**Pt 9 Client Instal·lació i administració**



**Objectius**

* Conèixer les característiques principals del protocol LDAP i la seva implementació a Linux, OpenLDAP.
* Dur a terme la instal·lació del client OpenLDAP sobre Ubuntu
* Configurar Ubuntu Desktop per tal que pugui autenticar els usuaris contra el servidor OpenLDAP instal·lat en un altre servidor.
* Conèixer les aplicacions que té el protocol LDAP sobre altres programes

**Introducció**

En aquesta pràctica instal·laràs el client OpenLDAP en un entorn desktop. El client de LDAP és el programa que serveix per accedir al servei LDAP.

En Ubuntu, necessitarem ajustar el comportament dels serveis NSS i PAM en cada client que hàgim de configurar.

És un servei que permet la resolució de noms d'usuari i contrasenyes mitjançant l'accés a diferents orígens de la informació. En condicions normals, aquesta informació es troba en els arxius locals del sistema operatiu, en concret en,

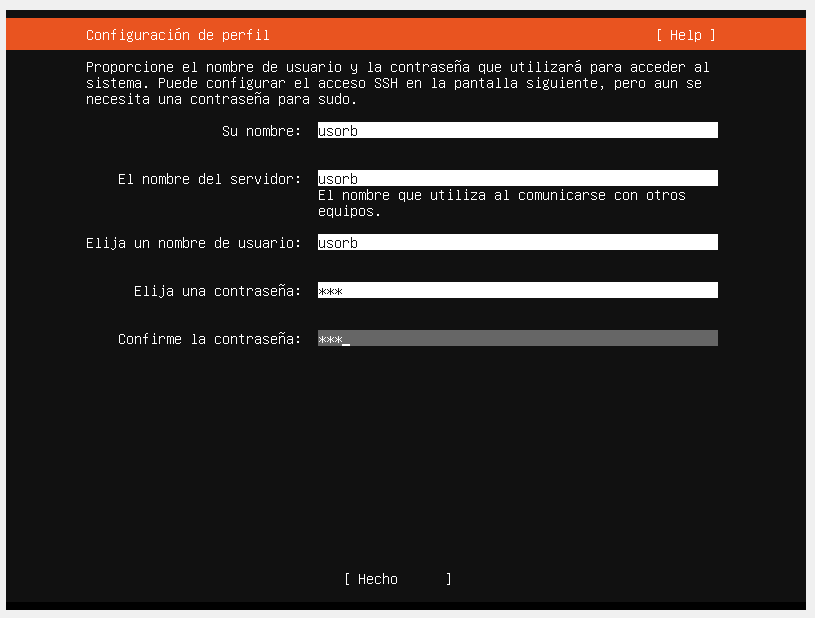
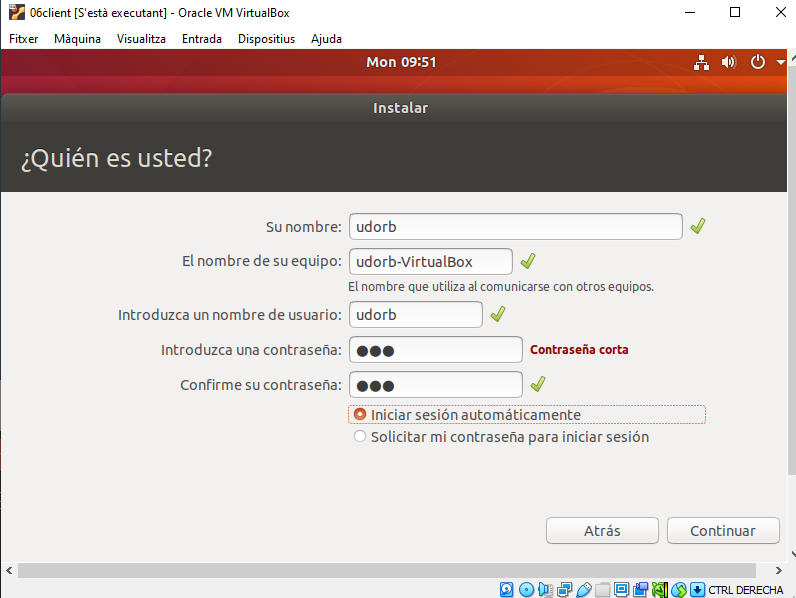
**Webgrafia**

1. [**Gestió LDAP amb interfície gràfica**](https://seicoll.gitbooks.io/sox/content/uf2.-sistemes-operatius-lliures-en-xarxa/uf2-gestio-dominis/uf2-ldap-gestio-grafica.html) **[Gitbook]**
2. [**Dominis amb Linux**](http://moodlecf.sapalomera.cat/apunts/smx/sox/index.html?cap=149&ref=2110) **[SOX Sa Palomera]**
3. [**Qué es LDAP**](http://somebooks.es/12-4-que-es-ldap/) **[Somebooks]**
4. [**Tutorial Eneko Amieva LDAP**](https://web.archive.org/web/20160422080807/http:/enekoamieva.com/que-es-ldap/) **[Serie de tutoriales OpenLDAP]**
5. [**YouTube Videocurso OpenLDAP (4 partes)**](https://www.youtube.com/watch?v=Zmj6A5ggcgg&t=1643s&ab_channel=Merkasys)
6. [**CURSO VIDEO OPENLDAP PROF. ALBERTO MOLINA**](https://aso.tinaja.es/ldap/) **-- NOU!**

**Paràmetres de configuració**

***Apunta les ips de la teva topologia a la taula***

| **XARXA NAT** | **Ubuntu Server** | **Ubuntu Desktop** |
| --- | --- | --- |
| **Nom equip (hostname)** | usorb  (on ***xxx*** han de ser les inicials del teu nom i cognoms) | udorb  (on ***xxx*** han de ser les inicials del teu nom i cognoms) |
| **Adreça IP** | 10.0.2.15 | 10.0.2.25 |
| **Màscara** | 255.255.255.0 | |
| **Porta d’enllaç (GW)** | 10.0.2.1 | |
| **Servidors DNS:** | 8.8.8.8 | |



**Part 1: Instal·lació al client**

Per a instal·lar les aplicacions al client haurem d'instal·lar els següents paquets:

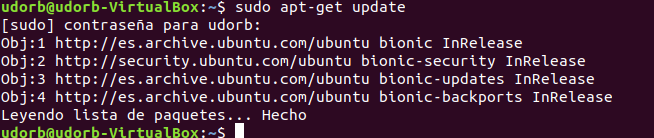
* 1. Per a instal·lar les aplicacions al client haurem d'instal·lar els següents paquets:

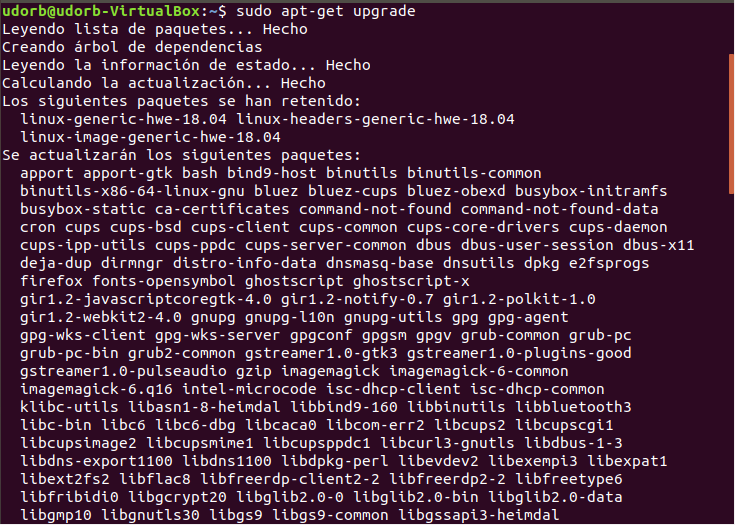
$sudo apt-get update

$sudo apt-get upgrade

$sudo apt-get install **libnss-ldap libpam-ldap ldap-utils**

Generarà un fitxer a /etc/ldap.conf





A continuació s’obrirà un wizard que ens demana dades:

-ip servidor LDAP (ldap://ip-del-teu-servidor)

-Base del domini (DN) dc=ldapxxx, dc=local

-versió: 3

-Crear BBDD: sí

-requerir login per accedir a la BBDD: NO

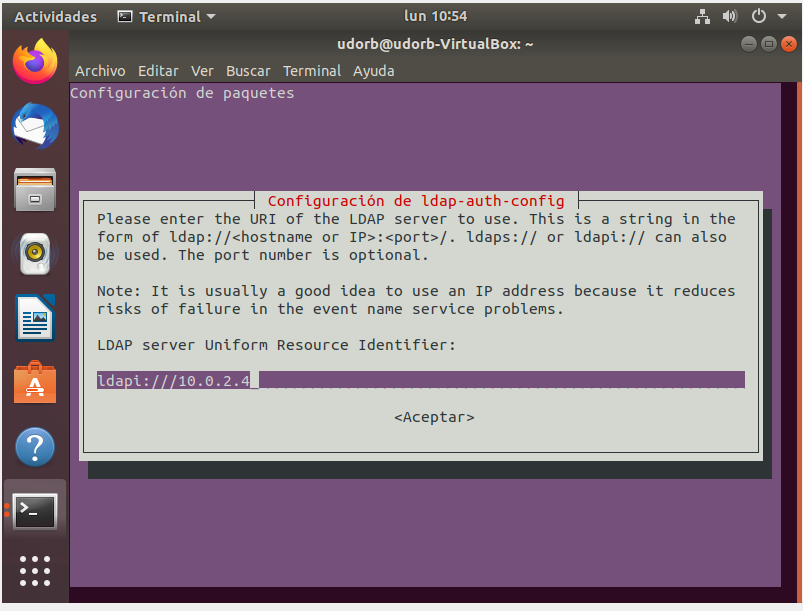
-cn de l’usuari administrador del directori: cn=admin, dc=ldapxxx,dc=local

