**Pràctica 2d: Mecanismes d'autenticació i autorització. Realms.**

# 1- Introducció

L'objectiu de la pràctica és fer un breu estudi dels mecanismes [**d'autenticació i autorització**](http://httpd.apache.org/docs/2.2/howto/auth.html) del servidor de pàgines web Apache2.

El mecanisme d'**autenticació** permet demanar a un usuari que vol accedir a un recurs del servidor un **nom** **d'usuari i una contrasenya** i d'aquesta manera es pot confirmar l'identitat de l'usuari, o en altres paraules,verificar que un usuari és realment qui afirma ser. La llista d'usuaris i les seves contrasenyes es desen en un **proveïdor d'autenticació**, que és un fitxer de texte o una base de dades SQL o LDAP.

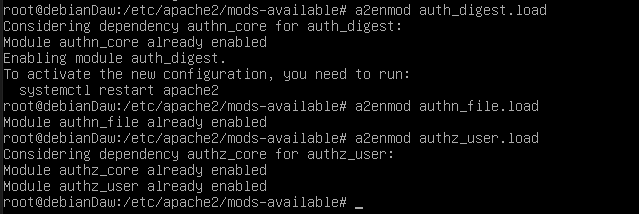
El mecanisme d'**autorització** és un procés pel qual es dóna a un usuari els permisos necessaris per accedir als recursos disponibles en el servidor. Per donar permisos, s'utilitza un sistema de [**llistes de**](http://httpd.apache.org/docs/2.2/howto/access.html) [**control d'accés ACL**](http://httpd.apache.org/docs/2.2/howto/access.html) alsdiferents recursos del servidor, com per exemple un directori, un fitxer o una basede dades.

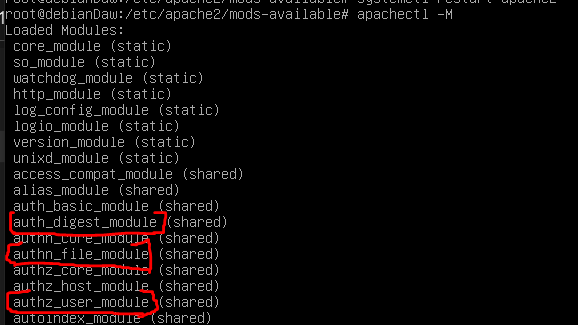
Un conjunt de recursos els quals es troben sota el control dels mateixos mecanismes d'autenticació i autorització, i que fa servir el mateix proveïdor d'autenticació conformen un **realm**. Un **realm** necessita un **nom de realm** per ser identificat.

Per poder implementar aquests mecanismes d'autenticació i autorització cal que el servidor Apache2 tingui habilitats una sèrie de mòduls. Els tres tipus de mòduls necessaris són els següents:

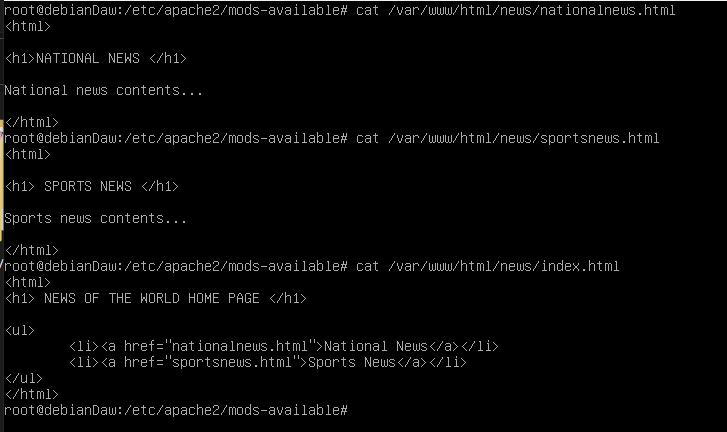
1. S'ha d'habilitar com a mínim un **mòdul d'autenticació**, que indica el tipus d'autenticació utilitzada. Existeixen dos mètodes autenticació. Primer hi ha el [**mètode bàsic**](https://en.wikipedia.org/wiki/Basic_access_authentication), a on els noms d'usuaris i contrasenyes son enviats dins d'una capçalera HTTP sense encriptar les dades (tot i que estiguin codificades amb el sistema [**base64**](https://en.wikipedia.org/wiki/Base64), que és facilment [**reversible**](http://www.motobit.com/util/base64-decoder-encoder.asp)). Per activar-lo cal tenir habilitat el mòdul **mod\_auth\_basic**. El segon, és el [**mètode digest**](https://en.wikipedia.org/wiki/Digest_access_authentication) que proporciona confidencialitat aplicant al nom d'usuari i contrasenya l'algorisme **MD5**, que és una [**funció hash criptogràfica**](https://en.wikipedia.org/wiki/Cryptographic_hash_function), que produeix un valor **hash** de 128 bits. Per activar-lo cal tenir habilitat el mòdul **mod\_auth\_digest**.
2. S'ha d'habilitar com a mínim un mòdul per indicar el **proveïdor d'autenticació**. Per defecte està habilitat el mòdul **mod\_authn\_file** que permet desar la llista d'usuaris i contrasenyes dins d'un fitxer de texte pla. Altres mòduls són per exemple **mod\_authn\_dbd** per desar la llista en una base de dades SQL o **mod\_authn\_ldap** per desar la llista en una base de dades LDAP.
3. S'ha d'habilitar com a mínim un mòdul d'**autorització** que proporciona el mecanisme per permetre que els usuaris autenticats se'ls doni o denegui el permís per accedir als diversos recursos del servidor per mitjà de **llistes de control d'accés**. Alguns d'aquests mòduls són per exemple: **mod\_authz\_user, mod\_authz\_host**, **mod\_authz\_dbm** o **mod\_authz\_ldap**.

