Actividad - LDAP. Conectar cliente Ubuntu a Openldap server:

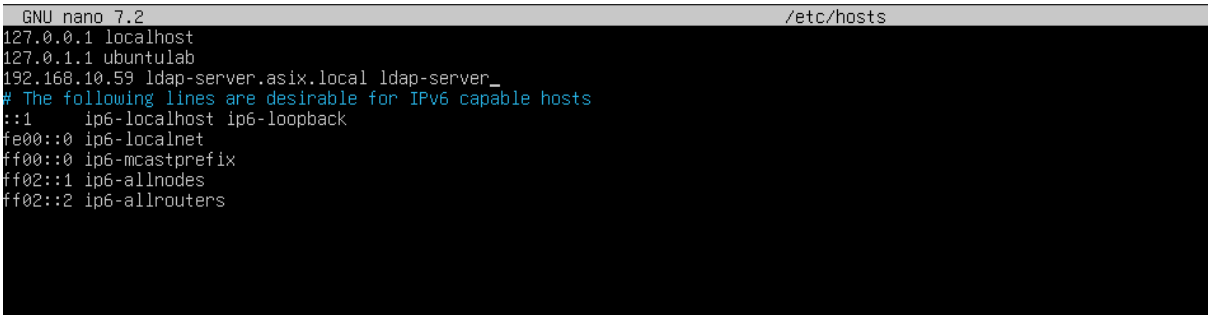
1. Introducción:

Esta guía detalla el procedimiento técnico para configurar la estación de trabajo Ubuntu (cliente) con IP 192.168.10.64 para autenticar usuarios centralizados alojados en el servidor OpenLDAP (192.168.10.59)

Esta guía asume que el servidor OpenLDAP está operativo y configurado con el dominio base: **dc=asix,dc=local**

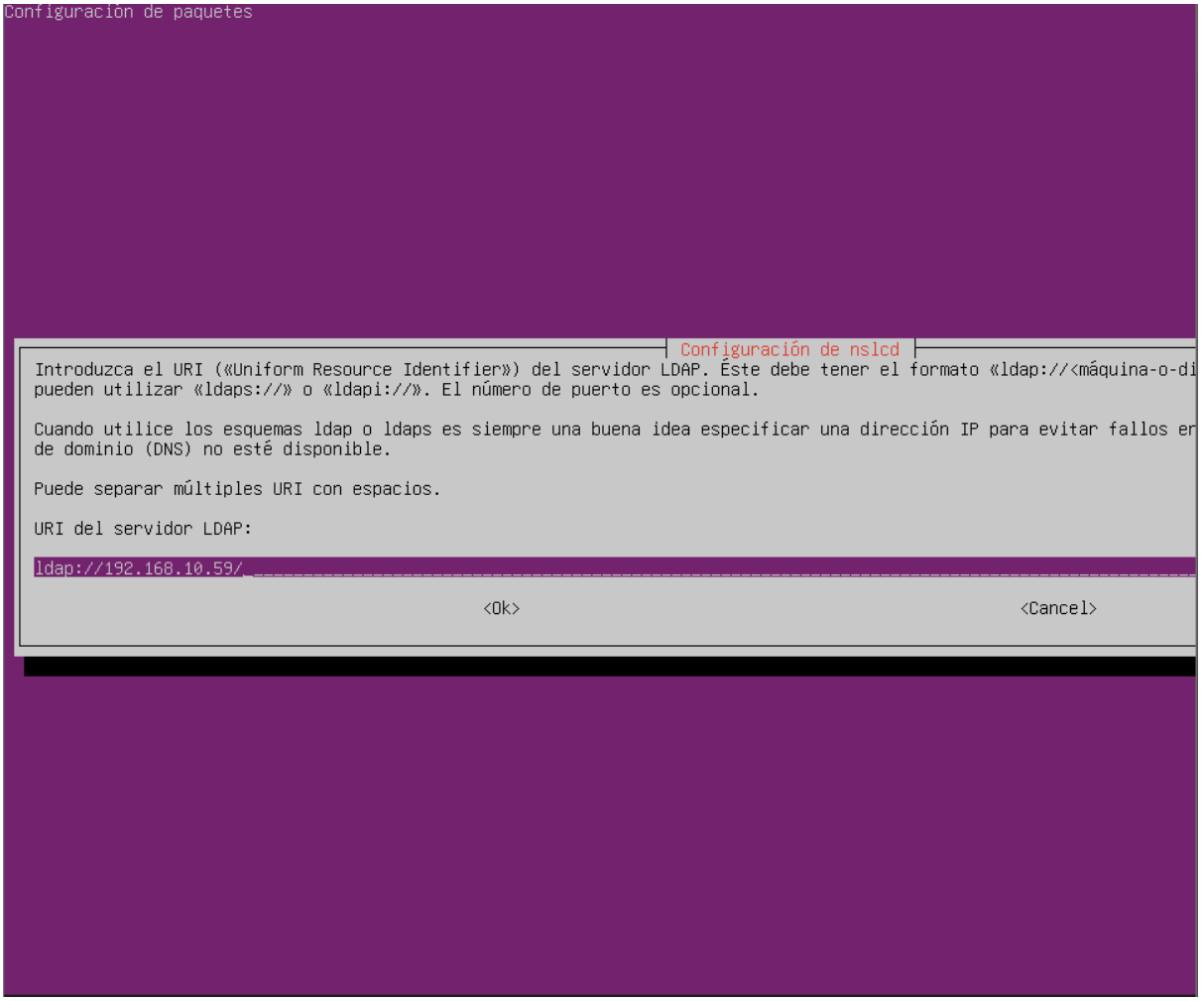
2. Configuración:

1. En el cliente ejecutamos el comando “sudo nano /etc/hosts” y añadimos lo siguiente al final del archivo: “192.168.10.59 ldap-server.asix.local ldap-server”

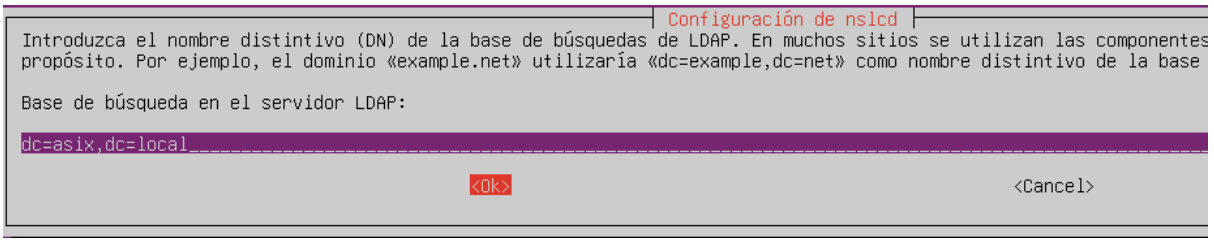


2. Instalamos las librerías LDAP con el siguiente comando: “**sudo apt update**” para actualizar la lista de repositorios y ejecutamos “**sudo apt install libnss-ldapd libpam-ldapd nscd**” para ejecutar la instalación:

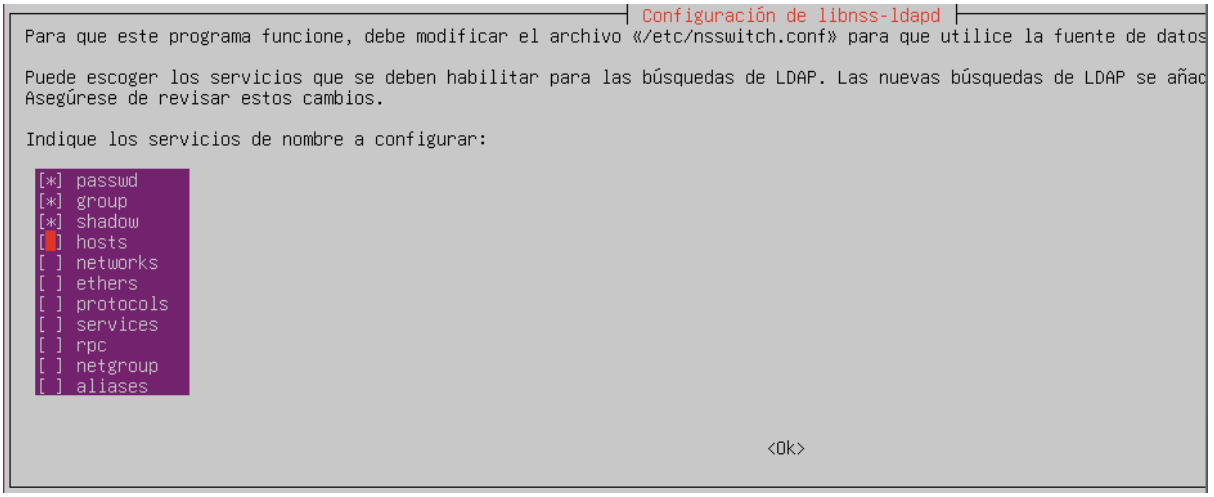
3. Nos pedirá la URL del servidor LDAP, la introducimos en este formato: “**ldap://192.168.10.59/**” (podríamos poner tambien “**ldap://ldap-server.asix.local/**”pero ponemos la IP directa para evitar problemas con el DNS):



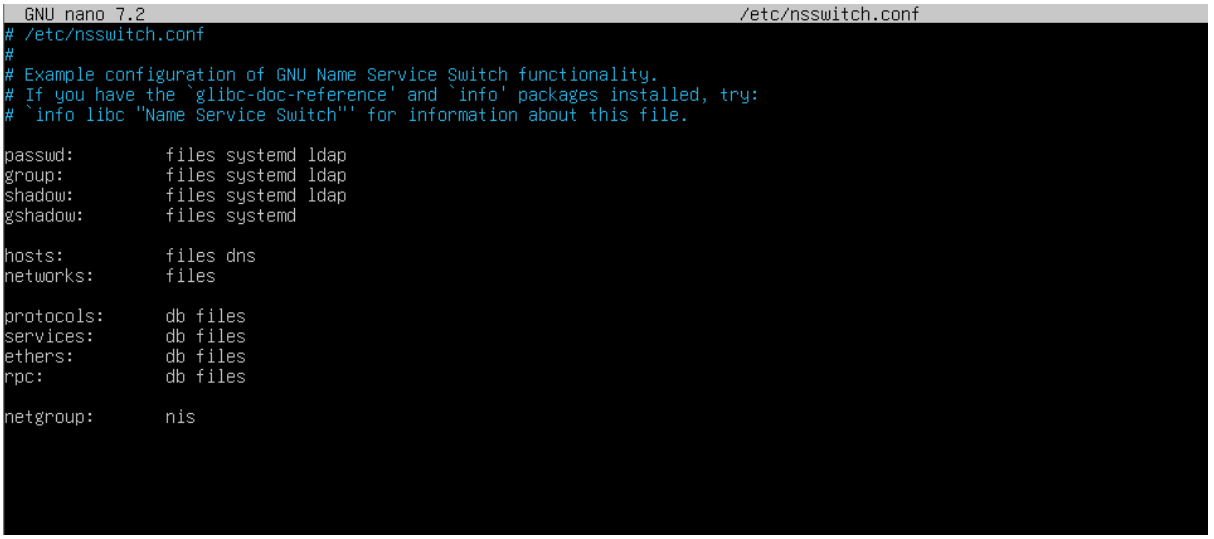
4. Configuramos la base de búsqueda: “**dc=asix,dc=local**” y pulsamos ok:



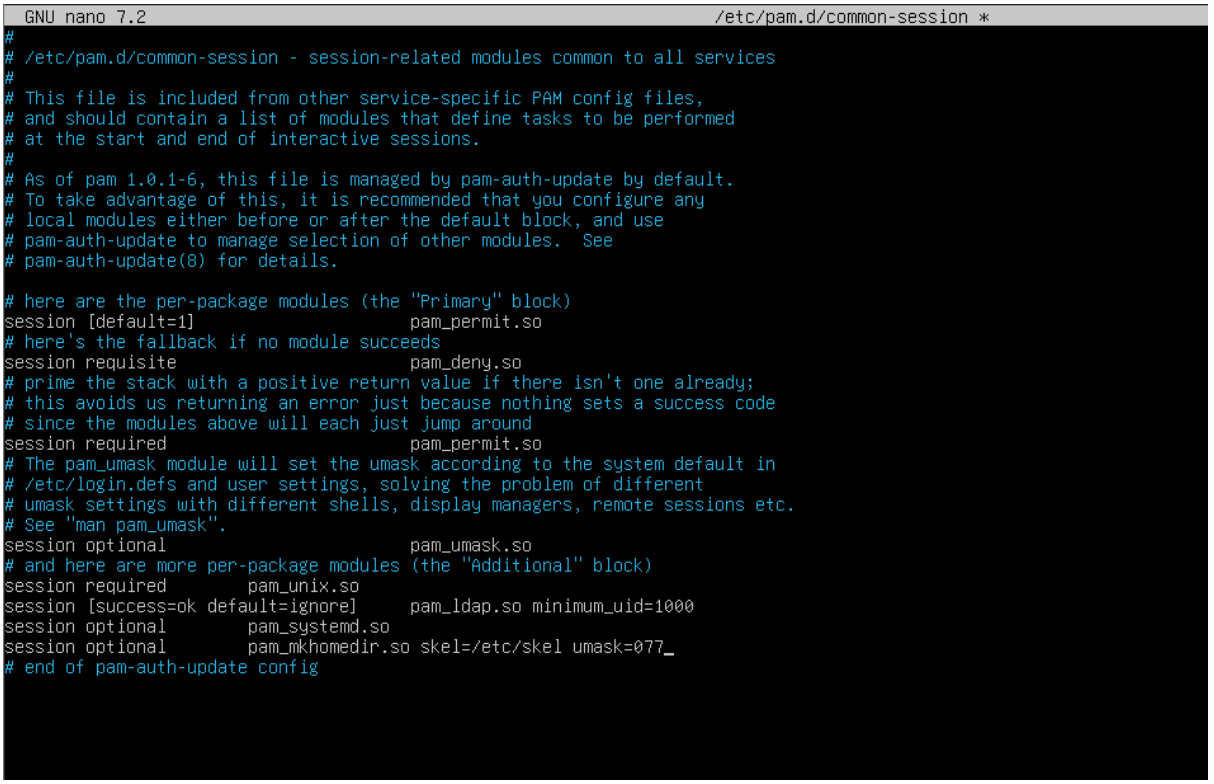
5. Marcamos “**passwd**”, “**group**” y “**shadow**” pulsando con barra espaciadora sobre ellos:



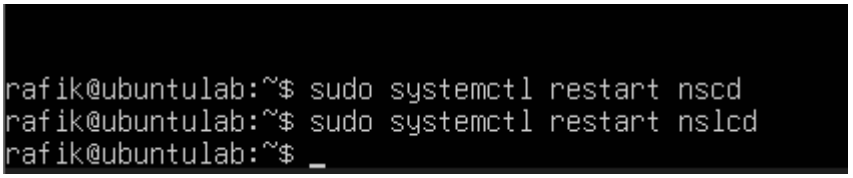
6. Ejecutamos “**sudo nano /etc/nsswitch.conf”** y comprobamos que las lineas de usuario y grupos contengan **ldap**:



7. Como los usuarios del dominio LDAP no tienen una carpeta personal creada físicamente en el cliente, se debe configurar PAM para generarla automáticamente en el primer inicio de sesión, para ello ejecutamos "**sudo nano /etc/pam.d/common-session**" y añadimos la siguiente linea alfinal del documento: "**session optional pam_mkhomedir.so skel=/etc/skel umask=077**":

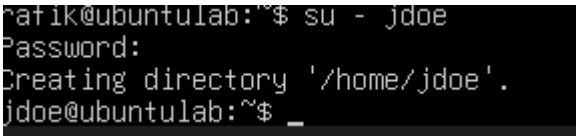


8. Aplicamos estos cambios reiniciando LDAP: "**sudo systemctl restart nscd**" y "**sudo systemctl restart nslcd**":



9. Comprobamos la conexión entre cliente (.64) y servidor (.59), para ello usaremos el comando "**getent passwd jdoe**". Si esta bien configurado, nos devolverá la información del usuario del servidor:

10. Ahora suplantamos la identidad del usuario **jdoe** para verificar el acceso y la creación del directorio home usando el comando: "**su - jdoe**":



Para acabar de comprobar que está bien configurado, abriremos una terminal de windows shell y nos conectaremos al cliente usando el usuario de LDAP: "**ssh jdoe@192.168.10.64**". Nos pedirá la contraseña del usuario y si queremos guardar la fingerprint, decimos "**Yes**" y ya estaremos conectados a la máquina a través de SSH, mediante el usuario de LDAP:

```
PS C:\Users\rafik> ssh jdoe@192.168.10.64
The authenticity of host '192.168.10.64 (192.168.10.64)' can't be established.
ED25519 key fingerprint is SHA256:xfMvk4f1SPGCkEWBWligiuO+wThfbdE1mpdOF9nR8/E.
This host key is known by the following other names/addresses:
    C:\Users\rafik/.ssh/known_hosts:4: 192.168.1.40
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.10.64' (ED25519) to the list of known hosts.
jdoe@192.168.10.64's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-88-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of lun 01 dic 2025 18:50:12 UTC

  System load:  0.08              Processes:               123
  Usage of /:   44.2% of 11.21GB  Users logged in:         1
  Memory usage: 12%               IPv4 address for enp0s3: 192.168.10.64
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge
```

```
 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 0 actualizaciones de forma inmediata.

6 actualizaciones de seguridad adicionales se pueden aplicar con ESM Apps.
Aprenda más sobre cómo activar el servicio ESM Apps at https://ubuntu.com/esm



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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

jdoe@ubuntulab:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:07:b3:2d brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.64/24 metric 100 brd 192.168.10.255 scope global dynamic enp0s3
       valid_lft 18786sec preferred_lft 18786sec
    inet6 fe80::a00:27ff:fe07:b32d/64 scope link
       valid_lft forever preferred_lft forever
jdoe@ubuntulab:~$
```

Esto nos hará más fácil administrar y monitorizar los usuarios de diferentes VM.