-contrasenya: podem o no posar-la

***Fes captures de tot el procès.***

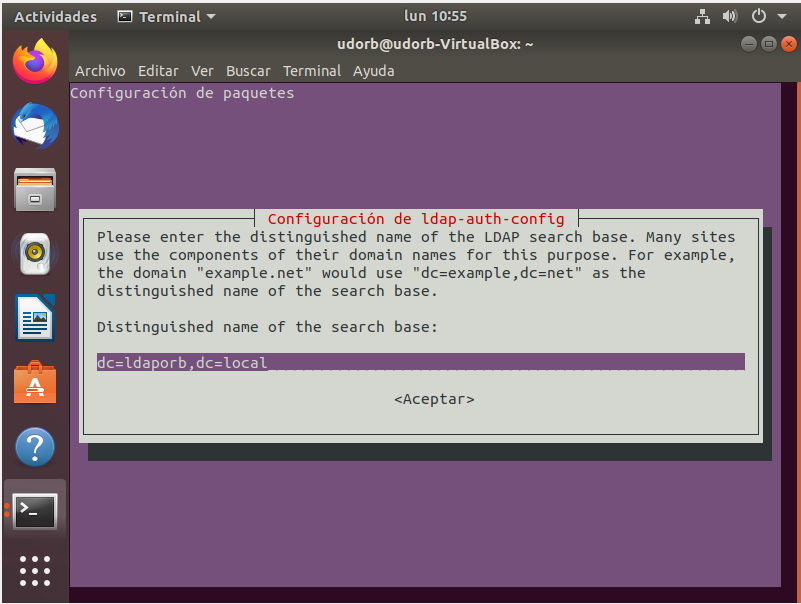
* 1. S’activarà un assitent per configurar ldap-atut-config. Com a primer pas haurem de configurar la URI (l’adreça IP del servidor) del servidor LDAP.

ldapi:///10.0.2.4

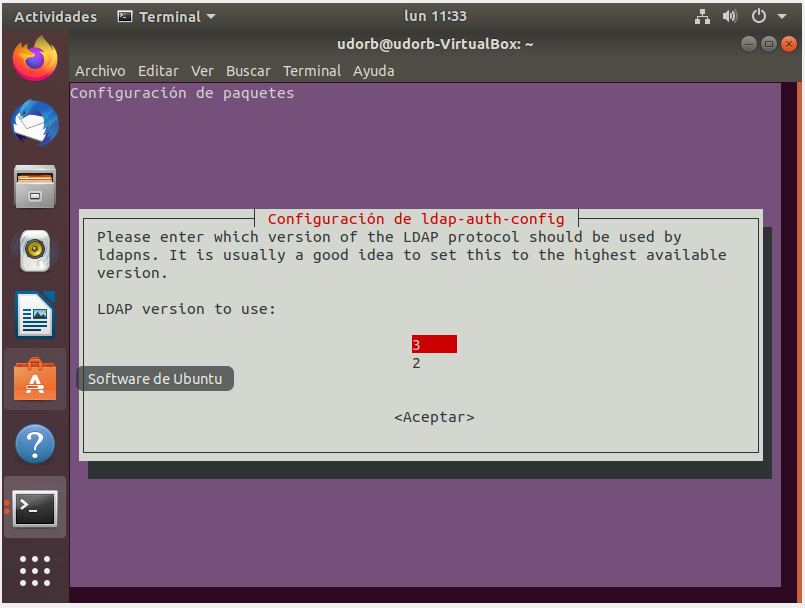
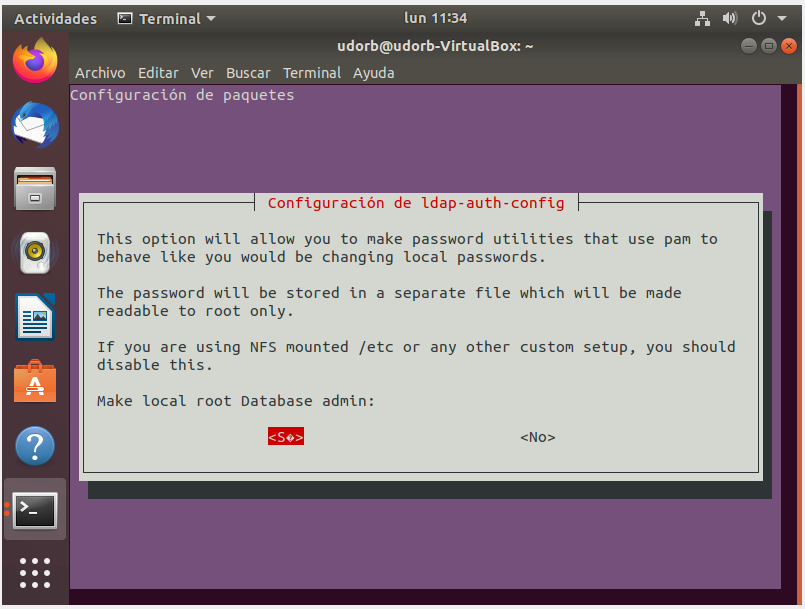