**2- Configurant Apache2 per accedir a un realm amb el mecanisme d'autenticació digest, proveïdor d'autorització de tipus *file* i autorització de tipus** ***user***

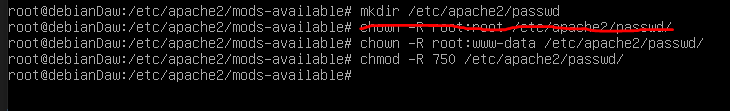
1.  Amb l'ordre **apachectl -M**, verifica que els mòduls **auth\_digest\_module**, **authn\_file\_module** i **authz\_user\_module** estan instal·lats i habilitats.En cas negatiu, comprova si tens aquest mòdul disponible a **/etc/apache2/mods-available**, i habilita'l amb l'ordre **a2enmod**.



1. Crea un directori de nom **news** dins del directori **/var/www/html**. Descarrega dins del directori **/var/www/html/news** el fixer **news.tar.gz** que trobaràs a[***aquest enllaç***](https://www.dropbox.com/s/xh4eqjvjj16rmtf/news.tar.gz).Extreu el seu contingut. Comprovaque has obtingut els següents fitxers: **index.html**, **sportsnews.html** i **nationalnews.html**. Esborra el fitxer descarregat (només has de tenir els fitxers **.html**).



1. Crea un directori de nom **passwd** dins del directori **/etc/apache2**. Fes que el propietari del directori **/etc/apache2/passwd/** (i tots els fitxers inclosos) sigui **root** i que el grup amb permisos especials sigui **www-data**. Dóna permisos **rwx** a root, **r-x** a www-data i **- - -** a la resta d'usuaris.

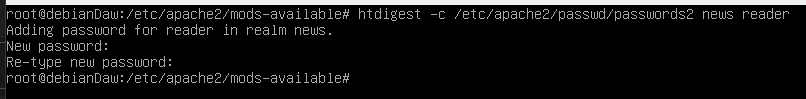


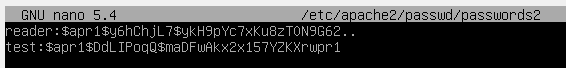
1. Crea un fitxer **proveïdor d'autenticació** de nom **passwords2** dins del directori **/etc/apache2/passwd** i que tingui definit a l'usuari **reader** amb contrasenya **fjeclot00** i autorització d'accés al realm **news**.

Per dur a terme aquesta tasca, s'ha d'utilitzar l'eina **htpdigest**. Per crear l'usuari **reader** i generar el fitxer **passwords2** d'acord amb l'enunciat, has d'executar:

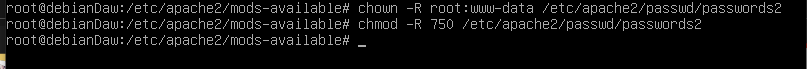
**htdigest ­-c /etc/apache2/passwd/passwords2 news reader**

**NOTA:** Si vols afegir un nou usuari a un fitxer proveïdor d'autenticació que ja existeix, **NO** s'ha de posarl'opció **-c**.





* 1. Fes que el propietari del fitxer **/etc/apache2/passwd/passwords2** sigui **root** i que el grup amb permisos especials sigui **www-data**. Dóna permisos **rwx** a root, **r-x** a **www-data** i **- - -** a la resta d'usuaris.



**chown root**

**chgrp www-data**

**chmod 750**

* 1. Fes una còpia de seguretat de **000-default.conf** que es troba dins de **/etc/apache2/sites-available** amb el nom **000-default.conf.original**.



* 1. Descarrega dins de **/etc/apache2/sites-available** una nova versió de **000-default.conf** que trobaràs en [**aquest enllaç**](https://www.dropbox.com/s/rieacwkjqk94ssz/000-default.conf).Fes els canvis necessaris dins de l'arxiu perquè la configuració final sigui:

**1-** Directori del realm: **/var/www/html/news**

**2-** Autenticació: **Digest**

**3-** Nom del realm: **“news”**

**4-** Tips de proveïdor d'autenticació: **file**

**5-** Fitxer proveïdor d'utenticació: **etc/apache2/passwd/passwords2**

**6-** Per accedir al realm, s'ha de ser l'usuari **reader**.



1. Reinicia el servidor **apache2** executant **systemctl restart apache2**.



1. Intenta accedir als recursos que es troben a **/var/www/html/news** i comprova que **reader** pot accedir al realm **news**. amb la contrasenya correcta. Comprova que qualsevol altre nom d'usuari o l'usuari reader amb la contrasenya incorrecta no pot accedir al realm **news**.fje

Si s’insertreixes un altre usuari o un altre constrasenya, la pagina tornara a pedir iniciar sessió. Si no mostrara la pagina:

