps for configuring a web server and accessing it. At the top, a file editor window displays the contents of `.htgroup` in `/etc/apache2/sites-available/usuarios`, which defines a group named `grupol` with the user `usuario`.

Below it, another file editor window shows the configuration for `pagina2.conf` in `/etc/apache2/sites-available`. The configuration includes a `VirtualHost` block for port 80, setting the document root to `/var/www/html/sitio2` and the server name to `practica2.josemagonzalez.es`. A `Directory` block for `/var/www/html/sitio2/carpeta` is configured with `Options +Indexes -SymLinksIfOwnerMatch +Multiviews` and `<Files pagina.html>`. It includes access control rules: `deny from all`, `order allow,deny`, `#Allow from all`, `#Deny from 192.168.1.154`, and `#Order Allow,Deny`. Crucially, it sets `AllowOverride AuthConfig`, `AuthType Digest`, `AuthName "password"`, `AuthUserFile /etc/apache2/sites-available/usuarios/.htaccess`, `AuthGroupFile /etc/apache2/sites-available/usuarios/.htgroup`, and `require group grupol`.

At the bottom, a web browser window shows the "Index of /carpeta" page for `practica2.josemagonzalez.es`. A Firefox password prompt is displayed, asking if it should remember credentials for the site, with fields for "usuario" and a masked password, and a "Recordar" button.

Apache/2.4.18 (Ubuntu) Server at practica2.josemagonzalez.es Port 80

6. ¿Qué indica el código de estado 401 que devuelve el navegador? ¿Y el 403? ¿Cuál y cuándo te ha aparecido?

lubuntu [Corriendo] - Oracle VM VirtualBox  
Archivo Máquina Ver Entrada Dispositivos Ayuda

**401 Unauthorized - Mozilla Firefox**

401 Unauthorized x +

← ⓘ practica2.josemagonzalez.es/carpeta/ ↻ 🔍

## Unauthorized

This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad username/password) or you supplied no credential at all. Your browser doesn't understand how to supply the credentials required.

---

*Apache/2.4.18 (Ubuntu) Server at practica2.josemagonzalez.es Port 80*

lubuntu [Corriendo] - Oracle VM VirtualBox  
Archivo Máquina Ver Entrada Dispositivos Ayuda

**403 Forbidden - Mozilla Firefox**

403 Forbidden x +

← ⓘ practica2.josemagonzalez.es/carpeta/ ↻ 🔍

## Forbidden

You don't have permission to access /carpeta/ on this server.

---

*Apache/2.4.18 (Ubuntu) Server at practica2.josemagonzalez.es Port 80*