***Fes captures de tot el procès.***

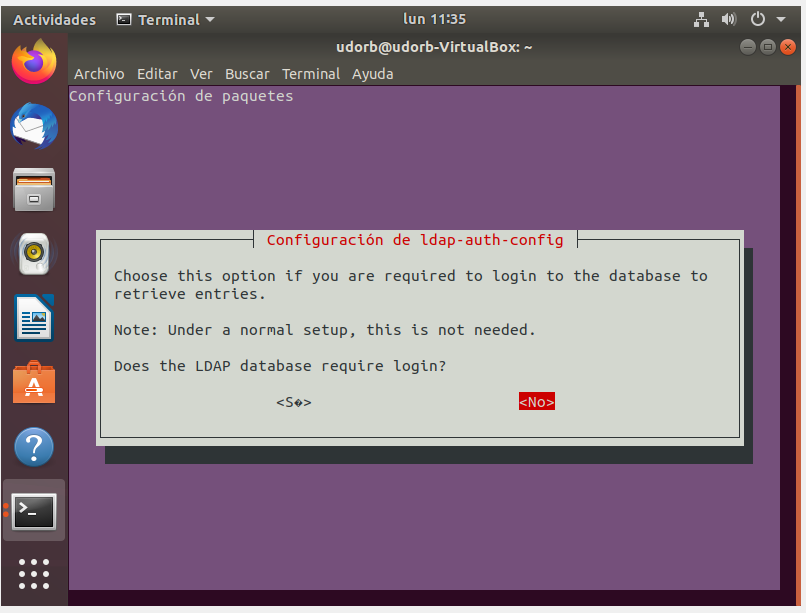
* 1. En el següent pas, hem d’indicar el nom global únic (Distinguished Name – DN). Inicialment apareix en valor dc=example,dc=net però nosaltres ho substituirem pel nostre:

dc=ldapxxx,dc=local

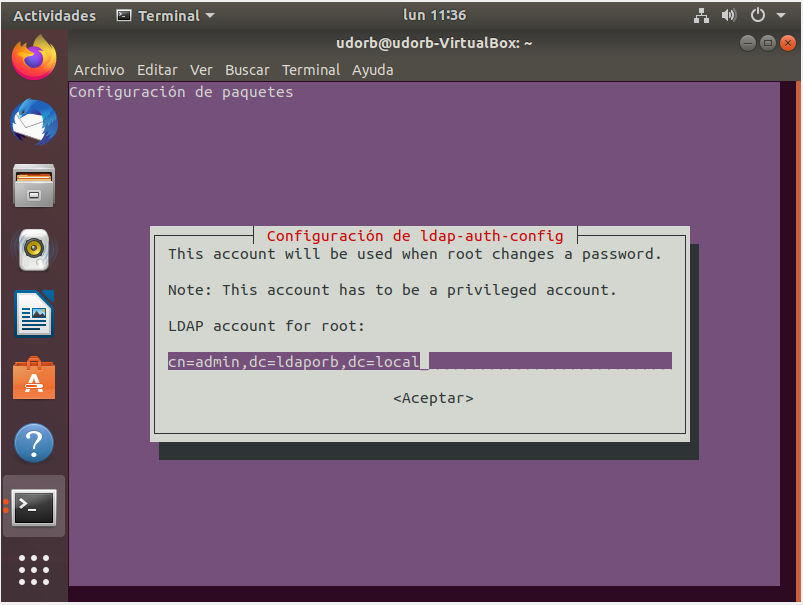
***Fes captures de tot el procès.***

* 1. Ara l’assistent ens demanrà la versió del protocol LDAP. Per defecte ja surt seleccionada la versió 3
  2. En aquest punt, l’assitent ens demanarà si volem que les utilitats que utilitzen PAM s’hauran de de comportar de la mateixa manera que quan canviem contrasenyes locals. Les contrasenyes es guadaran en un arxiu independent que només podrà llegir el superusuari. 

