

## LDAP

Per proseguir la instal·lació de LDAP hem de executar aquesta comanda que permetrà instal·lar el LDAP en el servidor:

```
root@server:/home/daw# sudo apt-get install slapd ldap-utils
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
 libodbc1 psmisc
Paquetes sugeridos:
 libsasl2-modules-gssapi-mit | libsasl2-modules-gssapi-heimdal libmyodbc
 odbc-postgresql tdsodbc unixodbc-bin
Se instalarán los siguientes paquetes NUEVOS:
 ldap-utils libodbc1 psmisc slapd
```

Inclus ens mostrara amb slapcat que no hi ha domini:

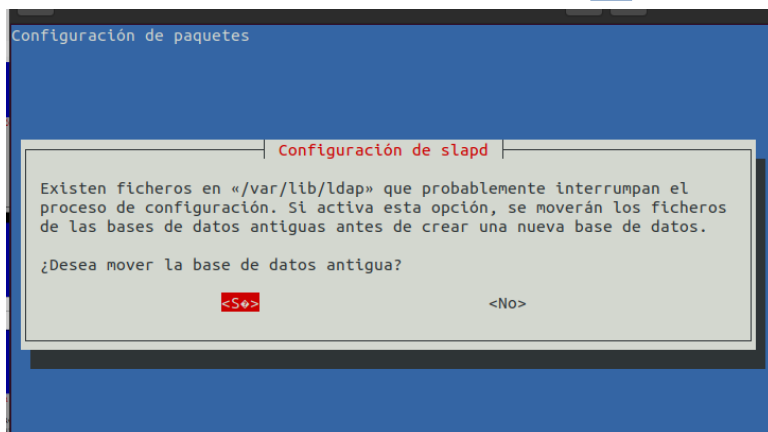
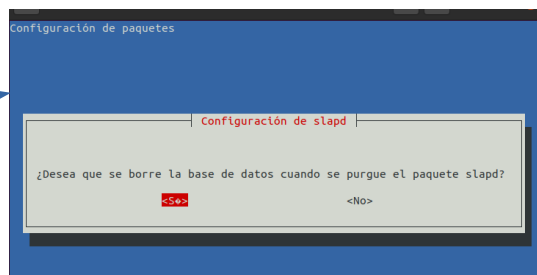
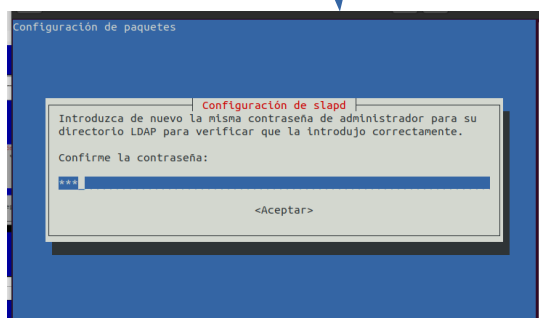
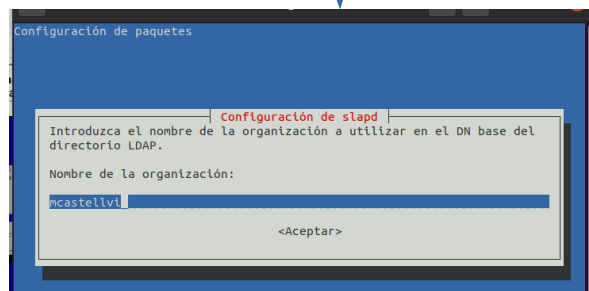
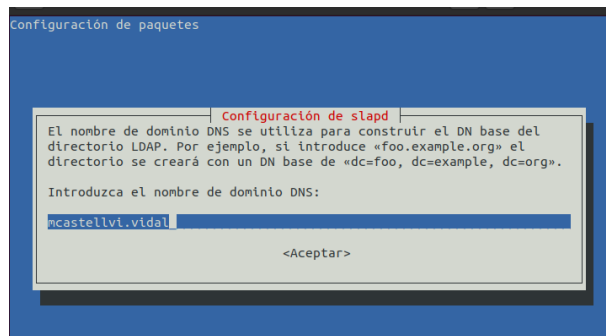
```
root@serverLDAP:/home/daw# slapcat
dn: dc=nodomain
objectClass: top
objectClass: dcObject
objectClass: organization
o: nodomain
dc: nodomain
structuralObjectClass: organization
entryUUID: a5727204-3e5b-103c-95fb-a973128eb6d7
creatorsName: cn=admin,dc=nodomain
createTimestamp: 20220322184301Z
entryCSN: 20220322184301.632603Z#000000#000#000000
modifiersName: cn=admin,dc=nodomain
modifyTimestamp: 20220322184301Z

root@serverLDAP:/home/daw#
```

Per configurar el LDAP en el servidor executarem aquesta comanda:

```
root@server:/home/daw# dpkg-reconfigure slapd
Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.4.57+dfsg-3... done.
Moving old database directory to /var/backups:
- directory unknown... done.
Creating initial configuration... done.
Creating LDAP directory... done.
root@server:/home/daw#
```

I ara ens mostrara diversos passos de configuració, afegirem a medida del servidor:



Ara podem observar que amb slapcat podem mostrar que el domini està ben configurat:

```
root@server:/home/daw# slapcat
dn: dc=mcastellvi,dc=vidal
objectClass: top
objectClass: dcObject
objectClass: organization
o: mcastellvi
dc: mcastellvi
structuralObjectClass: organization
entryUUID: 8dc29f58-3ae1-103c-9718-0f39f0c62f88
creatorsName: cn=admin,dc=mcastellvi,dc=vidal
createTimestamp: 20220318083129Z
entryCSN: 20220318083129.803365Z#000000#000#000000
modifiersName: cn=admin,dc=mcastellvi,dc=vidal
modifyTimestamp: 20220318083129Z
root@server:/home/daw#
```

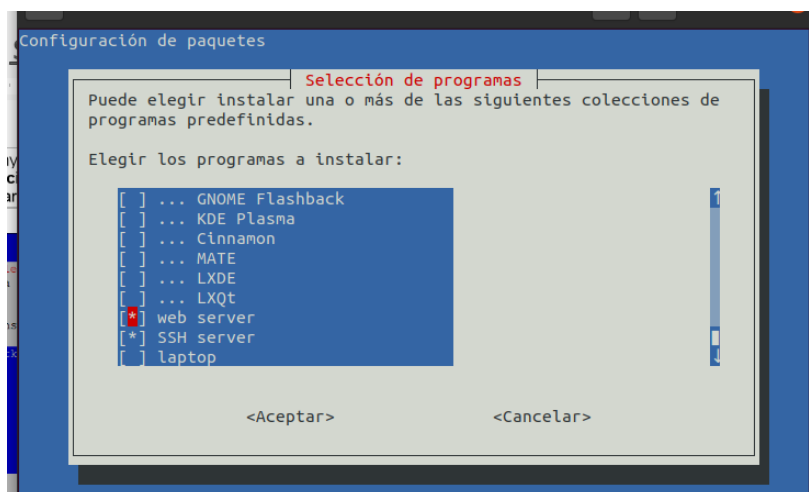
E inclús mostrar per buscador exactament:

```
root@server:/home/daw# ldapsearch -x -b dc=mcastellvi,dc=vidal
# extended LDIF
#
# LDAPv3
# base <dc=mcastellvi,dc=vidal> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# mcastellvi.vidal
dn: dc=mcastellvi,dc=vidal
objectClass: top
objectClass: dcObject
objectClass: organization
o: mcastellvi
dc: mcastellvi

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
root@server:/home/daw#
```

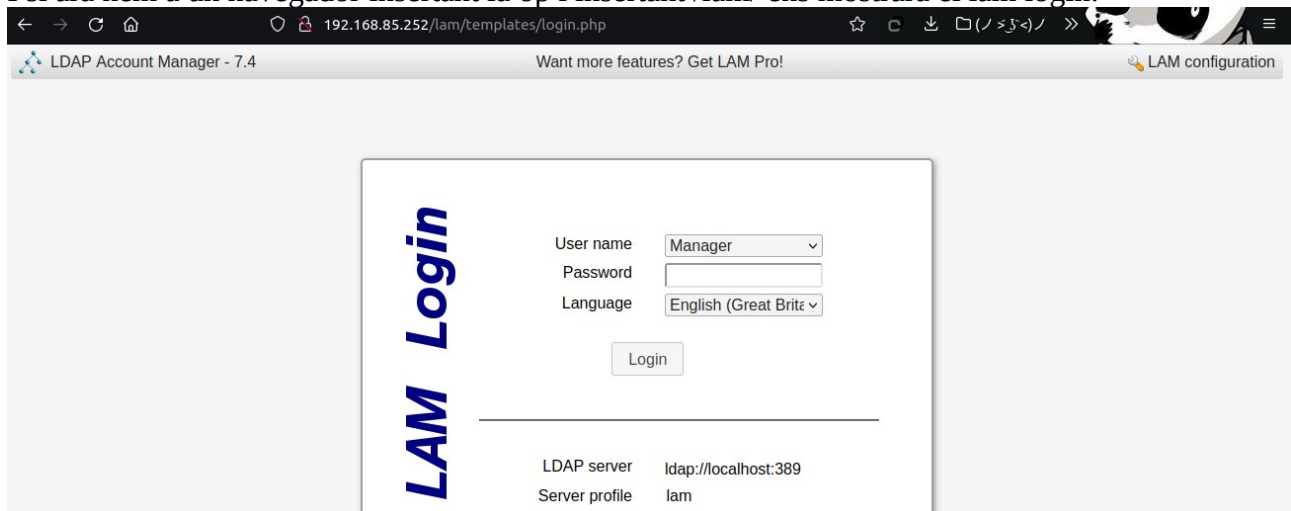
Ara amb tasksel podrem inserir un webserver:



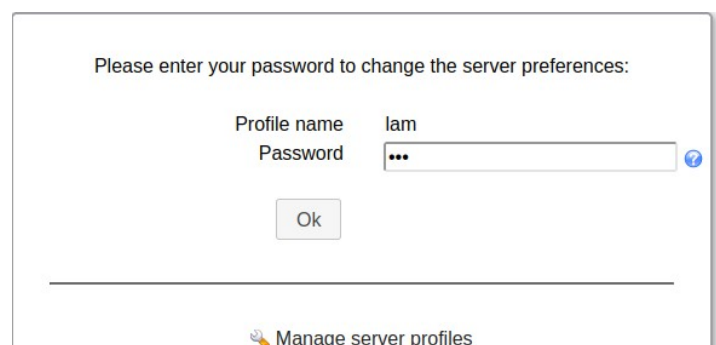
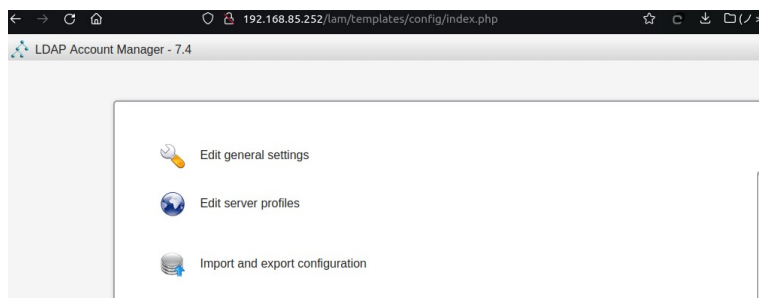
Ara crearem el client de lam en el webserver amb aquesta comanda:

```
root@server:/home/daw# sudo apt-get install ldap-account-manager
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
 fonts-dejavu libapache2-mod-php7.4 libsodium23 libxslt1.1 libzip4 php
 php-common php-curl php-gd php-gmp php-ldap php-monolog php-phpseclib
 php-psr-log php-xml php-zip php7.4 php7.4-cli php7.4-common php7.4-curl
 php7.4-gd php7.4-gmp php7.4-json php7.4-ldap php7.4-opcache php7.4-readline
 php7.4-xml php7.4-zip
Paquetes sugeridos:
 php-mcrypt ldap-account-manager-lamdaemon php-pear php-graylog2-gelf-php
 php-sentry php-doctrine-couchdb php-rufin-elastica php-amqplib php-amqp
 php-mongo php-mongodb php-aws-sdk php-rollbar php-console php-libsodium
Se instalarán los siguientes paquetes NUEVOS:
 fonts-dejavu ldap-account-manager libapache2-mod-php7.4 libsodium23
 libxslt1.1 libzip4 php php-common php-curl php-gd php-gmp php-ldap
 php-monolog php-phpseclib php-psr-log php-xml php-zip php7.4 php7.4-cli
