

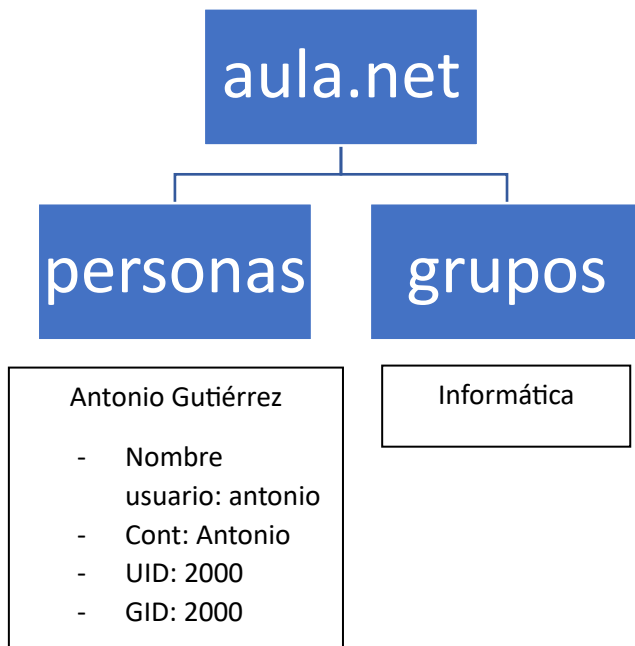
LDAP

Red NAT: Laboratorio 10.10.10.0/24

V.Server → 10.10.10.100 serveraula.net

V.Desktop → 10.10.10.101 DHCP

Objetivo: Crear la siguiente estructura(directorio)



Añadir la IP y el nombre FQDN (full qualified domain name) al archivo hosts del servidor

```
ubuntu server pristine [Corriendo] - Oracle VM VirtualBox
GNU nano 6.2 /etc/hosts *
127.0.0.1 localhost
127.0.1.1 pristine
10.10.10.100 serveraula.net_

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

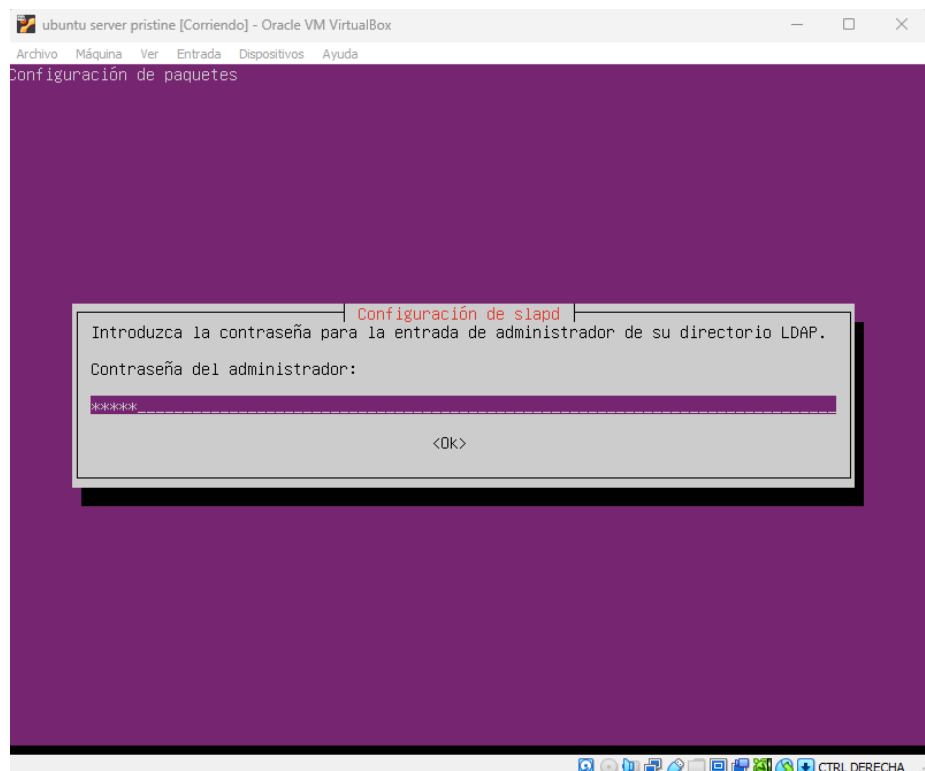
Hacer update y upgrade

```
root@pristine:~# apt update && apt upgrade
```

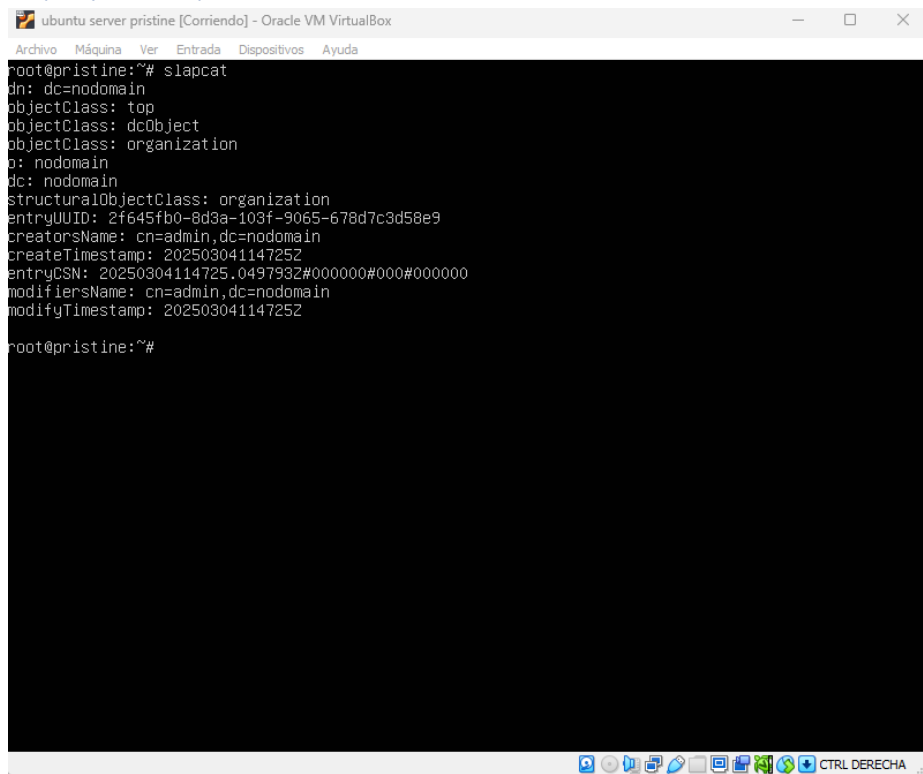
Instalar OpenLDAP y sus herramientas

```
root@pristine:~# apt install slapd ldap-utils -y_
```

Poner contraseña



Vemos (exportar) base de datos del servidor LDAP



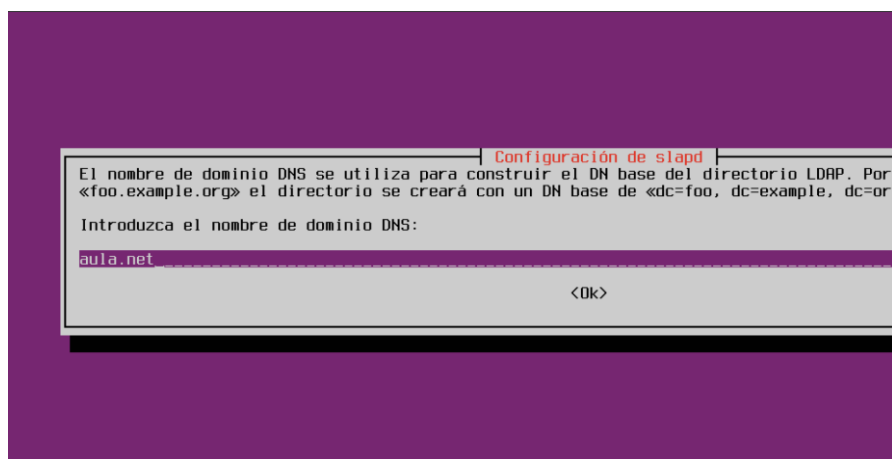
```
root@pristine:~# slapcat
dn: dc=nodomain
objectClass: top
objectClass: dcObject
objectClass: organization
o: nodomain
dc: nodomain
structuralObjectClass: organization
entryUUID: 2f645fb0-8d3a-103f-9065-678d7c3d58e9
creatorsName: cn=admin,dc=nodomain
createTimestamp: 20250304114725Z
entryCSN: 20250304114725.049793Z#000000#000#000000
modifiersName: cn=admin,dc=nodomain
modifyTimestamp: 20250304114725Z