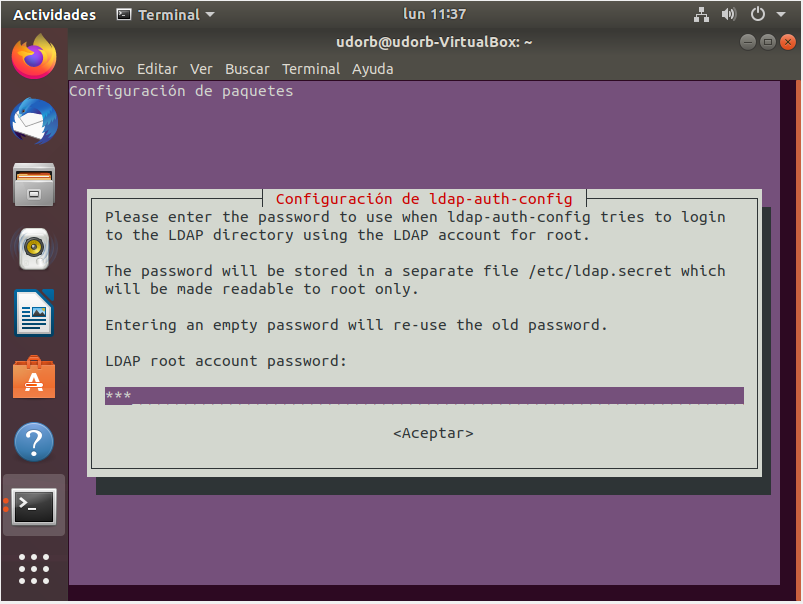
***Fes captures del resultat.***

* 1. Ara respondrem que NO sigui necessari identificar-se per realitzar consultes dins LDAP

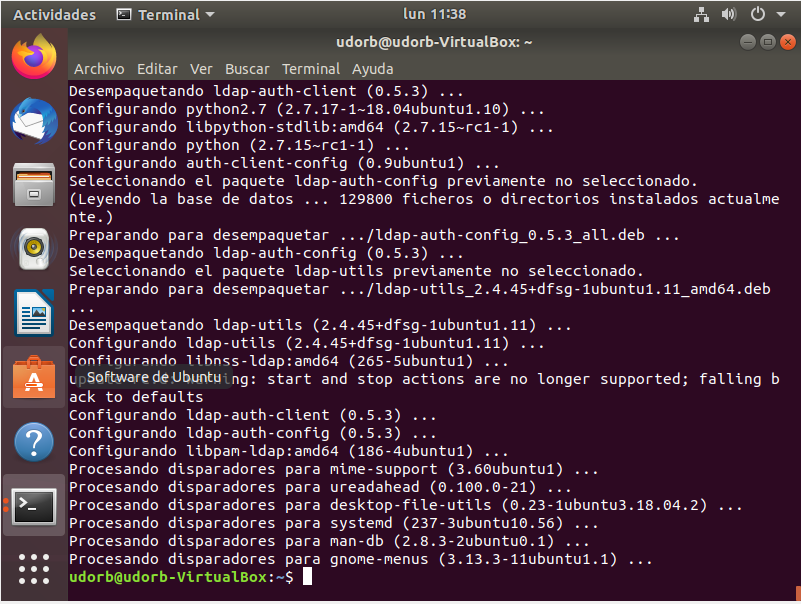
***Fes captures del resultat.***

* 1. Només ens queda indicar el nom del compte LDAP que tindrà privilegis per realitzar canvis en les contrasenyes. Haurem d’escriure el DN substituint el valor predefinit pel del nostre servidor (cn=admin, dc=ldapems, dc=local)

***Fes captures del resultat.***

* 1. Configurarem el password pel compte anterior (la posarem per duplicat) que coincidirà amb la que vam instal·lar a OpenLDAP al servidor.

***Fes captures del resultat.***

* 1. Un cop tornem al terminal, comprovarem que no han hagut errors durant el procés.

