Prácticas sobre HTTP

Autenticación HTTP en Apache

Contenido

[Configuración de autenticación HTTP 2](#_Toc150511737)

[1. Autenticación HTTP Basic 2](#_Toc150511738)

[2. Autenticación HTTP Digest 4](#_Toc150511739)

# Configuración de autenticación HTTP

**Revisar si Apache está arrancado: systemctl status apache2.**

**Asegurarse que tenemos Apache 2.4 : sudo apachectl -v**

## Autenticación HTTP Basic

Consulta la documentación de ***Apache*** sobre las directivas *AuthName, AuthType, AuthUserFile* y *Require (*[*https://httpd.apache.org/docs/current/mod/quickreference.html*](https://httpd.apache.org/docs/current/mod/quickreference.html)) para comprender su funcionamiento.

* 1. Inicia una sesión en Linux (DespliegueUbuntu).
  2. Comprueba, consultando el directorio **/etc/apache2/mods-enabled**, que el módulo

**auth\_basic.load** está habilitado.



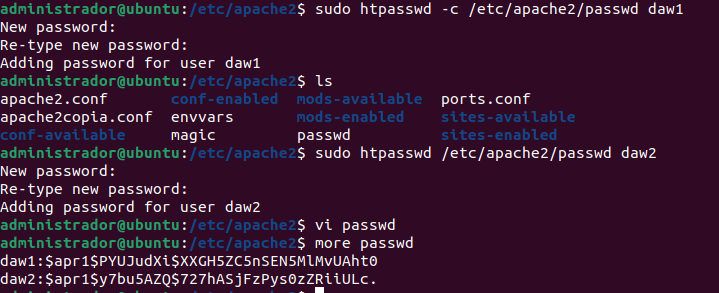
* 1. Para usar la autenticación ***basic*** hay que crear un fichero accesible por *Apache* en el que se guardarán los usuarios y sus contraseñas. Para crear este fichero se utilizará el comando **htpasswd** <https://httpd.apache.org/docs/2.4/programs/htpasswd.html>

1. Crea el fichero y añade el usuario *daw1* (la opción -c es para crear el fichero).

sudo htpasswd -c /etc/apache2/passwd daw1

1. Añade el usuario *daw2* (no se usa la opción -c porque el fichero ya existe).

sudo htpasswd /etc/apache2/passwd daw2

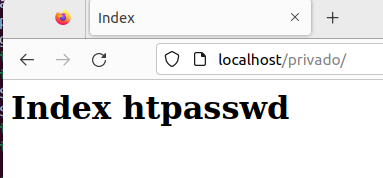
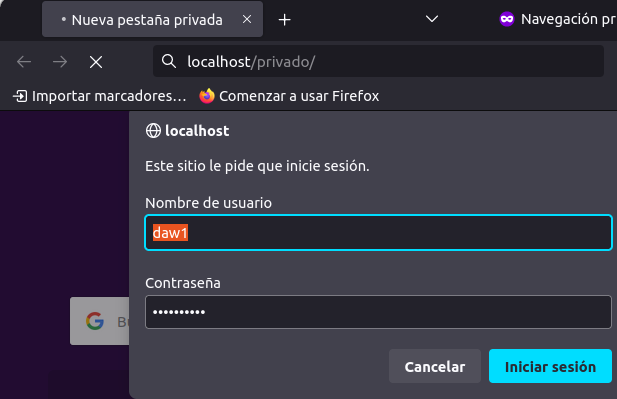


* 1. Crea el directorio **/var/www/html/privado** y un archivo **index.html** con el contenido que quieras.
  2. Edita el fichero de configuración **/etc/apache2/sites-available/000-default.conf** y permite el acceso al directorio **/var/www/html/privado** a los usuarios ***daw1*** y ***daw2***.



* 1. Reinicia el servidor para que los cambios tengan efecto. systemctl restart apache2
  2. Accede a [*http://ServidorHTTP/privado/*](http://servidorhttp/privado/) con el usuario *daw1, 2*. Intenta el acceso con otro usuario.

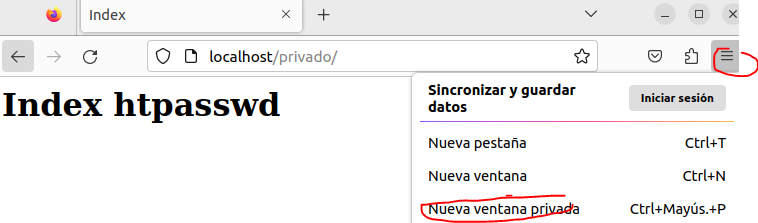
¿ Es posible ?.



Si por defecto queda autenticado el usuario

<https://support.mozilla.org/es/kb/limpia-la-cache-y-elimina-los-archivos-temporales-#w_limpiar-la-cache>

o nueva ventana privada



## Autenticación HTTP Digest

[*https://www.zeppelinux.es/autenticacion-digest-en-apache/*](https://www.zeppelinux.es/autenticacion-digest-en-apache/)

El método **Digest** es más seguro sobre todo a nivel de posible captura de tráfico, ya que el intercambio de **hashes** entre nuestro navegador y el servidor es más complejo. La codificación va en base al **timestamp** generado por el servidor en el momento de la petición, lo que lo hace más difícil de decodificar y por lo tanto más seguro.