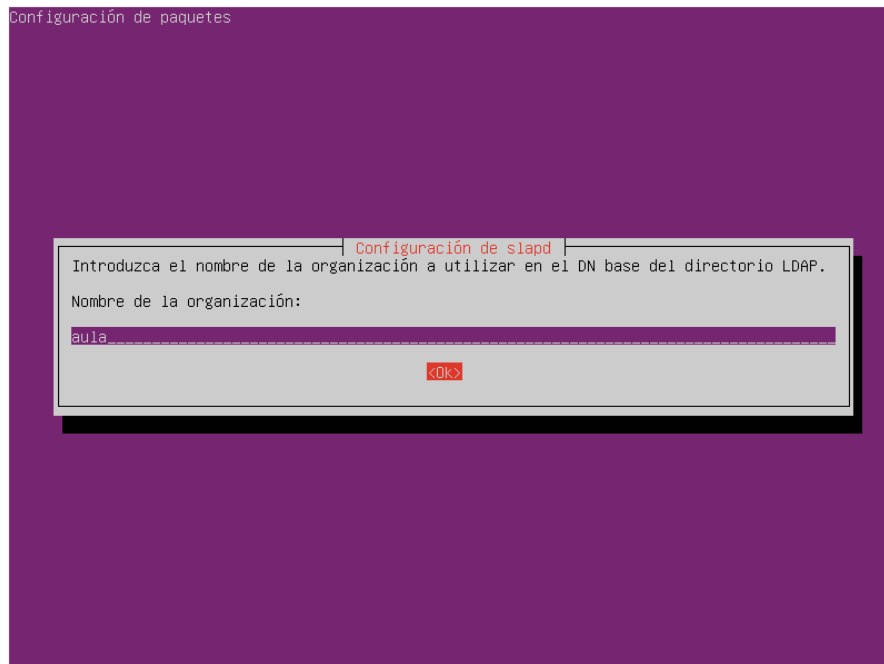
root@pristine:~#
```

Reconfiguramos el slapd

```
root@pristine:~# dpkg-reconfigure slapd
```

Le decimos no y luego ponemos el nombre del dominio (aula.net), el nombre de la organización similar al del dominio, revisamos el slapcat





Comprobamos que esta running

```
root@pristine:~# systemctl status slapd
• slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
   Loaded: loaded (/etc/init.d/slapd; generated)
   Drop-In: /usr/lib/systemd/system/slapd.service.d
            └─slapd-remain-after-exit.conf
   Active: active (running) since Tue 2025-03-04 12:02:55 UTC; 6min ago
     Docs: man:systemd-sysv-generator(8)
  Process: 26369 ExecStart=/etc/init.d/slapd start (code=exited, status=0/SUCCESS)
    Tasks: 3 (limit: 2224)
   Memory: 3.3M
      CPU: 19ms
   CGroup: /system.slice/slapd.service
            └─26376 /usr/sbin/slapd -h "ldapi:/// ldapi:///" -g openldap -u openldap -F /etc/ldap/slapd.conf

mar 04 12:02:55 pristine systemd[1]: Starting LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol).
mar 04 12:02:55 pristine slapd[26369]: * Starting OpenLDAP slapd
mar 04 12:02:55 pristine slapd[26375]: @(#) $OpenLDAP: slapd 2.5.18+dfsg-0ubuntu0.22.04.3 (Dec  9 2022);
        Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
mar 04 12:02:55 pristine slapd[26376]: slapd starting
mar 04 12:02:55 pristine slapd[26369]: ...done.
mar 04 12:02:55 pristine systemd[1]: Started LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol).
lines 1-20/20 (END)
```

Instalar la instrucción net-tools para utilizar la instrucción netstat para comprobar que el servidor esta a la escucha

```
root@pristine:~# apt install net-tools
```

```
root@pristine:~# netstat -tulpn | grep slapd
tcp        0      0 0.0.0.0:389          0.0.0.0:*           LISTEN     26376/slapd
tcp6       0      0 :::389              :::*                 LISTEN     26376/slapd
root@pristine:~# netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:389          0.0.0.0:*              LISTEN      26376/slapd
tcp        0      0 127.0.0.1:3306        0.0.0.0:*              LISTEN      25738/mysql
tcp        0      0 127.0.0.1:33060       0.0.0.0:*              LISTEN      25738/mysql
tcp        0      0 0.0.0.0:21           0.0.0.0:*              LISTEN      25668/vsftpd
tcp        0      0 0.0.0.0:22           0.0.0.0:*              LISTEN      25681/sshd: /usr/sb
tcp        0      0 127.0.0.53:53        0.0.0.0:*              LISTEN      25712/systemd-resol
tcp6       0      0 :::389               :::*                   LISTEN      26376/slapd
tcp6       0      0 :::22                :::*                   LISTEN      25681/sshd: /usr/sb
tcp6       0      0 :::80                :::*                   LISTEN      25717/apache2
udp        0      0 127.0.0.53:53        0.0.0.0:*              LISTEN      25712/systemd-resol
root@pristine:~#
```

Crear fichero ldif que contendrá la unidad organizativa llamada personas (usuarios)

```
GNU nano 6.2      basedn.ldif *
dn: ou=personas,dc=aula,dc=net
objectClass: organizationalUnit
ou: personas

dn: ou=groups,dc=aula,dc=net
objectClass: organizationalUnit
ou: groups_

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo
```

Añade la entrada del fichero creado antes

```
root@pristine:~# ldapadd -x -D cn=admin,dc=aula,dc=net -W -f basedn.ldif
Enter LDAP Password:
adding new entry "ou=personas,dc=aula,dc=net"

adding new entry "ou=groups,dc=aula,dc=net"

root@pristine:~#
```

Con slapcat comprobamos

```
dn: dc=aula,dc=net
objectClass: top
objectClass: dcObject
objectClass: organization
o: aula
dc: aula
structuralObjectClass: organization
entryUUID: 59f9f602-8d3c-103f-8a94-976094744a30
creatorsName: cn=admin,dc=aula,dc=net
createTimestamp: 20250304120255Z
entryCSN: 20250304120255.487900Z#000000#000#000000
modifiersName: cn=admin,dc=aula,dc=net
modifyTimestamp: 20250304120255Z

dn: ou=personas,dc=aula,dc=net
objectClass: organizationalUnit
ou: personas
structuralObjectClass: organizationalUnit
entryUUID: ca807678-8d3f-103f-9146-4bb4c5108f99
creatorsName: cn=admin,dc=aula,dc=net
createTimestamp: 20250304122732Z
entryCSN: 20250304122732.764384Z#000000#000#000000
modifiersName: cn=admin,dc=aula,dc=net
modifyTimestamp: 20250304122732Z

dn: ou=groups,dc=aula,dc=net
objectClass: organizationalUnit
ou: groups
structuralObjectClass: organizationalUnit
entryUUID: ca80edec-8d3f-103f-9147-4bb4c5108f99
creatorsName: cn=admin,dc=aula,dc=net
createTimestamp: 20250304122732Z
entryCSN: 20250304122732.767452Z#000000#000#000000
modifiersName: cn=admin,dc=aula,dc=net
modifyTimestamp: 20250304122732Z

ubuntu@pristine:~$
```

Creamos el fichero para usuarios y a parte le generamos la contraseña cifrada

