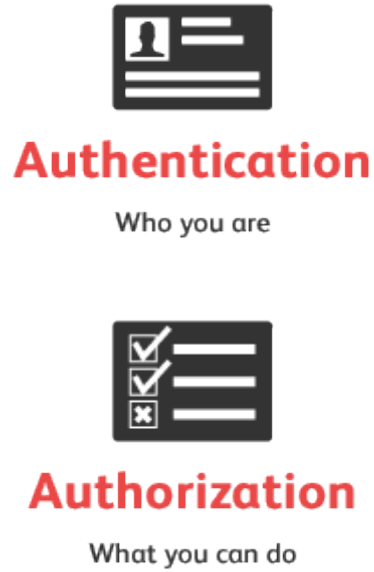
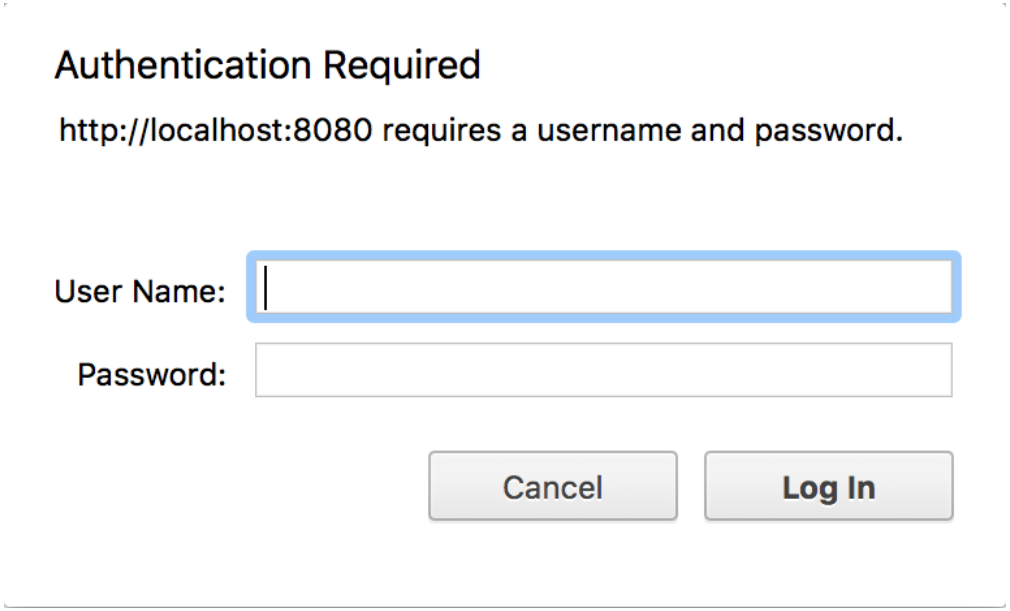
Restricción de acceso. Autenticación y autorización



Autenticar es el proceso de verificar que un usuario es quién dice ser y **autorizar** es el proceso mediante el cual un usuario se le permite o no acceder a un determinado recurso o consultar determinada información. Apache nos permite restringir el acceso a información en nuestra web a un usuario o grupo de usuarios.

Métodos de autenticación



Apache nos permite utilizar dos tipos de autenticación:

- **Autenticación básica**. Utiliza el módulo `mod_auth_basic` que en Ubuntu viene habilitado por defecto. Este tipo de autenticación se caracteriza en que las **credenciales** (nombre de usuario y contraseña) se envían sin cifrar, por lo que si utilizamos este método deberíamos utilizar https en el servidor para evitar que cualquier usuario pueda capturar la información.
- **Autenticación digest**. Utiliza el módulo `mod_auth_digest`. Con este tipo de autenticación se le aplica a las credenciales una función hash para **cifrarlas**.