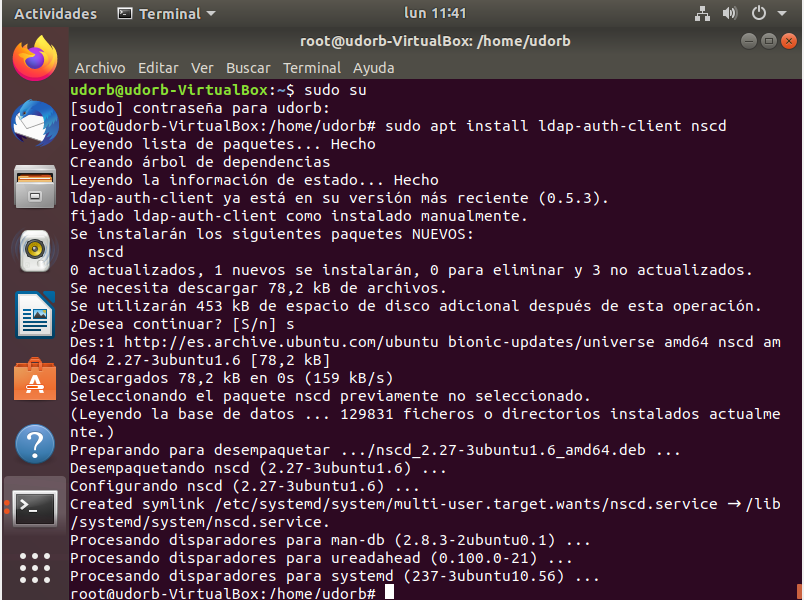
***Fes captures del resultat.***

* 1. En qualsevol moment podem reconfigurar el sistema mitjançant la comanda:

sudo dpkg-reconfigure ldap-auth-config

**Part 2: Configurar l’autenticació d’usuaris LDAP (NSS i configuració de PAM)**

Les següents comandes serveixen per configurar els serveis de validació de forma que utilitzin tant la base de dades d'usuaris locals (arxius /etc/password, /etc/shadow i /etc/group) com la base de dades del servei LDAP:

$ sudo apt install ldap-auth-client nscd

$ sudo auth-client-config -t nss -p lac\_ldap

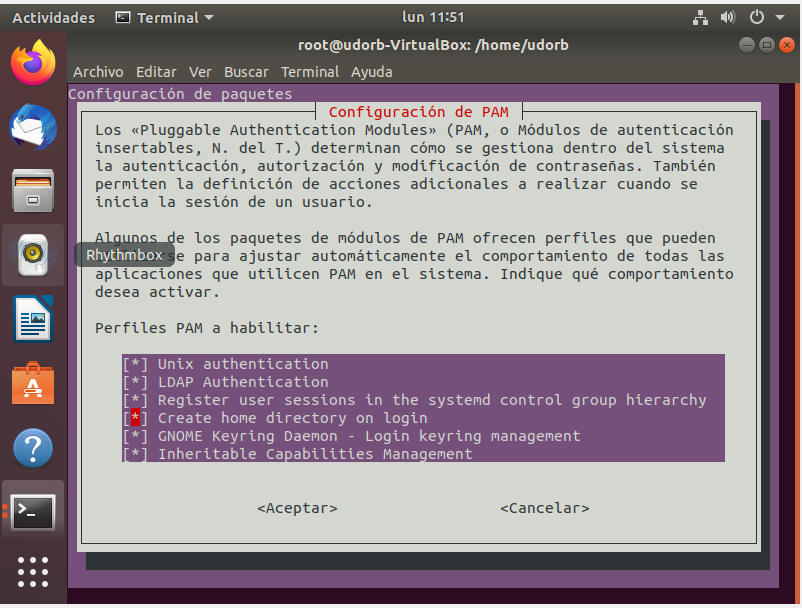
$ sudo pam-auth-update

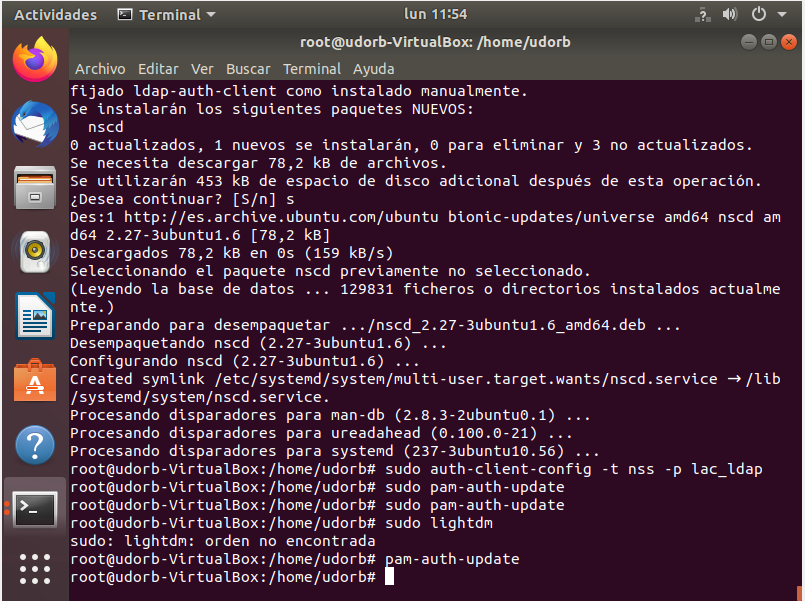
$ sudo lightdm

* 1. En la tercera comanda (sudo pam-auth-update) s'ha de marcar l'opció Create home directory on login. Si no se selecciona, no es crearà automàticament el directori de l'usuari i no podrà iniciar sessió (en el mode gràfic) o no tindrà un directori on guardar els seus arxius. Actualitzem la configuració de polítiques de PAM mitjançant la comanda