```
GNU nano 6.2 usuarios.ldif
dn: uid=Antonio,ou=personas,dc=aula,dc=net
objectClass: inetOrgPerson
objectClass: posixAccount
cn: Antonio
sn: Gutiérrez
userPassword:
```

```
ubuntu@pristine:~$ sudo slappasswd >> usuarios.ldif
```

```
GNU nano 6.2 usuarios.ldif *
dn: uid=Antonio,ou=personas,dc=aula,dc=net
objectClass: inetOrgPerson
objectClass: posixAccount
cn: Antonio
sn: Gutiérrez
userPassword:{SSHA}B3rrxwCfW1rs9rvUQQWhLguL8mobHL1z
loginShell: /bin/bash
uidNumber 2000
gidNumber: 2000
homeDirectory: /home/agutierrez
```

Añade entrada del fichero

```
root@pristine:~# ldapadd -x -D cn=admin,dc=aula,dc=net -W -f usuarios.ldif
Enter LDAP Password:
adding new entry "uid=Antonio,ou=personas,dc=aula,dc=net"
```

Crear fichero para grupos

```
GNU nano 6.2 grupo.ldif *
dn: cn=Informatica,ou=grupos,dc=aula,dc=net
objectClass: posixGroup
cn: Informatica
gidNumber: 2000
memberUid: Informatica
```

Instalar php y características

```
ubuntu@pristine:~$ sudo apt install php libapache2-mod-php php-cli php-mysql php-xml php-mbstring php-curl php-gd php-bcmath -y
```

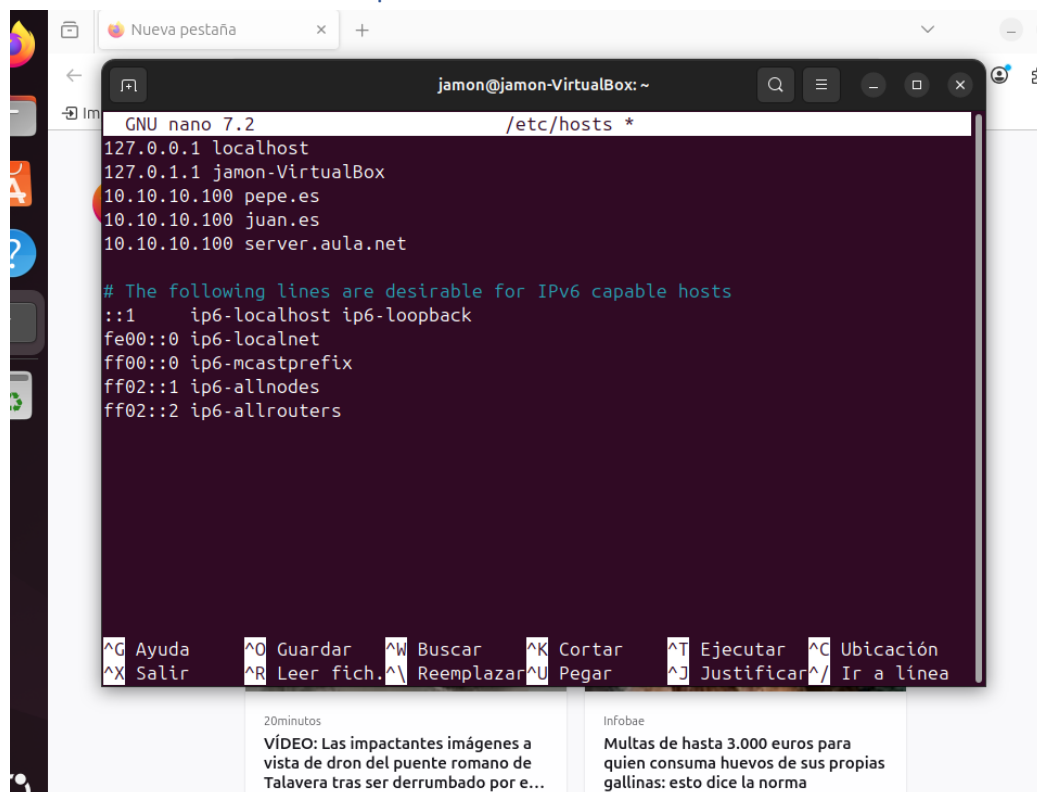
Creemos archivo php

```
GNU nano 6.2 /var/www/juan/info.php *
<?php
    phpinfo();
?>_
```


Instalar algo grafico para ldap gestor de usuarios