* 1. Crea un directorio ***/var/www/html/departamento***. Dentro del directorio crea un fichero denominado

***index.html*** con el contenido que quieras.

* 1. Habilita el módulo auth\_digest. **sudo a2enmod auth\_digest**

Es lo mismo que si se hubiera realizado

sudo ln -s /etc/apache2/mods-available/auth\_digest.load /etc/apache2/mods-enabled/auth\_digest.load

Comprueba que su link ya aparece en el directorio mods-enabled

* 1. Reinicia el servidor para que los cambios tengan efecto. systemctl restart apache2
  2. Para usar la autenticación ***digest*** hay que crear un fichero accesible por *Apache* en el que se guardarán los usuarios y sus contraseñas asociados a un “grupo/dominio/realm”, en nuestro caso informatica. Para crear este fichero se utilizará el comando ***htdigest:***

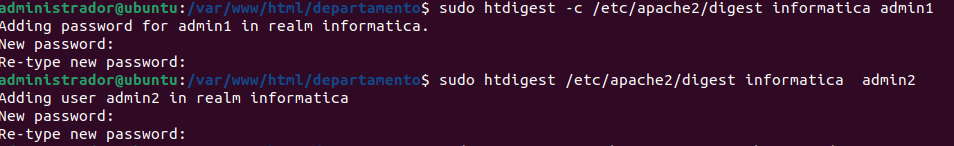
<https://httpd.apache.org/docs/2.4/programs/htdigest.html>

* + 1. Crea el fichero y añade el usuario ***admin1*** al dominio ***informatica*** (la opción -c es para crear el fichero).

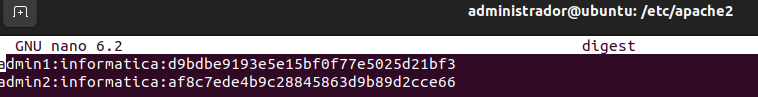
sudo htdigest -c /etc/apache2/digest informatica admin1

* + 1. Añade el usuario ***admin2*** (no se usa la opción -c porque el fichero ya existe).

sudo htdigest /etc/apache2/digest informatica admin2



El fichero digest habrá quedado de la siguiente forma



El archivo deberá tener los siguientes propietarios y permisos: Si el servidor está configurado para correr como usuario www-data y como grupo www-data, el **usuario root** podrá leerlo y escribirlo, el grupo www-data sólo leerlo y prohibido para el **resto.**

Para conocer el usuario y grupo asignados a [Apache](https://httpd.apache.org/), podremos comprobarlo en el archivo: /etc/apache2/envvars en el que aparecerá algo como sigue:

|  |
| --- |
| export APACHE\_RUN\_USER=www-data  export APACHE\_RUN\_GROUP=www-data |

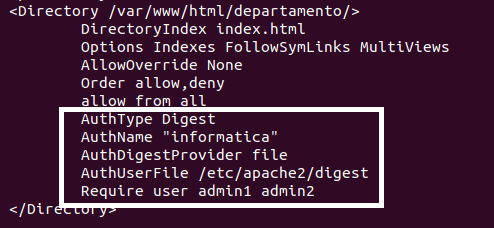
Para asignar los **permisos**, ejecutaremos el siguiente comando:

|  |
| --- |
| $ sudo chmod 640 /etc/apache2/digest |

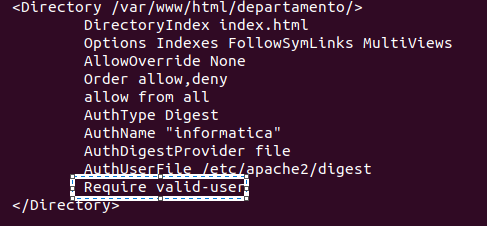
Para asignar **propietario** y **grupo** utilizaremos el siguiente comando:

|  |
| --- |
| $ sudo chown root.www-data /etc/apache2/digest |

* 1. Edita el fichero de configuración **/etc/apache2/sites-available/000-default.conf** y permite el acceso al directorio ***/var/www/html/departamento*** a los usuarios ***admin1*** y ***admin2***



En la directiva **Require** podremos optar por especificar los usuarios que accederán al recurso como en el ejemplo anterior o bien, indicar la opción **valid-user** como se indica a continuación. Con esta opción le decimos a **Apache** que podrán acceder todos los usuarios que pertenezcan al **realm «informatica»**



* 1. Reinicia el servidor para que los cambios tengan efecto. sytemctl restart apache2
  2. Sccede a [*http://ServidorHTTP/departamento*](http://servidorhttp/departamento/)con el usuario *admin1*, admin*2*. Intenta el acceso con otro usuario. ¿ Es posible ?.