 php7.4-common php7.4-curl php7.4-gd php7.4-gmp php7.4-json php7.4-ldap
 php7.4-opcache php7.4-readline php7.4-xml php7.4-zip
0 actualizados, 29 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 24,3 MB de archivos.
Se utilizarán 89,6 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

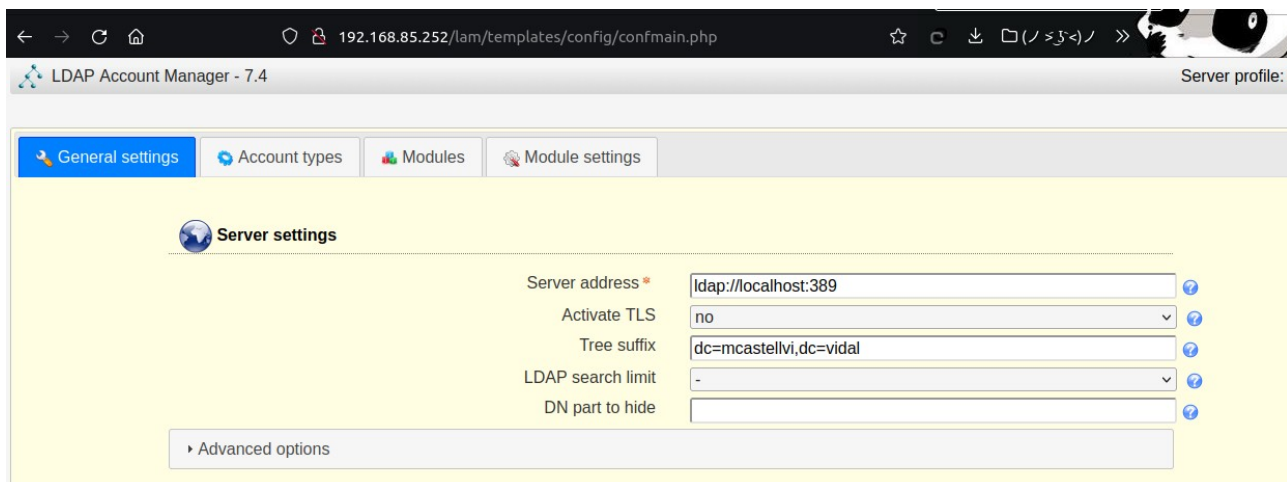
I si ara nem a un navegador insertant la op i insertant /lam/ ens mostrara el lam login:



Ara anirem a «LAM configuration» → Edit server profiles → USER: lam PASSW: lam →



Ara podrem configurar el server, en el tree suffix podrem insertar el nostre domini:



LDAP Account Manager - 7.4

Server profile: I

General settings | Account types | Modules | Module settings

**Server settings**

Server address \*

Activate TLS

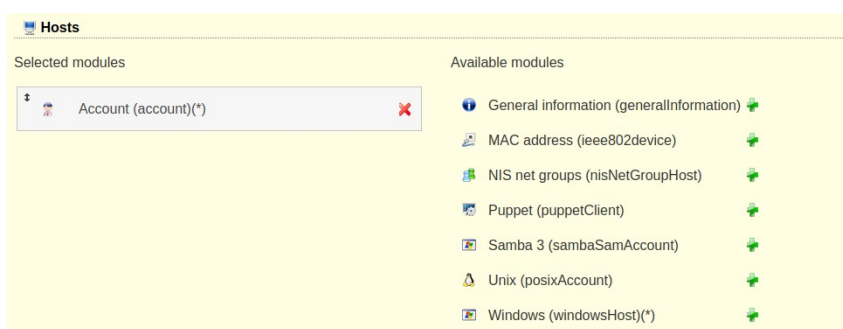
Tree suffix

LDAP search limit

DN part to hide

Advanced options

En hosts afegirem account:



**Hosts**

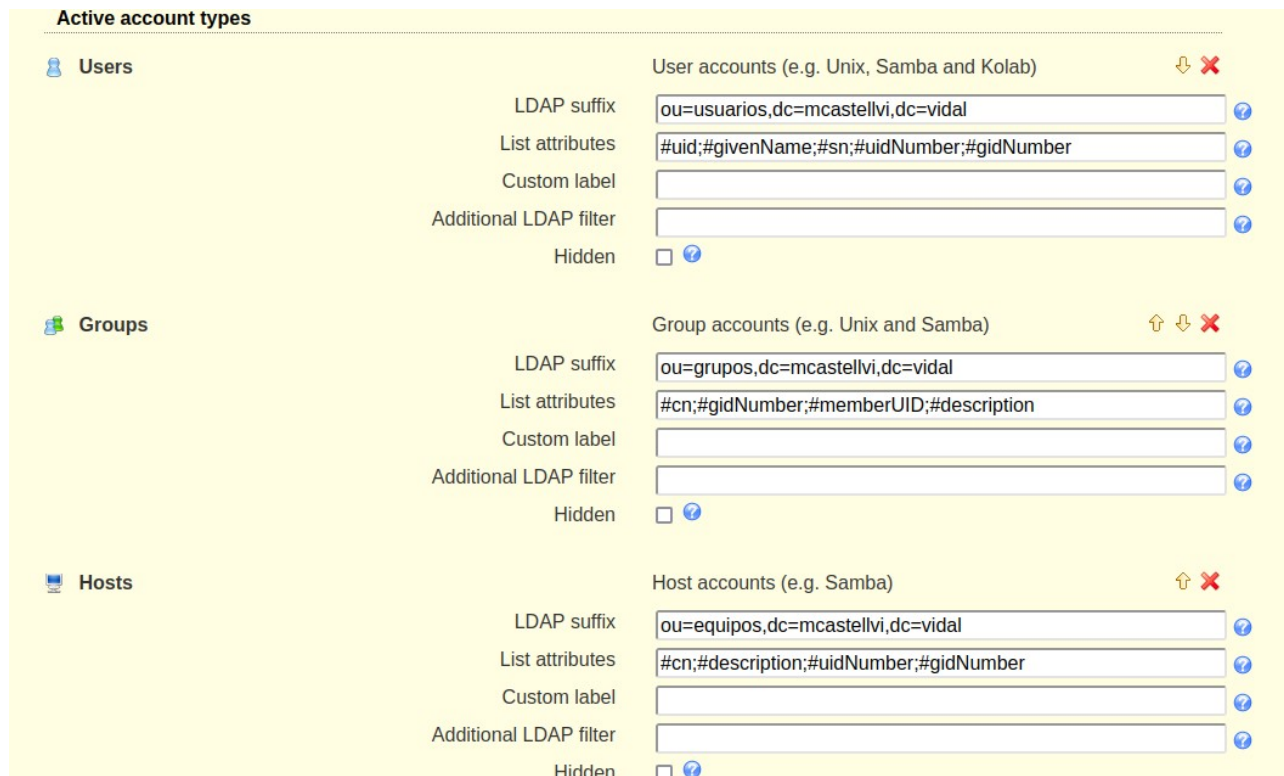
Selected modules

- Account (account)(\*)

Available modules

- General information (generalInformation)
- MAC address (ieee802device)