```
ubuntu@pristine:~$ sudo apt install ldap-account-manager-y_
```

Asociar dominio a la ip en cliente



Colocamos el dominio en la información requerida

 **Ajustes de herramientas**


Herramientas ocultas

Importación/exportación LDAP	<input type="checkbox"/>	Dispositivos WebAuthn	<input type="checkbox"/>	Edición múltiple	<input type="checkbox"/>
Comprobar	<input type="checkbox"/>	Enviar archivos	<input type="checkbox"/>	Explorador de esquemas	<input type="checkbox"/>
Información del servidor	<input type="checkbox"/>	Editor de perfiles	<input type="checkbox"/>	Editor de OU	<input type="checkbox"/>
Visor del árbol	<input type="checkbox"/>	Editor de PDF	<input type="checkbox"/>		

Visor del árbol

Sufijo del árbol

dc=aula,dc=net

 **Preferencias de seguridad**

Método del inicio de sesión

Lista fijada

Lista de usuarios válidos *

cn=admin,dc=aula,dc=net

Ponemos información del usuario y establecemos contraseña

Guardar


Restablecer cambios.

Establecer contraseña

default

Cargar perfil

Eliminar

 **Antonio Gutiérrez**


Sufijo

personas > aula > net

Identificador RDN

uid

 Personal

 Unix

 Sombra

Nombre del usuario *

agutierrez

Nombre común

agutierrez

Número UID

10000

Gecos

Antonio Gutierrez

Grupo primario

Informatica

Grupos adicionales

Editar grupos

Directorio inicial *

/home/agutierrez