$ sudo pam-auth-update

Apareixerà un assistent, que comença mostrant-nos una pantalla informativa sobre la funció dels mòduls PAM. Has de marcar la opció “Crear directory home al fer login”

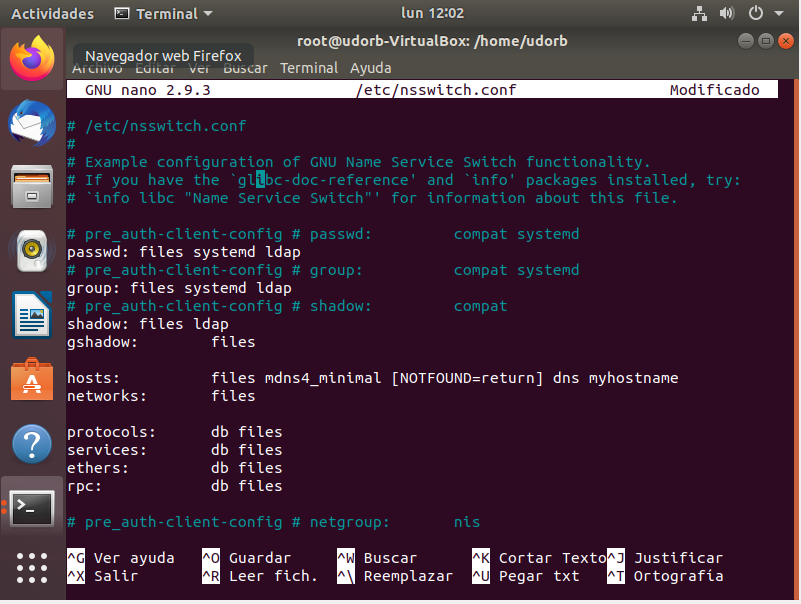


***Fes captures del resultat.***

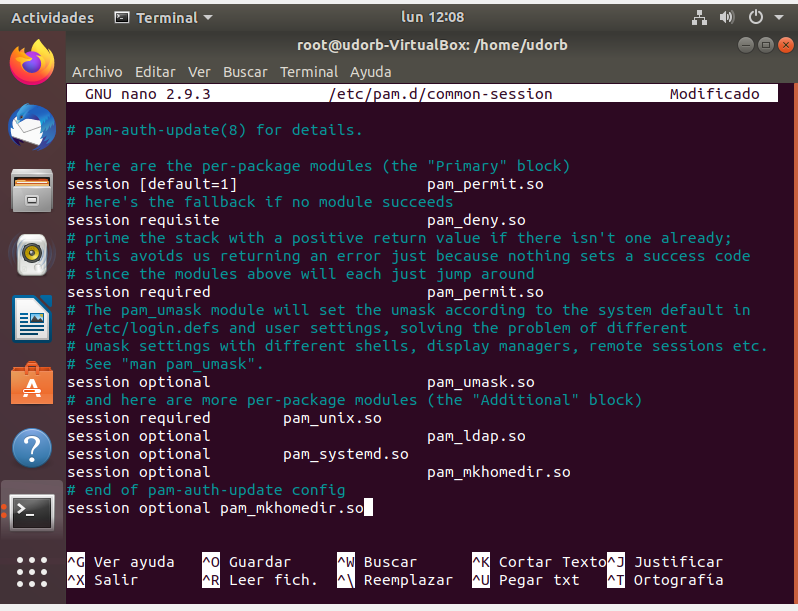
* 1. En l'arxiu **/etc/nsswitch.conf**, afegir el valor ldap al final de les línies que comencen amb les variables passwd i group:

$ sudo nano /etc/nsswitch.conf

passwd: files systemd **ldap**

group: files systemd **ldap**

* 1. Per crear el directori personal de cada usuari hem d’editar l’arxiu **/etc/pam.d/common-session** i afegir al final de l’arxiu el següent:

session optional pam\_mkhomedir.so

* 1. A partir d’ara, quan s'engegui la màquina, buscarà el servidor LDAP per validar els usuaris, per tant:
* Cal tenir engegat el servidor abans d'engegar el client.
* Cal apagar el client abans que el servidor.
* No s'hauria de canviar l'adreça del servidor (si es canvia, cal [reconfigurar el client LDAP](https://seicoll.gitbooks.io/sox/content/uf2.-sistemes-operatius-lliures-en-xarxa/uf2-gestio-dominis/uf2-auteticacio-ldap.html#reconfigurar-el-client-ldap)).

