Restricciones por usuarios.

El servidor web Apache tiene muchas maneras de autenticarse: kerberos, pam, radius, mysql, psql... . Yo voy a a explicar las dos mas básicas basic y digest.

Autenticación basic.

Esta autenticación guarda los usuarios y sus contraseña encriptadas en un archivo. Los usuarios y contraseñas se tienen que ir metiendo uno a uno. Este modulo de apache viene activado por defecto. Para utilizarlo en nuestra pagina añadiremos las siguientes lineas al fichero .htaccess.

```
# cat /var/www/prueba/.htaccess
AuthType basic
AuthName "Identifiquese"
AuthUserFile "/etc/apache2/auth_basic"
Require valid-user
```

Bueno estas opciones quieren decir:

1. Le especificamos que es autenticación básica.
2. Este sera el mensaje que nos aparecerá al pedir la contraseña.
3. Esta es la ubicación del fichero con los usuarios y sus contraseñas.
4. Le indicamos que requiere un usuario valido. También se podría poner uno o varios usuarios poniendo por ejemplo "Require user juan, jose, maria".

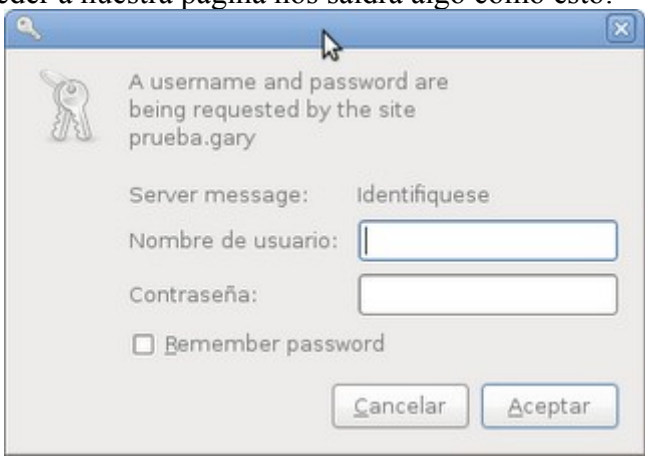
Si queremos combinar este tipo de acceso con el que vimos antes podemos añadirle la opción "Satisfy". Esta puede tener dos valores all/any, para que se tengan que cumplir las dos restricciones utilizaremos "all", para que con que se cumpla una nos baste "any".

Por ultimo, para crear el fichero utilizamos el comando "htpasswd". La primera vez que lo utilicemos tenemos que ponerle la opción -c, para que cree el archivo. Crearíamos el usuario de la siguiente manera:

```
# htpasswd -c /etc/apache2/auth_basic juanlu
New password:
Re-type new password:
```

Como veis nos pedirá la contraseña. Si queremos añadir otro usuario no le pondremos la opción -c.

Si ahora intentamos acceder a nuestra pagina nos saldrá algo como esto:



Autenticación digest.

La autenticación tipo digest soluciona el problema de la transferencia de contraseñas en claro sin necesidad de usar SSL. El procedimiento, como veréis, es muy similar al tipo básico pero cambiando algunas de las directivas y usando la utilidad "htdigest" en lugar de "htpassword" para crear el fichero de contraseñas. El módulo de autenticación necesario suele venir con Apache pero no habilitado por defecto. Para habilitarlo:

```
# a2enmod auth_digest
# /etc/init.d/apache2 restart
```

En este caso el fichero .htaccess nos quedaría así:

```
# cat /var/www/prueba/.htaccess
     AuthType Digest
     AuthName "grupo1"
     AuthUserFile "/etc/apache2/auth_digest"
     Require valid-user
```

En este caso en la primera opción ponemos digest en vez de basic. La directiva AuthName en este caso no especifica el mensaje que nos saldrá, si no el dominio al que pertenecen los usuarios. Este seria mas o menos algo parecido a un grupo. Las otras dos opciones no hace falta que las explique.

En este caso, como dije antes, no se utiliza el comando "htpasswd". Esta vez los usuarios y dominios se agregan de la siguiente manera:

```
# htdigest -c /etc/apache2/auth_digest grupo1 juanlu
Adding password for juanlu in realm grupo1.
New password:
Re-type new password:
```

Si intentamos acceder a nuestra pagina nos saldrá un cartel parecido al anterior.

Cuando estéis comprobando tener cuidado con la cache de los navegadores, pueden hacer que te lleves un rato pensando porque no te pide autenticación.

Por ultimo decir que esto también se puede aplicar a archivos. Si intentamos descargar o ver ese archivo nos pedirá usuario y contraseña. El archivo .htaccess nos quedaría así:

```
# cat /var/www/prueba/.htaccess
<Files "prueba.txt">
AuthType Digest
AuthName "grupo1"
AuthUserFile "/etc/apache2/auth_digest"
Require valid-user
```

</Files>