Intérprete del inicio de sesión

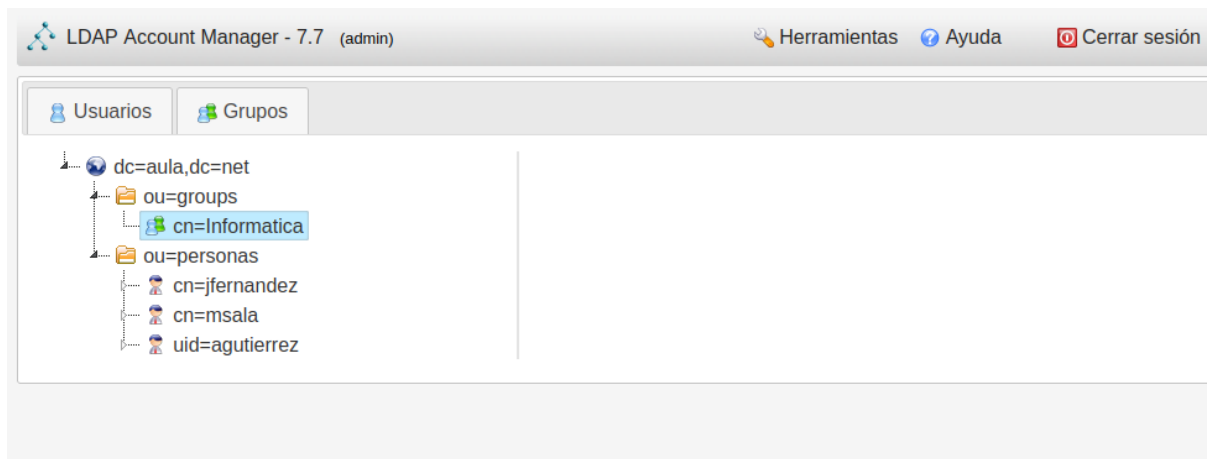
/bin/bash

Contraseña

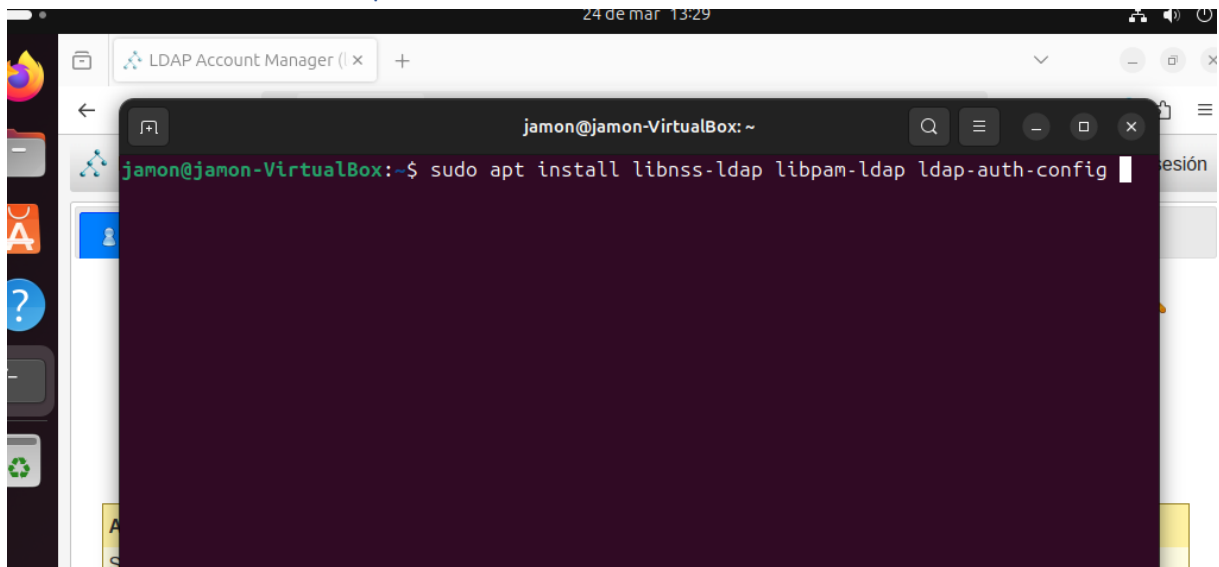
Bloquear contraseña

Quitar contraseña

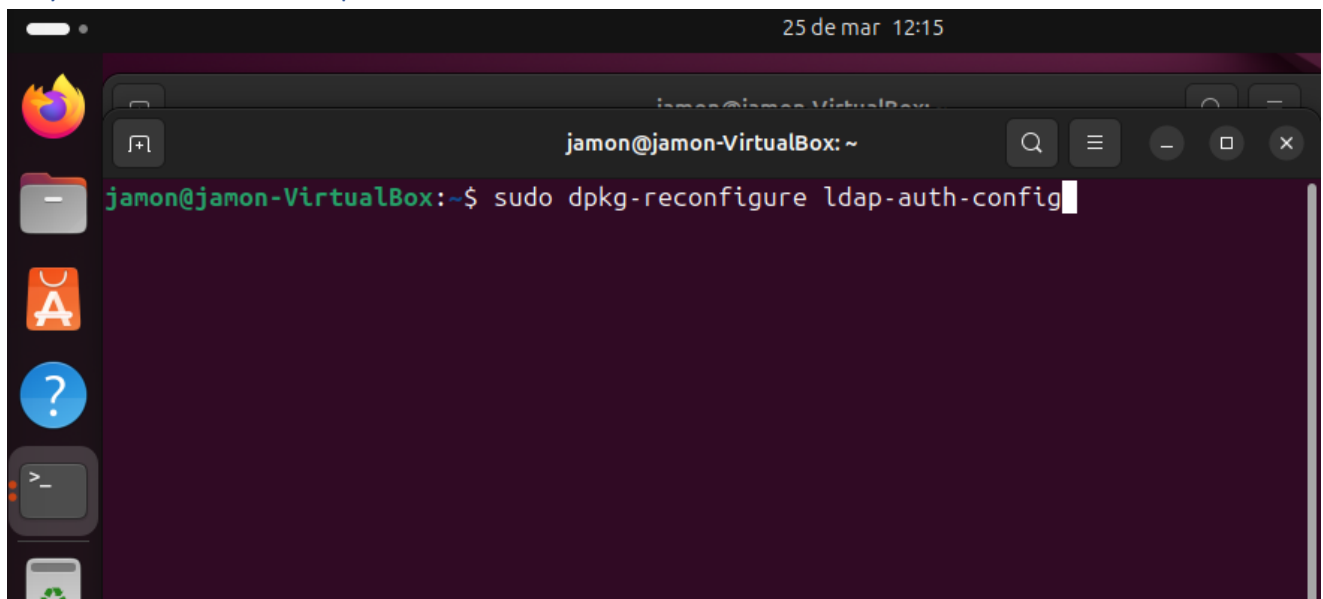
Visor de árbol



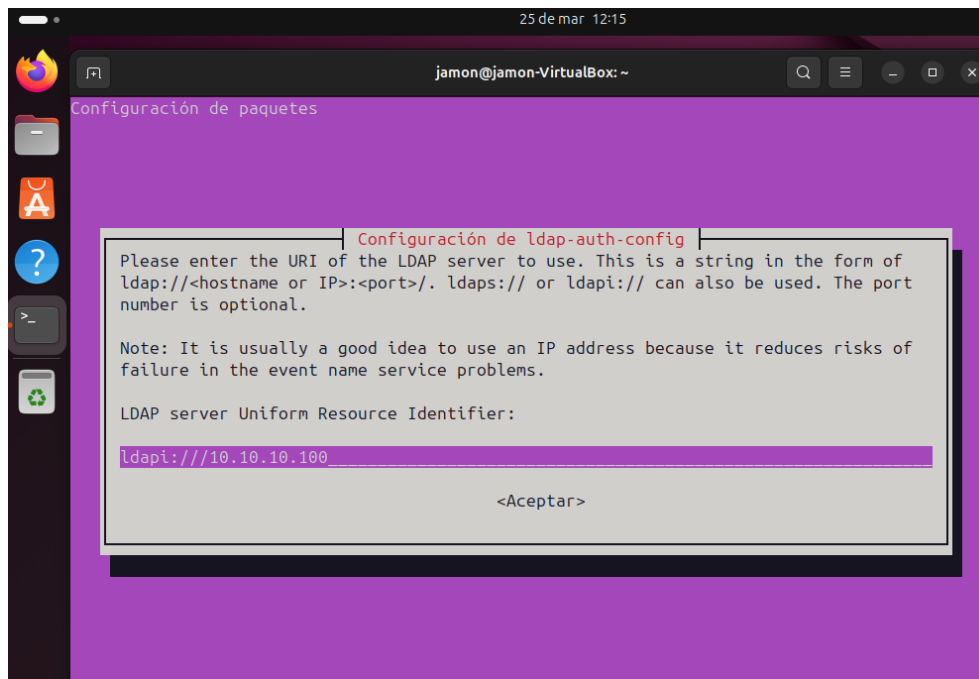
Instalar utilidades ldap en cliente



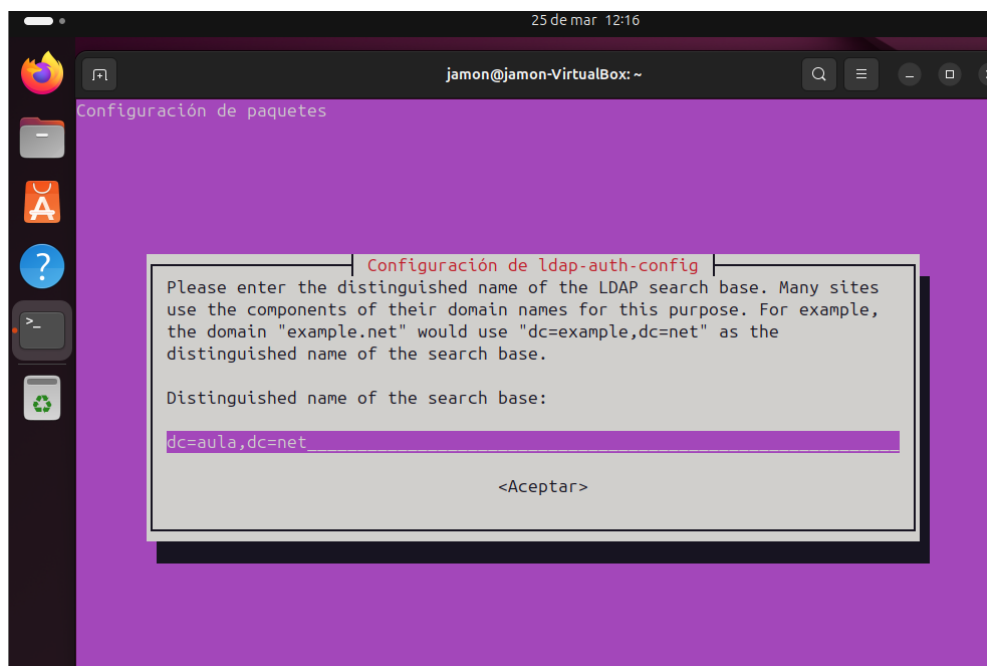
Si ya esta instalado poner este comando



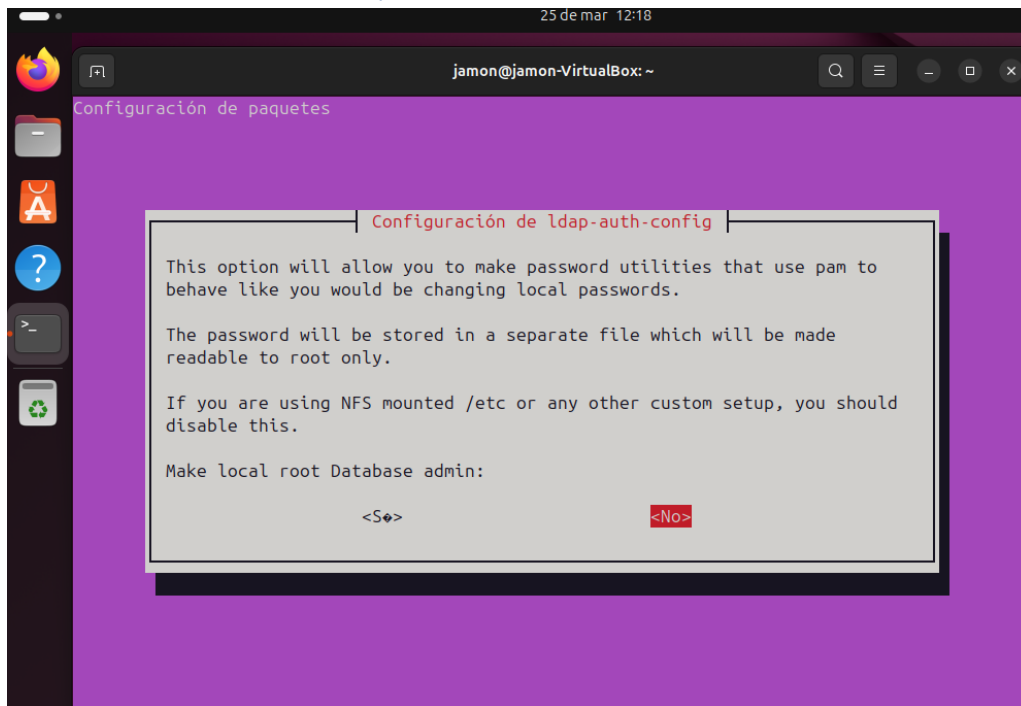
Poner IP del servidor



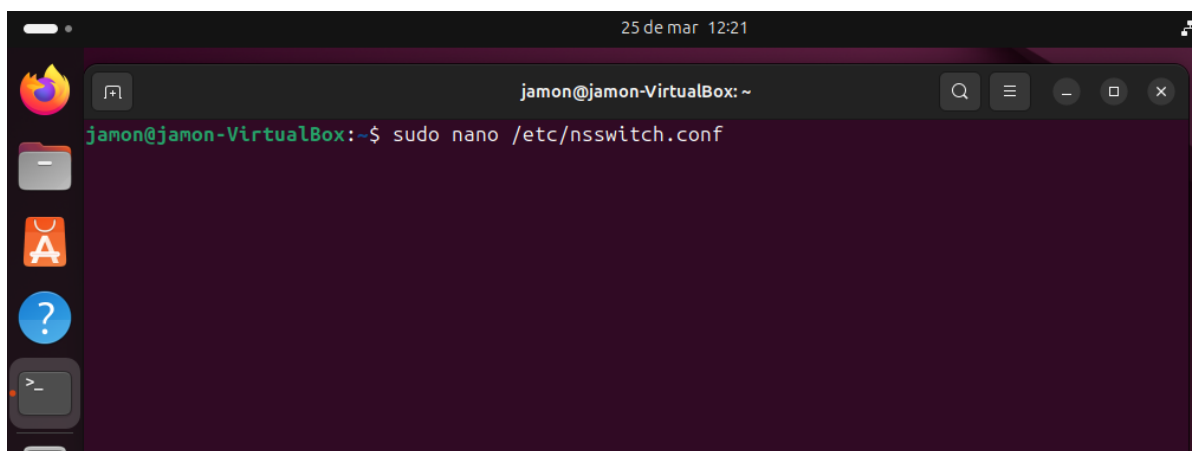
Poner dominio del servidor



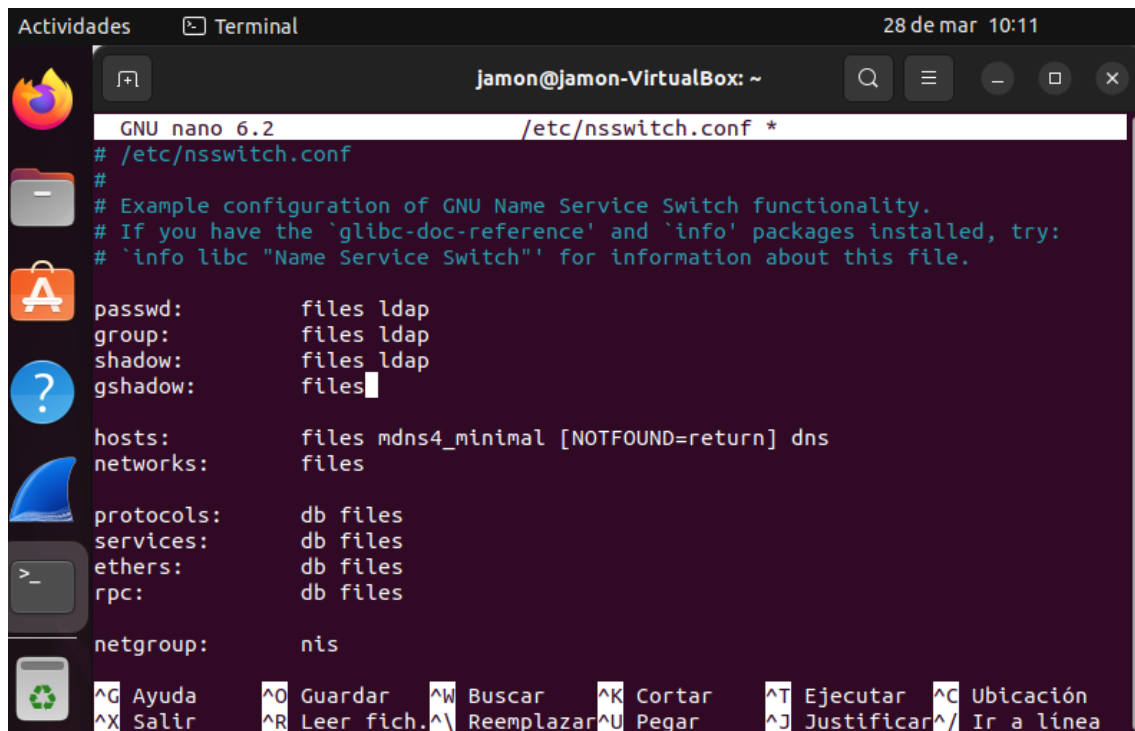
Versión más reciente y no



Configurar como el sistema busca información sobre usuarios, si está en servidor u otro sitio



Colocamos la información necesaria



The screenshot shows a terminal window titled "Terminal" with the user "jamon@jamon-VirtualBox: ~". The terminal is running the GNU nano 6.2 editor, editing the file "/etc/nsswitch.conf". The file content is as follows:

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the 'glibc-doc-reference' and 'info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:      files ldap
group:       files ldap
shadow:      files ldap
gshadow:     files

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

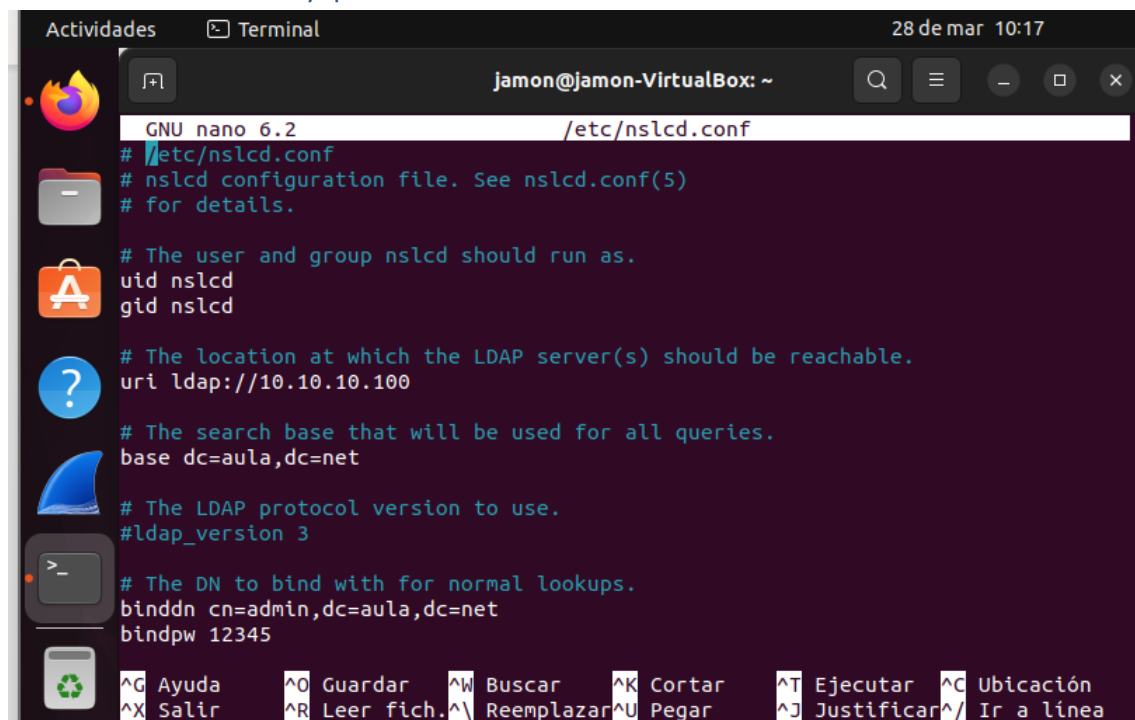
protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis
```