finalment hem de reiniciar el sistema



**Part 2: Comprovar que es veuen els usuaris i grups LDAP**

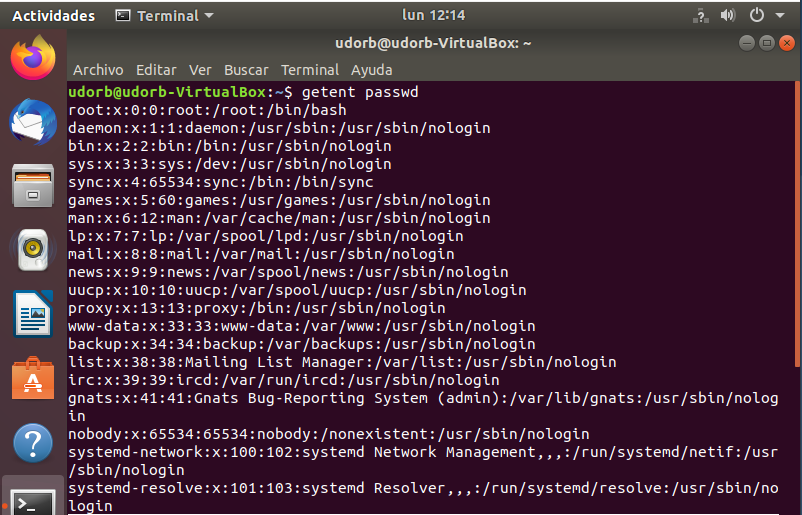
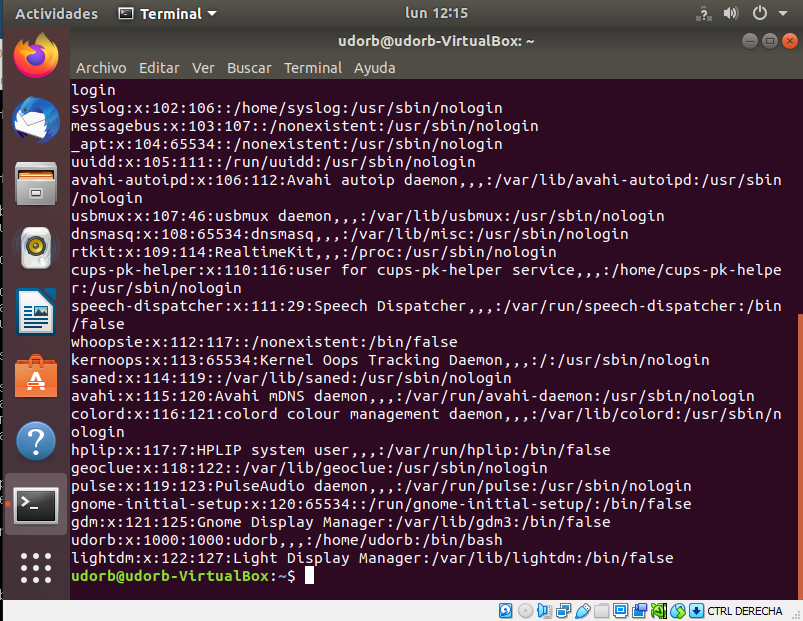
* 1. Si s'ha configurat correctament el client LDAP, es podran veure els usuaris i grups LDAP amb la comanda

$ getent passwd

S'haurien de veure tots els usuaris i grups, tant els locals com els que s'han creat amb LDAP.

Els usuaris i grups LDAP es distingeixen per les següents dades:

* Tenen un \* en lloc d'una x en el segon camp.
* L'identificador ha de ser superior o igual a 10000.
* La carpeta personal ha d'estar dins de **/home/ldapxxx**.

Si no es veuen els usuaris i grups LDAP, s'ha de reconfigurar el client LDAP.

**Part 3: Validar usuaris**

* 1. Per validar usuaris des de l’entorn gràfic, hem **d'activar el login d’Ubuntu** a la màquina client per poder escriure el nom de l’usuari.

Cal crear el fitxer /etc/lightdm/lightdm.conf i afegir el següent:

[Seat:\*]

greeter-hide-users=false

greeter-show-manual-login=true

* **greeter-hide-users**: amaga (true) o mostra (false) la llista dels últims usuaris que han accedit.
* **greeter-show-manual-login**: si és true, obliga a introduir manualment l'identificador de l'usuari.

Per carregar aquesta configuració cal reiniciar **lightdm** (es tancarà la sessió):

sudo service lightdm restart