- NIS net groups (nisNetGroupHost)
- Puppet (puppetClient)
- Samba 3 (sambaSamAccount)
- Unix (posixAccount)
- Windows (windowsHost)(\*)

Ara podrem insertar les dades de usuaris, grups i hosts.



**Active account types**

**Users**

User accounts (e.g. Unix, Samba and Kolab)

LDAP suffix

List attributes

Custom label

Additional LDAP filter

Hidden ☐

**Groups**

Group accounts (e.g. Unix and Samba)

LDAP suffix

List attributes

Custom label

Additional LDAP filter

Hidden ☐

**Hosts**

Host accounts (e.g. Samba)

LDAP suffix

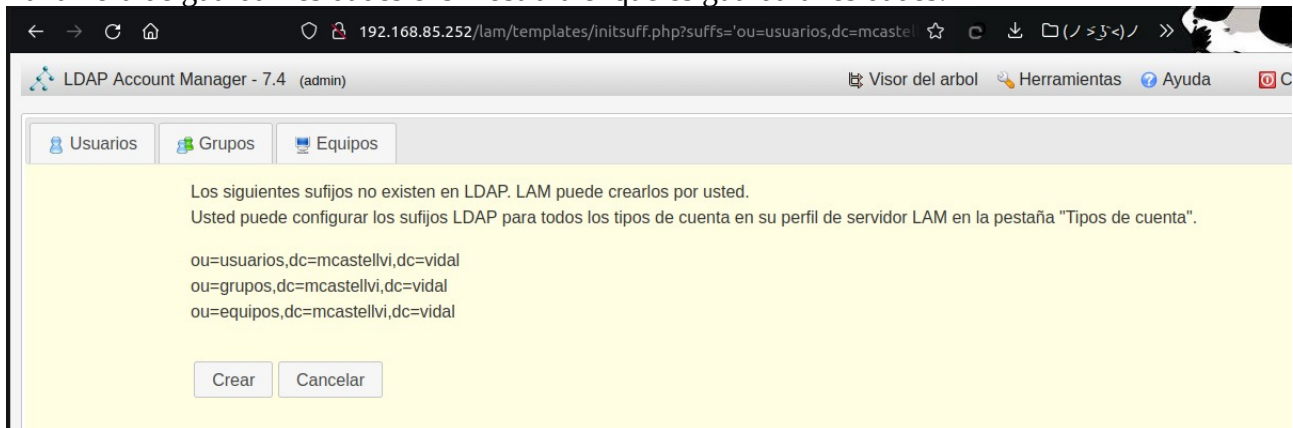
List attributes

Custom label

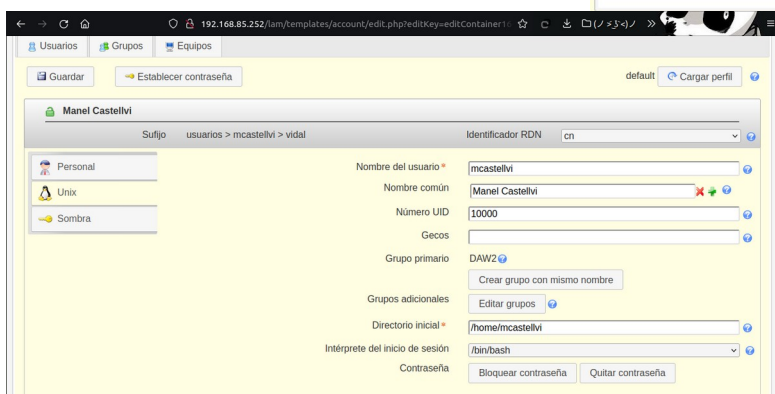
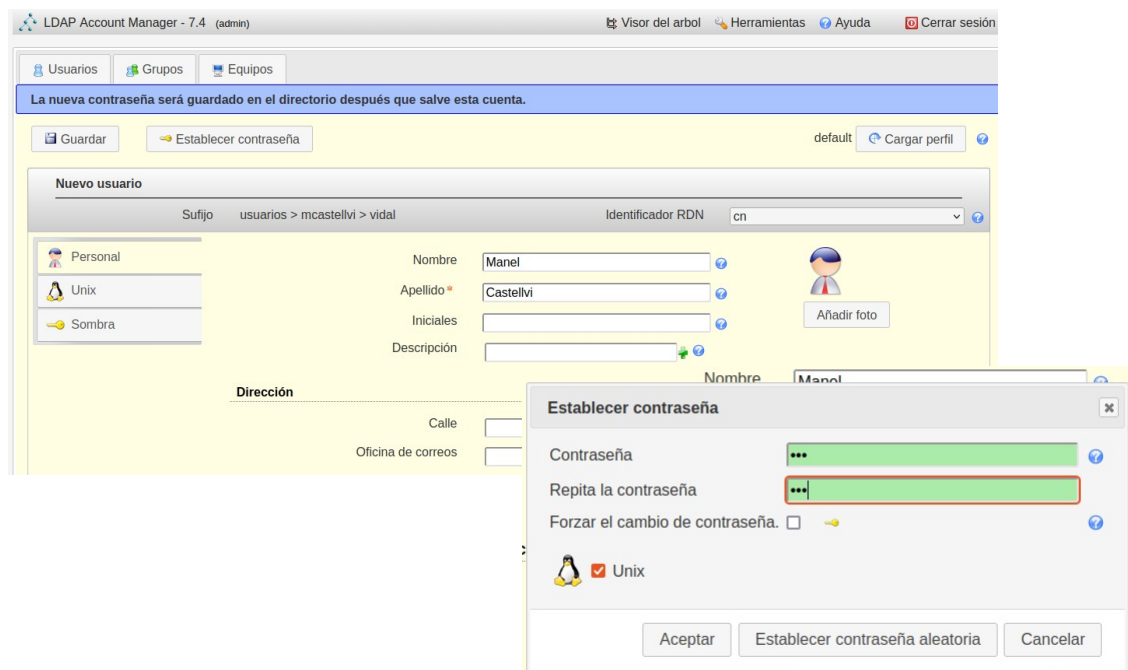
Additional LDAP filter

Hidden ☐

I a la hora de guardar les dades ens mostrara el que es guardarà les dades:



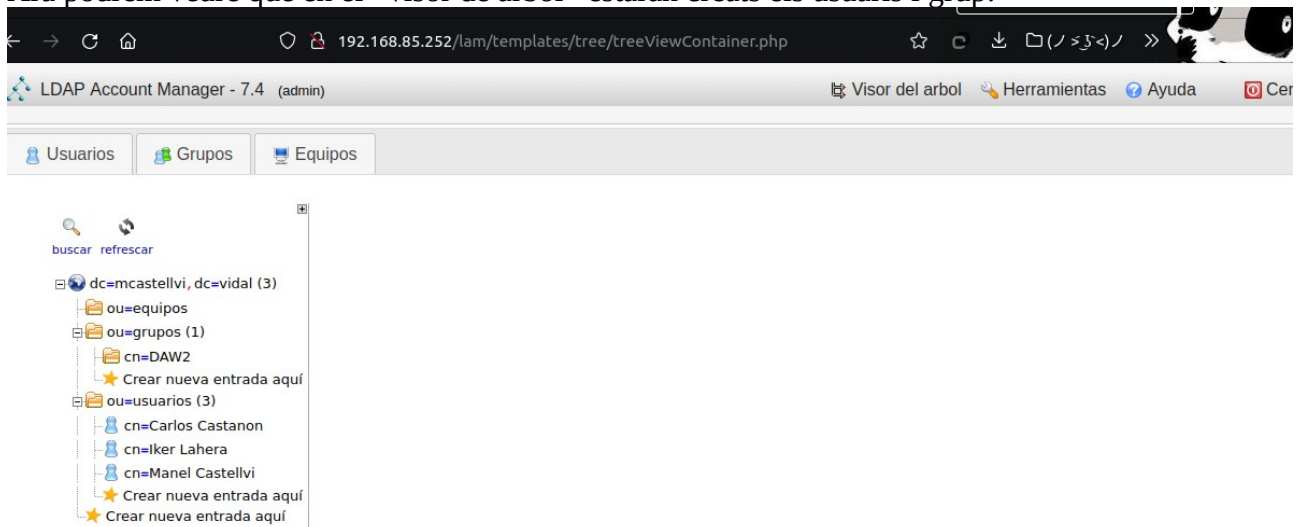
Ara podem crear els grups i usuaris:



I en unix en el usuari ens mostrara que esta en el grup adequat:



Ara podrem veure que en el «visor de arbol» estaran creats els usuaris i grup:



Pero ara per crear un grup amb un arxiu ldif hem d'escriure això:

```
root@serverLDAP:/home/daw# ls
superherois.ldif
root@serverLDAP:/home/daw# cat superherois.ldif
# Nou grup de superherois
dn: cn=superherois,ou=grupos,dc=mcastellvi,dc=vidal
objectClass: top
objectClass: posixGroup
gidNumber: 10001
root@serverLDAP:/home/daw#
```

I ara amb aquesta comanda s'executara la comanda per crear el grup:

```
root@serverLDAP:/home/daw# ldapadd -x -W -D "cn=admin,dc=mcastellvi,dc=vidal" -f
superherois.ldif
Enter LDAP Password:
adding new entry "cn=superherois,ou=grupos,dc=mcastellvi,dc=vidal"
root@serverLDAP:/home/daw#
```

I per crear un usuari amb un arxiu ldif es farà així:

```
root@serverLDAP:/home/daw# cat ironman.ldif
dn: cn=ironman,ou=usuarios,dc=mcastellvi,dc=vidal
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: ironman
uid: ironman
uidNumber: 10003
gidNumber: 10001
homeDirectory: /home/ironman
loginShell: /bin/bash
gecos: ironman
userPassword: iron
shadowLastChange: 0
shadowMax: 0
shadowWarning: 0
root@serverLDAP:/home/daw# ldapadd -x -W -D "cn=admin,dc=mcastellvi,dc=vidal" -f
ironman.ldif
Enter LDAP Password:
adding new entry "cn=ironman,ou=usuarios,dc=mcastellvi,dc=vidal"
root@serverLDAP:/home/daw#

root@serverLDAP:/home/daw# cat hulk.ldif
dn: cn=hulk,ou=usuarios,dc=mcastellvi,dc=vidal
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: Hulk
#sn: Banner
uid: hulk
uidNumber: 10004
gidNumber: 10001
homeDirectory: /home/hulk
loginShell: /bin/bash
gecos: hulk
userPassword: hulk
shadowLastChange: 0
shadowMax: 0
shadowWarning: 0
root@serverLDAP:/home/daw# ldapadd -x -W -D "cn=admin,dc=mcastellvi,dc=vidal" -f
hulk.ldif
Enter LDAP Password:
adding new entry "cn=hulk,ou=usuarios,dc=mcastellvi,dc=vidal"
root@serverLDAP:/home/daw#
```

I en el tree es mostrà així i també comprovaré que els usuaris estan el el grup:

The screenshot shows the LDAP Account Manager 7.4 web interface. On the left, a tree view displays the directory structure: `dc=mcastellvi,dc=vidal (3)` containing `ou=equipos`, `ou=grupos (2)` (with `cn=DAW2` and `cn=superherois`), and `ou=usuarios (5)` (containing `cn=Carlos Castanon`, `cn=hulk`, `cn=Iker Lahera`, `cn=ironman`, and `cn=Manel Castellvi`). The right panel shows the configuration for the `cn=ironman` user. Fields include: `cn` (required, `rdn`), `gecos` (text input with `ironman`), `gidNumber` (required, `superherois ()`), and `homeDirectory` (required, `/home/ironman`).

I ara configurarem el client per que estigui enllaçat insertant en aquest arxius la ip del servidor:

```
GNU nano 4.8 /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
# Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d

auto enp0s3
iface enp0s3 inet static interface
address 192.168.85.208
netmask 255.255.255.0
gateway 192.168.85.1
dns-nameservers 192.168.85.208 8.8.8.8
```