At the bottom of the terminal, there is a keyboard shortcut menu:

^G Ayuda	^O Guardar	^W Buscar	^K Cortar	^T Ejecutar	^C Ubicación
^X Salir	^R Leer fich.	^N Reemplazar	^U Pegar	^J Justificar	^_ Ir a línea

Creamos archivo y ponemos texto



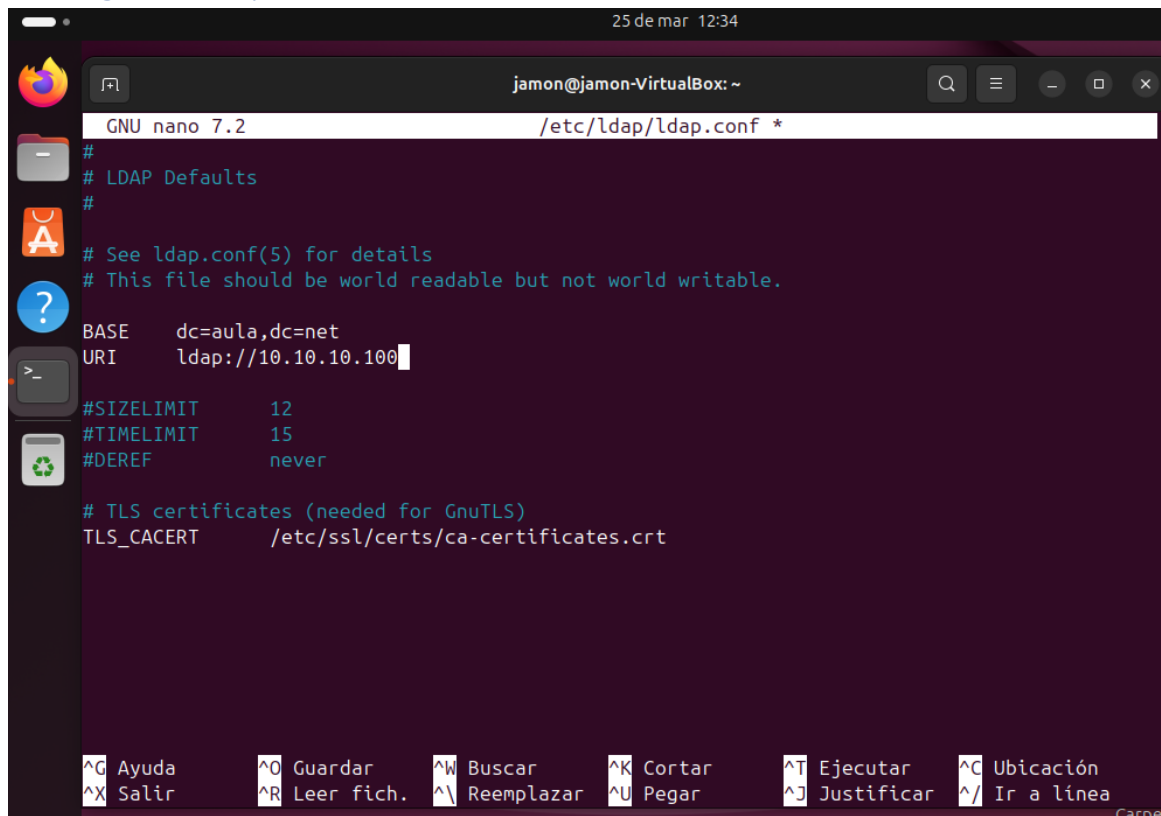
The screenshot shows a terminal window titled "Terminal" with the user "jamon@jamon-VirtualBox: ~". The terminal is running the GNU nano 6.2 editor, editing the file "/etc/nslcd.conf". The file content is as follows:

```
# /etc/nslcd.conf
# nslcd configuration file. See nslcd.conf(5)
# for details.
#
# The user and group nslcd should run as.
uid nslcd
gid nslcd
#
# The location at which the LDAP server(s) should be reachable.
uri ldap://10.10.10.100
#
# The search base that will be used for all queries.
base dc=aula,dc=net
#
# The LDAP protocol version to use.
#ldap_version 3
#
# The DN to bind with for normal lookups.
binddn cn=admin,dc=aula,dc=net
bindpw 12345
```