Uso de autenticación básica

Para almacenar las credenciales de los usuarios debemos crear un fichero en el que almacenar las mismas. Para ello utilizamos la utilidad `htpasswd` que debemos añadir a nuestro sistema instalando el paquete `apache2-utils`:

```
$ sudo apt update
$ sudo apt install apache2-utils
```

La primera vez que usamos la utilidad debemos añadir la opción `-c` para que se cree el fichero:

```
$ sudo htpasswd -c /etc/apache2/.htpasswd user1
```

Al ejecutar el comando anterior se nos solicitará la contraseña para el usuario `user1` y se creará el fichero oculto `/etc/apache2/.htpasswd` y en el mismo se almacenarán las credenciales del usuario.

Una vez añadido el primer usuario, si quisiéramos añadir las credenciales de más usuarios usamos el mismo comando del caso anterior, pero sin la opción `-c`, ya que si la añadiéramos se borraría el contenido anterior del fichero:

```
$ sudo htpasswd /etc/apache2/.htpasswd user2
```

Si consultamos el contenido del fichero vemos que las credenciales se han almacenado cifradas en el mismo:

```
$ sudo cat /etc/apache2/.htpasswd
user1:$apr1$JXMUCYcs$DbEYq7mtqFtOtGGfMOPrh.
user2:$apr1$oxzXWAtX$hIBZu6/TJxoiKBP160EG61
```

Autenticación básica con grupos de usuarios

Podemos autorizar el acceso a usuarios individuales o a **grupos de usuarios**. Para autorizar a grupos de usuarios mediante autenticación básica, aparte de generar las contraseñas de los mismos, hemos de definir grupos de usuario. Para ello creamos un fichero donde almacenarlos y añadimos líneas con el formato:

`nombre_grupo:usuario1 usuario2`

Por ejemplo. Creamos el fichero `/etc/apache2/.htgroups` y añadimos al mismo:

```
alumnos:user1 user2 user3
profesores:profe1 profe2
```

Si vamos a utilizar la autenticación basada en grupos de usuario definidos mediante archivos debemos **habilitar el módulo correspondiente** y reinciar apache para que se apliquen los cambios:

```
$ sudo a2enmod authz_groupfile
$ sudo systemctl restart apache2
```

Uso de autenticación digest

No viene habilitada por defecto, así que deberemos activar el módulo de la misma y reinciar apache:

```
$ sudo a2enmod auth_digest
$ sudo systemctl restart apache2
```

Para crear las credenciales de los usuarios y almacenarlas en un fichero utilizamos en este caso la utilidad `htdigest` a la que además de especificar el fichero y el usuario debemos especificar como parámetro el ámbito o **dominio** al que pertenece el usuario.

Para crear el fichero y añadir un usuario:

```
$ sudo htdigest -c /etc/apache2/.htdigest dominio1 duser1
```

Para crear un segundo usuario ejecutamos:

```
$ sudo htdigest /etc/apache2/.htdigest dominio1 duser2
```

Autorización

Una vez que hemos creado las credenciales de los usuario y/o los grupos a los que pertenecen, podemos restringir el acceso a toda nuestro hosts virtual o a determinadas subcarpetas o archivos a dichos usuarios

Las directivas a utilizar son las siguientes:

Directiva	Descripción	valores
AuthType	Tipo de autenticación de usuarios	Basic Digest
AuthName	Cadena de texto que identifica la zona dominio a utilizar en la autenticación	-
AuthUserFile	Ruta y nombre del fichero que contiene los nombres y claves de los usuarios	-
AuthGroupFile	Ruta y nombre del fichero que contiene el nombre de los grupos de usuarios y los usuarios que conforman ese grupo	-
Require	Indica los nombres de los usuarios, grupos o todos los usuarios a los que se le permite el acceso si proporcionan de forma correcta la contraseña	user, group, valid-user
Satisfy	Como se deben satisfacer las condiciones de control de acceso, todas o alguna	all, any

Ejemplos

1. Autenticación básica en subcarpeta

Para el host virtual `server1.local`, vamos a restringir el acceso a la subcarpeta de nombre `backend`, utilizando `autenticación básica` a un usuario de nombre de `admin`