```
root@vib2022: /home/vib
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 4.8 /etc/hostname
cliente08
```

```
GNU nano 4.8 /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not
#
# This is a dynamic resolv.conf file for connecting local
# internal DNS stub resolver of systemd-resolved. This fi
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink
# currently in use.
#
# Third party programs must not access this file directly
# symlink at /etc/resolv.conf. To manage man:resolv.conf(
# replace this symlink by a static file or a different sy
#
# See man:systemd-resolved.service(8) for details about t
# operation for /etc/resolv.conf.
nameserver 192.168.85.208
nameserver 192.168.85.252
nameserver 8.8.8.8
search vib
```



I ara amb la comanda «**apt-get install libnss-ldap libpam-ldap ldap-utils**» podrem configurar el client per enllaçar-lo amb ldap:

```
root@vib2022:/home/vib# apt-get install libnss-ldap libpam-ldap ldap-utils
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  ldap-auth-client ldap-auth-config
Paquetes sugeridos:
  libsassl2-modules-gssapi-mit | libsassl2-modules-gssapi-heimdal nscd
Se instalarán los siguientes paquetes NUEVOS:
  ldap-auth-client ldap-auth-config ldap-utils libnss-ldap libpam-ldap
0 actualizados, 5 nuevos se instalarán, 0 para eliminar y 175 no actualizados.
Se necesita descargar 231 kB de archivos.
Se utilizarán 1.099 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://es.archive.ubuntu.com/ubuntu focal-updates/main amd64 ldap-utils amd64 2.4.49+dfsg-1 [122 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 ldap-auth-config all 0.5.4 [9.0 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 libpam-ldap amd64 186-4ubuntu1 [8,6 kB]
Des:4 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 libnss-ldap amd64 265-5ubuntu1 [122 kB]
```

Archivo Editar Ver Buscar Terminal Ayuda  
Configuración de paquetes

#### Configuración de ldap-auth-config

Please enter the URI of the LDAP server to use. This is a string in the form of ldap://<hostname or IP>:<port>/. ldaps:// or ldapi:// can also be used. The port number is optional.

Note: It is usually a good idea to use an IP address because it reduces risks of failure in the event name service problems.

LDAP server Uniform Resource Identifier:

ldap://192.168.85.252

<Aceptar>

root@vib2022:/home/vib  
Archivo Editar Ver Buscar Terminal Ayuda  
Configuración de paquetes

#### Configuración de ldap-auth-config

Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.com" would use "dc=example,dc=com" as the distinguished name of the search base.

Distinguished name of the search base:

dc=mcastellvi,dc=vidal

<Aceptar>

root@vib2022:/home/vib  
Archivo Editar Ver Buscar Terminal Ayuda  
Configuración de paquetes

#### Configuración de ldap-auth-config

Please enter which version of the LDAP protocol should be used by ldapns. It is usually a good idea to set this to the highest available version.

LDAP version to use:

3

2

<Aceptar>

root@vib2022:/home/vib  
Archivo Editar Ver Buscar Terminal Ayuda  
Configuración de paquetes

#### Configuración de ldap-auth-config

This option will allow you to make password utilities that use pam to behave like you would be changing local passwords.

The password will be stored in a separate file which will be made readable to root only.

If you are using NFS mounted /etc or any other custom setup, you should disable this.

Make local root Database admin:

<Se>

<No>

Archivo Editar Ver Buscar Terminal Ayuda  
Configuración de paquetes

#### Configuración de ldap-auth-config

Choose this option if you are required to login to the database to retrieve entries.

Note: Under a normal setup, this is not needed.

Does the LDAP database require login?

<Se>

<No>

root@vib2022:/home/vib  
Archivo Editar Ver Buscar Terminal Ayuda  
Configuración de paquetes

#### Configuración de ldap-auth-config

This account will be used when root changes a password.

Note: This account has to be a privileged account.

LDAP account for root:

cn=admin,dc=mcastellvi,dc=vidal

<Aceptar>

Archivo Editar Ver Buscar Terminal Ayuda  
Configuración de paquetes

#### Configuración de ldap-auth-config

Please enter the password to use when ldap-auth-config tries to login to the LDAP directory using the LDAP account for root.

The password will be stored in a separate file /etc/ldap.secret which will be made readable to root only.

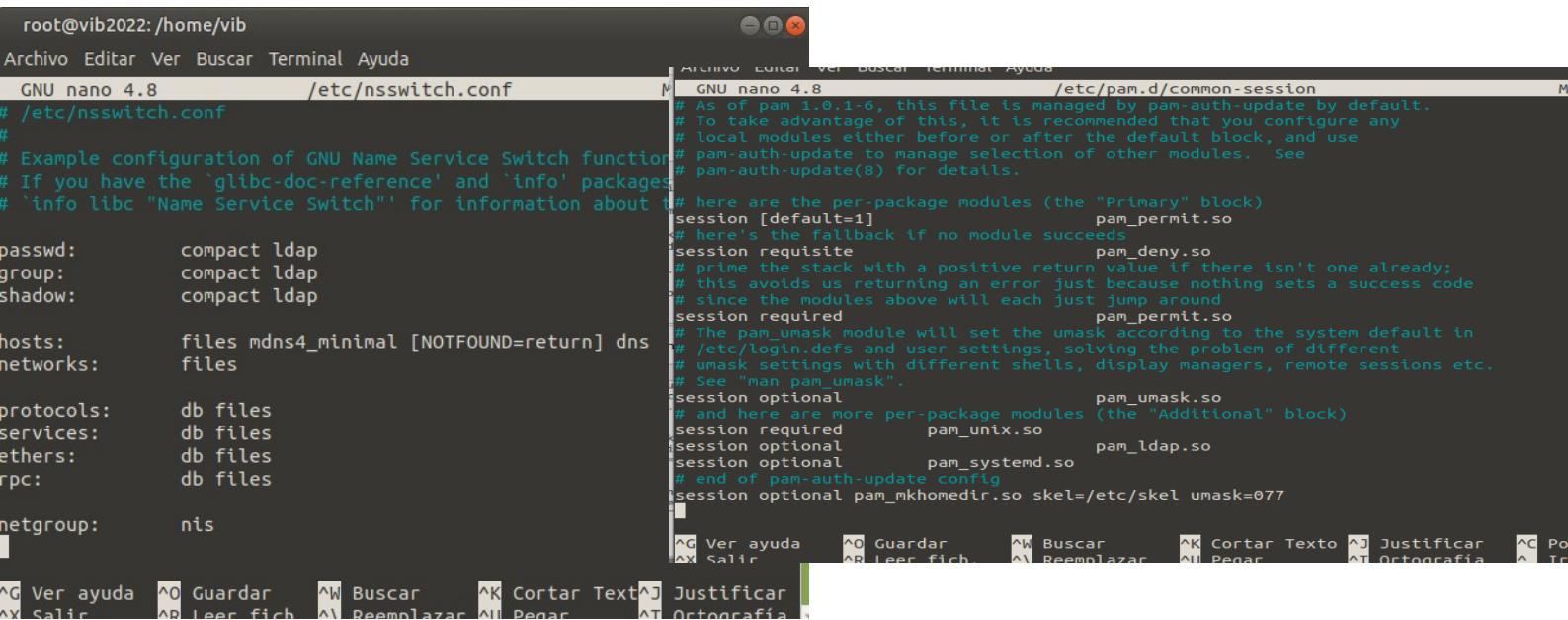
Entering an empty password will re-use the old password.

LDAP root account password:

\*\*\*

<Aceptar>

I cambiarem les dades insertant ldap:



```
root@vib2022: /home/vib
GNU nano 4.8 /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality:
# If you have the 'glibc-doc-reference' and 'info' packages
# 'info libc "Name Service Switch"' for information about this
# file.

passwd:      compact ldap
group:       compact ldap
shadow:      compact ldap

hosts:       files mdns4_minimal [NOTFOUND=return] dns
networks:    files

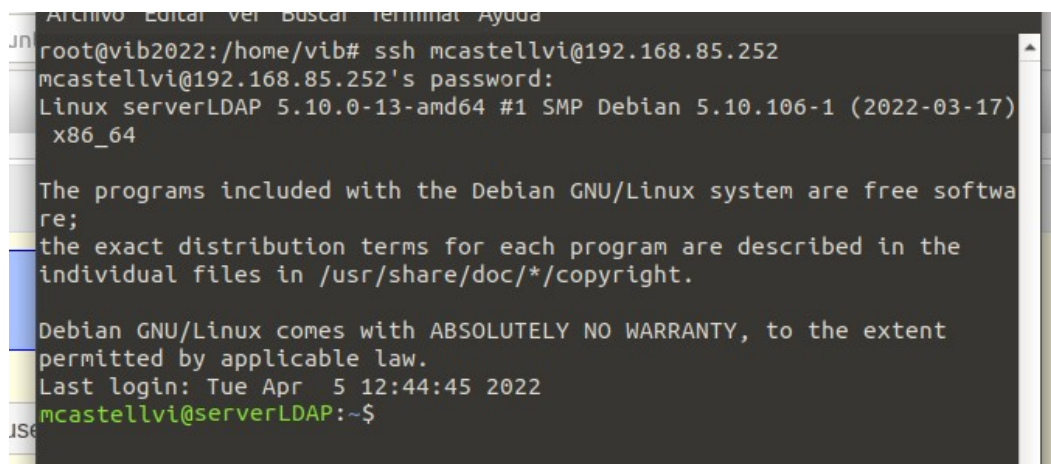
protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis

GNU nano 4.8 /etc/pam.d/common-session
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
session [default=1]                                pam_permit.so
# here's the fallback if no module succeeds
session requisite                                    pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
session required                                    pam_permit.so
# The pam_umask module will set the umask according to the system default in
# /etc/login.defs and user settings, solving the problem of different
# umask settings with different shells, display managers, remote sessions etc.
# See "man pam_umask".
session optional                                    pam_umask.so
# and here are more per-package modules (the "Additional" block)
session required                                    pam_unix.so
session optional                                    pam_ldap.so
session optional                                    pam_systemd.so
# end of pam-auth-update config
session optional pam_mkhomedir.so skel=/etc/skel umask=077
```

Ara podrem iniciar sessio amb ssh mostrant que hi ha connexió:



```
root@vib2022:/home/vib# ssh mcastellvi@192.168.85.252
mcastellvi@192.168.85.252's password:
Linux serverLDAP 5.10.0-13-amd64 #1 SMP Debian 5.10.106-1 (2022-03-17)
x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Apr  5 12:44:45 2022
mcastellvi@serverLDAP:~$
```