At the bottom of the terminal, there is a keyboard shortcut menu:

^G Ayuda	^O Guardar	^W Buscar	^K Cortar	^T Ejecutar	^C Ubicación
^X Salir	^R Leer fich.	^N Reemplazar	^U Pegar	^J Justificar	^_ Ir a línea

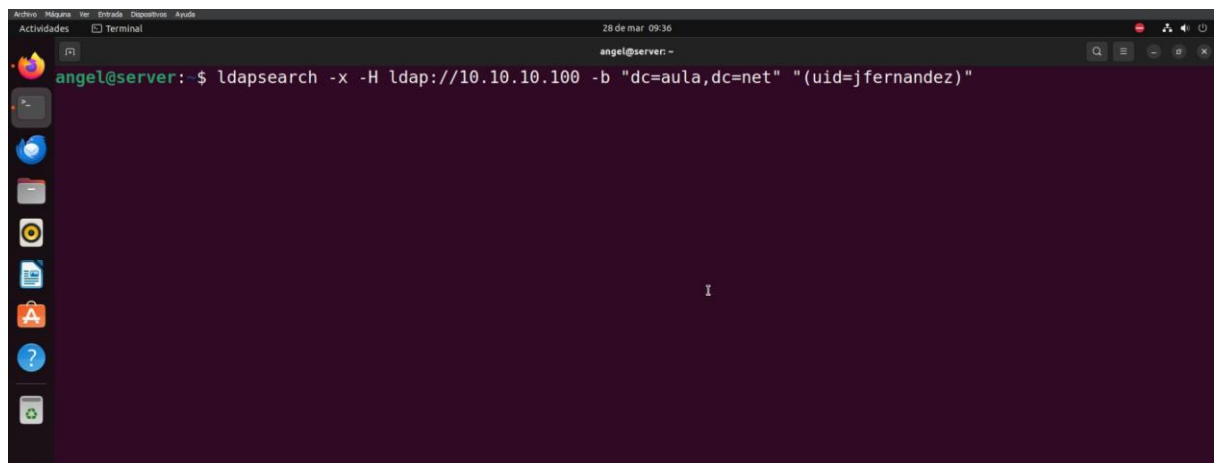
Configurar ldap.conf



```
GNU nano 7.2 /etc/ldap/ldap.conf *
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
BASE    dc=aula,dc=net
URI     ldap://10.10.10.100
#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never
# TLS certificates (needed for GnuTLS)
TLS_CACERT      /etc/ssl/certs/ca-certificates.crt
```

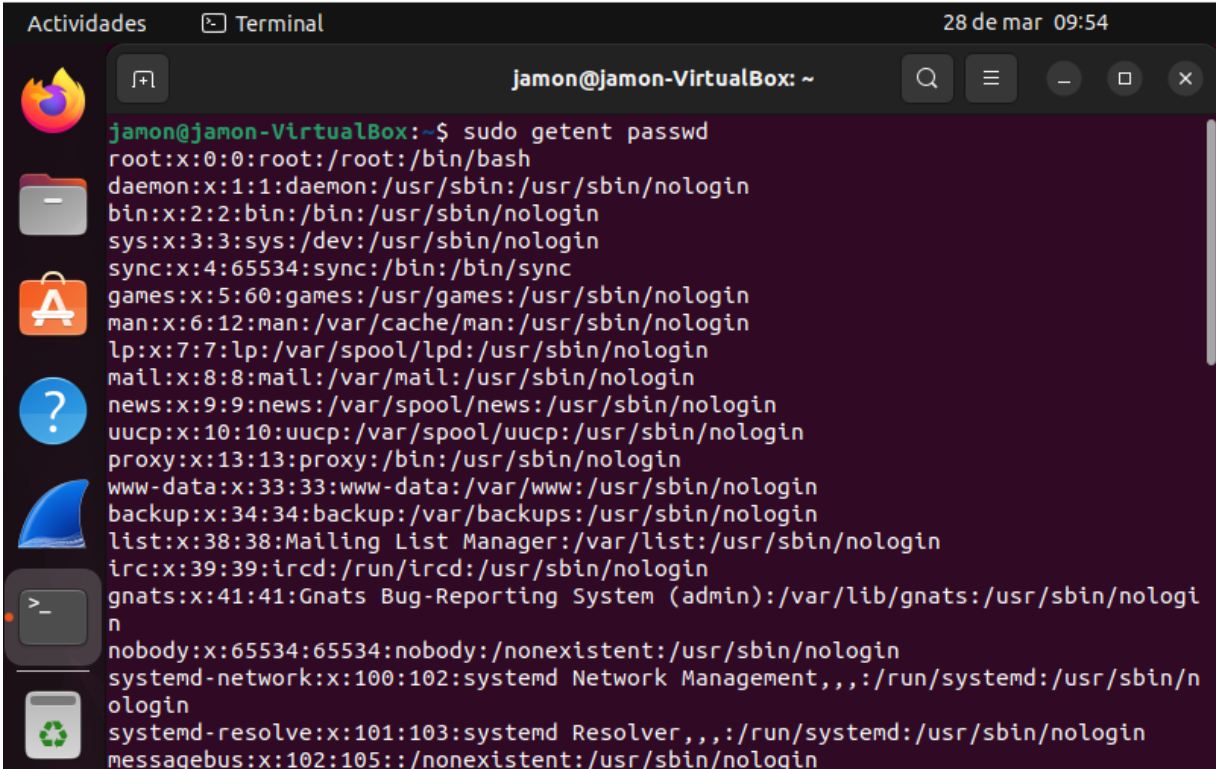
^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^J Justificar ^_ Ir a línea

Buscar usuario



```
angel@server: ~$ ldapsearch -x -H ldap://10.10.10.100 -b "dc=aula,dc=net" "(uid=jfernandez)"
```