1. Creamos los archivos y carpetas de nuestro sítio

```
$ sudo mkdir /var/www/server1.local
$ sudo mkdir /var/www/server1.local/backend
$ echo "<h1>acceso libre</h1>" | sudo tee -a /var/www/server1.local/index.html
$ echo "<h1>acceso restringido</h1>" | sudo tee -a /var/www/server1.local/backend/index.html
```

2. Creamos el usuario admin, lo almacenamos en fichero y le asignamos contraseña:

```
$ sudo htpasswd -c /etc/apache2/.htpasswd admin
```

3. Creamos el host virtual, definiendo los parámetros por defecto y restringiendo el acceso a la subcarpeta `backend`. Añadimos el siguiente contenido al fichero `/etc/apache2/sites-available/server1.local.conf`

```
<VirtualHost *:80>
    # Directivas globales del host virtual
    ServerName server1.local
    ServerAlias www.server1.local
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/server1.local
```

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

    #Definimos directivas generales para la carpeta raíz del sitio
    <Directory "/var/www/server1.local">
        DirectoryIndex index.html
    </Directory>

    # Añadimos directivas de restricción de acceso para la subcarpeta backend
    <Directory "/var/www/server1.local/backend">
        AuthType Basic
        AuthName "Administración del sitio"
        AuthUserFile /etc/apache2/.htpasswd
        Require user admin # sólo permitimos acceso al usuario admin
    </Directory>
</VirtualHost>
```

Sólo nos queda habilitar el host virtual y reiniciar apache:

```
$ sudo a2ensite server1.local.conf
$ sudo systemctl restart apache2
```

Y comprobar desde un equipo cliente que podemos acceder si restricciones a `http://server1.local` y que sólo podremos acceder a `http://server1.local/backend` si introducimos las credenciales del usuario `admin`

2. Autenticación básica a dominio completo

Para el host virtual `server2.local`, vamos a restringir el acceso a todo el host virtual, utilizando `autenticación básica` a todos los usuarios para los que hemos creado credenciales

1. Creamos los archivos y carpetas de nuestro sítio

```
$ sudo mkdir /var/www/server2.local
$ echo "<h1>acceso restringido</h1>" | sudo tee -a /var/www/server2.local/index.html
```

2. Creamos dos usuarios, los almacenamos en fichero y les asignamos contraseña:

```
$ sudo htpasswd -c /etc/apache2/.htpasswd_server2 user1
$ sudo htpasswd /etc/apache2/.htpasswd_server2 user2
```

3. Creamos el host virtual, definiendo los parámetros por defecto y restringiendo el acceso a todo el mismo. Añadimos el siguiente contenido al fichero `/etc/apache2/sites-available/server2.local.conf`

```
<VirtualHost *:80>
    # Directivas globales del host virtual
    ServerName server2.local
    ServerAlias www.server2.local
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/server2.local
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    #Definimos directivas generales para la carpeta raíz del sitio y restringimos acceso
```

```
    <Directory "/var/www/server1.local">
        DirectoryIndex index.html
        # Restricción de acceso
        AuthType Basic
        AuthName "Acceso restringido"
        AuthUserFile /etc/apache2/.htpasswd_server2
        Require valid-user # permitimos el acceso a todos los usuarios almacenados
    </Directory>
</VirtualHost>
```

Habilitar el host virtual y reiniciar apache:

```
$ sudo a2ensite server2.local.conf
$ sudo systemctl restart apache2
```

Y comprobar desde un equipo cliente que sólo podremos acceder a `http://server2.local` si introducimos las credenciales de los usuarios `user1` o `user2`

3. Autenticación digest para subcarpeta

Para el host virtual `server3.local`, vamos a restringir el acceso a la subcarpeta `restricted`, utilizando `autenticación digest` a un usuario de nombre `admin`. 1. Creamos los archivos y carpetas de nuestro sítio

```
$ sudo mkdir /var/www/server3.local
$ echo "<h1>acceso permitido</h1>" | sudo tee -a /var/www/server3.local/index.html
$ sudo mkdir /var/www/server3.local/restricted
$ echo "<h1>acceso permitido solo al administrador</h1>" | sudo tee -a /var/www/server3.local/restricted/index.html
```

2. Creamos el usuario `admin`, lo asociomos al dominio `admin_zone`, los almacenamos en fichero y le asignamos contraseña:

```
$ sudo htdigest -c /etc/apache2/.htdigest_server3 admin_zone admin
```

3. Creamos el host virtual, definiendo los parámetros por defecto y restringiendo el acceso a la subcarpeta restricted. Añadimos el siguiente contenido al fichero `/etc/apache2/sites-available/server3.local.conf`

```
<VirtualHost *:80>
    # Directivas globales del host virtual
    ServerName server3.local
    ServerAlias www.server3.local
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/server3.local
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    #Definimos directivas generales para la carpeta raíz del sitio y restringimos acceso
    <Directory "/var/www/server3.local">
        DirectoryIndex index.html
     </Directory>
    <Directory "/var/www/server3.local/restricted">
        # Restricción de acceso
        AuthType Digest
        AuthName "admin_zone"   # Debe coincidir con el nombre de dominio utilizado al crear el usuario
        AuthUserFile /etc/apache2/.htdigest_server3
        Require user admin      # permitimos el acceso solo al usuario admin
```

```
    </Directory>
</VirtualHost>
```

Habilitar el host virtual y el módulo para htdigest y reiniciar apache:

```
$ sudo a2enmod auth_digest
$ sudo a2ensite server3.local.conf
$ sudo systemctl restart apache2
```

Y comprobar desde un equipo cliente que sólo podremos acceder a `http://server3.local/restricted` si introducimos las credenciales del usuario `admin`

4. Autenticación básica para grupo de usuarios en subcarpeta

Para el host virtual `server4.local`, vamos a restringir el acceso a la subcarpeta apuntes, utilizando autenticación básica a los usuarios del **grupo** alumnos.

1. Creamos los archivos y carpetas de nuestro sítio

```
$ sudo mkdir /var/www/server4.local
$ echo "<h1>acceso permitido a la página principal</h1>" | sudo tee -a /var/www/server4.local/index.html
$ sudo mkdir /var/www/server3.local/apuntes
$ echo "<h1>acceso permitido solo a los alumnos</h1>" | sudo tee -a /var/www/server4.local/apuntes/index.html
```

2. Creamos los usuario `alu1` y `alu2` los almacenamos en fichero y le asignamos contraseña:

```
$ sudo htpasswd -c /etc/apache2/.htpasswd_server4 alu1
$ sudo htpasswd /etc/apache2/.htpasswd_server4 alu2
```

3. Creamos el fichero en el que se definen los grupos existentes

```
$ echo "alumnos:alu1 alu2" | sudo tee -a /etc/apache2/.htgroups_server4
```

4. Creamos el host virtual, definiendo los parámetros por defecto y restringiendo el acceso a la subcarpeta `apuntes`. Añadimos el siguiente contenido al fichero `/etc/apache2/sites-available/server4.local.conf`

```
<VirtualHost *:80>
    # Directivas globales del host virtual
    ServerName server4.local
    ServerAlias www.server4.local
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/server4.local
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    #Definimos directivas generales para la carpeta raíz del sitio y restringimos acceso a la subcarpeta apuntes
    <Directory "/var/www/server4.local">
        DirectoryIndex index.html
    </Directory>
    <Directory "/var/www/server3.local/apuntes">
        # Restricción de acceso
        AuthType Basic
        AuthName "Apuntes clase"   # Debe coincidir con el nombre de dominio utilizado al crear el usuario
        AuthUserFile /etc/apache2/.htpasswd_server4
        AuthGroupFile /etc/apache2/.htgroups_server4
        Require group alumnos      # permitimos el acceso solo al usuario admin
```

```
    </Directory>
</VirtualHost>
```

5. Habilitar el host virtual y el módulo para grupos y reiniciar apache:

```
$ sudo a2enmod authz_groupfile
$ sudo a2ensite server3.local.conf
$ sudo systemctl restart apache2
```

Y comprobar desde un equipo cliente que sólo podremos acceder a `http://server4.local/apuntes` si introducimos las credenciales de los usuarios `alu1 y alu2.`