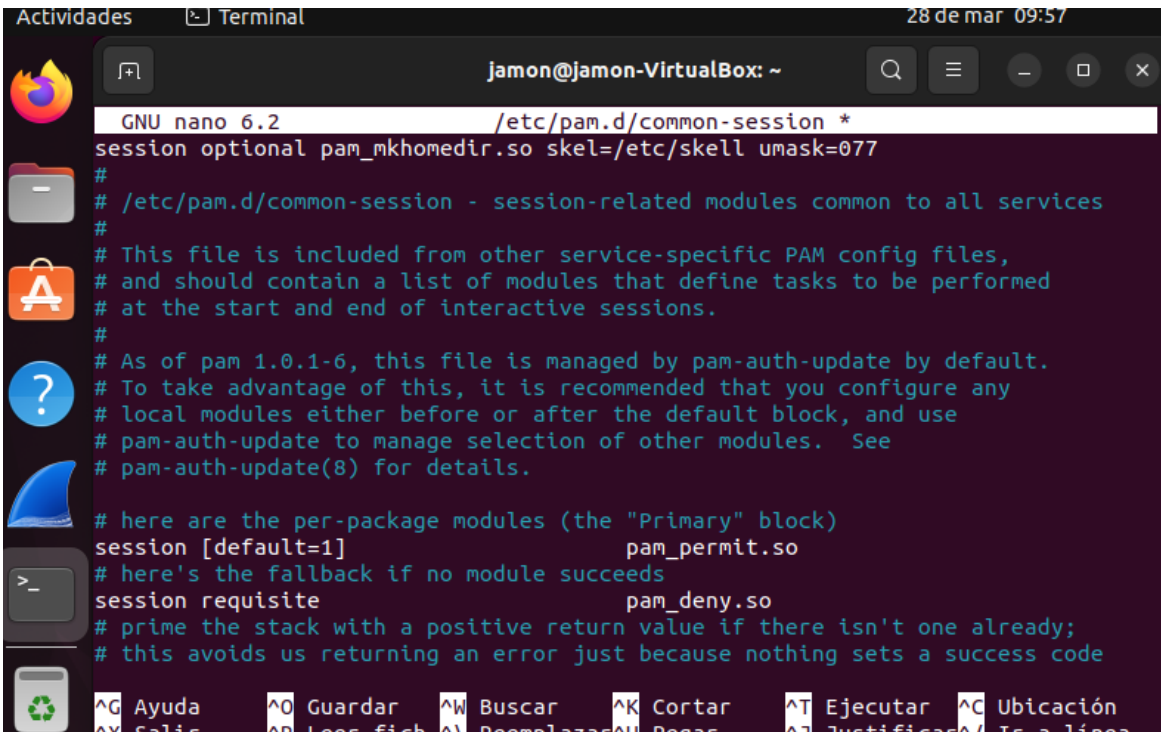
Listado de usuarios locales y remotos



A terminal window titled 'jamón@jamón-VirtualBox: ~' showing the output of the command 'sudo getent passwd'. The output lists system and regular users with their IDs, names, and home directories. The window has a sidebar with application icons and a top bar with the date '28 de mar 09:54'.

```
jamón@jamón-VirtualBox:~$ sudo getent passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
ircd:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:102:105:,:/nonexistent:/usr/sbin/nologin
```

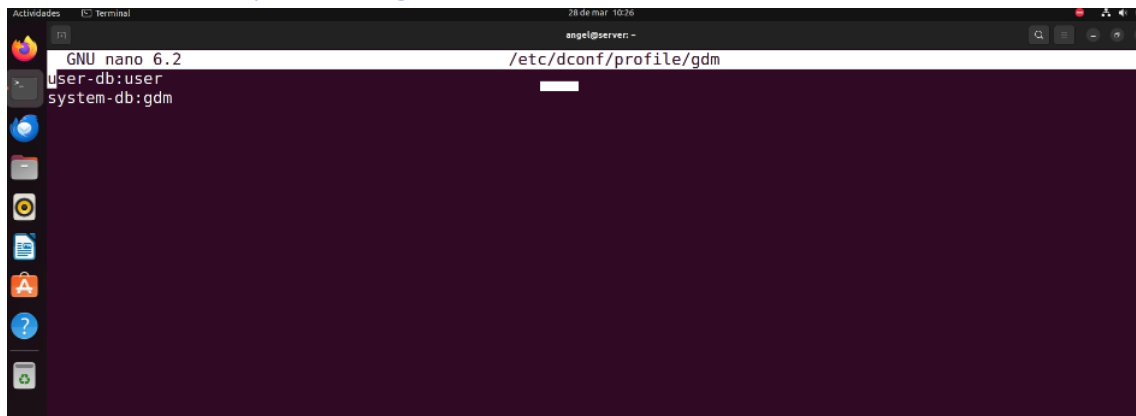
Parrafon para que los usuarios tengan sus carpetas personales al iniciar sesión



A terminal window titled 'jamón@jamón-VirtualBox: ~' showing the nano editor editing the file '/etc/pam.d/common-session'. The editor shows the default configuration for the session module, including comments and module definitions. The window has a sidebar with application icons and a top bar with the date '28 de mar 09:57'.


```
GNU nano 6.2 /etc/pam.d/common-session *
session optional pam_mkhomedir.so skel=/etc/skel umask=077
#
# /etc/pam.d/common-session - session-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be performed
# at the start and end of interactive sessions.
#
# 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
```

Editar archivo para no guardar usuarios



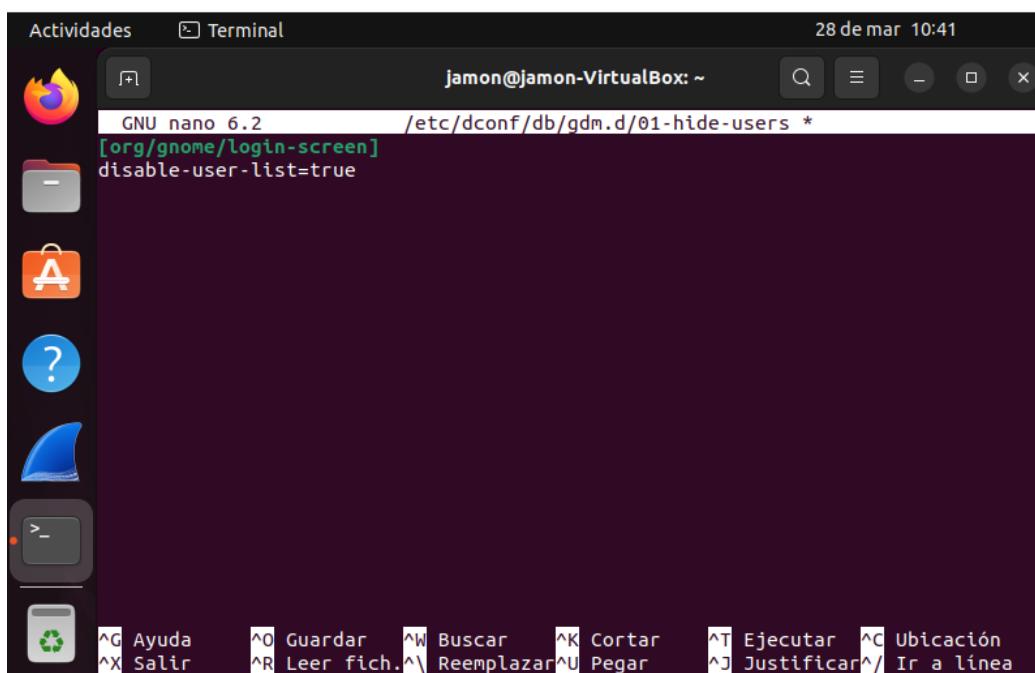
```
GNU nano 6.2 /etc/dconf/profile/gdm
user-db:user
system-db:gdm
```

Creamos ruta con fichero para ocultar usuarios



```
jamón@jamón-VirtualBox: ~$ sudo nano /etc/dconf/profile/gdm
[sudo] contraseña para jamón:
jamón@jamón-VirtualBox: ~$ sudo mkdir -p /etc/dconf/db/gdm.d
jamón@jamón-VirtualBox: ~$ sudo nano /etc/dconf/db/gdm.d/01-hide-users
jamón@jamón-VirtualBox: ~$
```

Editamos el archivo



```
GNU nano 6.2 /etc/dconf/db/gdm.d/01-hide-users *
[org/gnome/login-screen]
disable-user-list=true
```

^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación
^X Salir ^R Leer fich. ^E Reemplazar ^U Pegar ^J Justificar ^_ Ir a línea

Actualizar para aplicar cambios

