

# 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”

```
GNU nano 7.2 /etc/hosts
127.0.0.1 localhost
127.0.1.1 ubuntu1ab
192.168.10.59 ldap-server.asix.local ldap-server_
# 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
```

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 también  
“**ldap://ldap-server.asix.local/**” pero ponemos la IP directa para evitar problemas  
con el DNS):

Configuración de paquetes

Configuración de nsld

Introduzca el URI («Uniform Resource Identifier») del servidor LDAP. Este debe tener el formato «ldap://máquina-o-dominio». El número de puerto es opcional.  
pueden utilizar «ldaps://» o «ldapi://». El número de puerto es opcional.

Cuando utilice los esquemas ldap o ldaps es siempre una buena idea especificar una dirección IP para evitar fallos en caso de que el dominio (DNS) no esté disponible.

Puede separar múltiples URI con espacios.

URI del servidor LDAP:

ldap://192.168.10.59/

<Ok> <Cancel>

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

Configuración de nsld

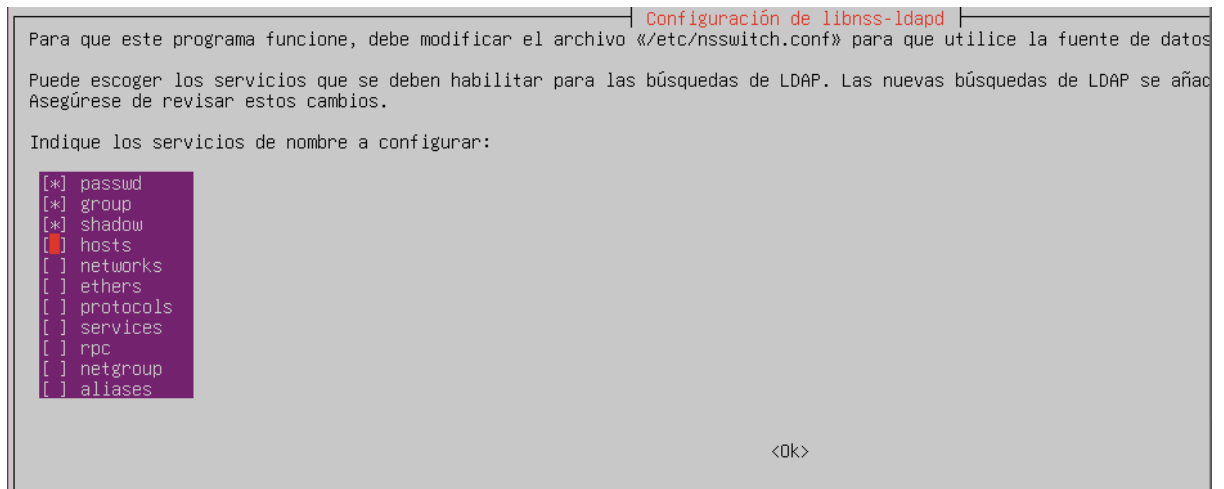
Introduzca el nombre distintivo (DN) de la base de búsquedas de LDAP. En muchos sitios se utilizan las componentes de la base de búsqueda. Por ejemplo, el dominio «example.net» utilizaría «dc=example,dc=net» como nombre distintivo de la base de búsqueda.

Base de búsqueda en el servidor LDAP:

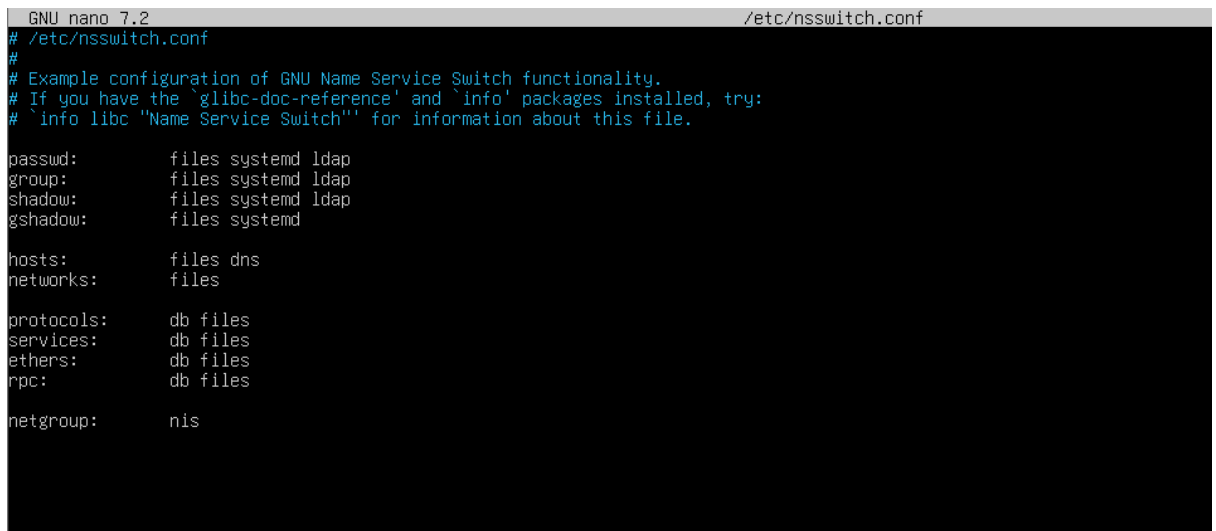
dc=asix,dc=local

<Ok> <Cancel>

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



6. Ejecutamos “**sudo nano /etc/nsswitch.conf**” y comprobamos que las líneas 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 línea al final del documento: “**session optional pam\_mkhomedir.so skel=/etc/skel umask=077**”:

```
GNU nano 7.2 /etc/pam.d/common-session *
#
# /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
# 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 [success=ok default=ignore] pam_ldap.so minimum_uid=1000
session optional pam_systemd.so
session optional pam_mkhomedir.so skel=/etc/skel umask=077_
# end of pam-auth-update config
```

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

```
rafik@ubuntulab:~$ sudo systemctl restart nscd
rafik@ubuntulab:~$ sudo systemctl restart nslcd
rafik@ubuntulab:~$ _
```

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

```
rafik@ubuntulab:~$ getent passwd jdoe
jdoe:x:10000:5000:John Doe:/home/jdoe:/bin/bash
```

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

```
rafik@ubuntulab:~$ su - jdoe
Password:
Creating directory '/home/jdoe'.
jdoe@ubuntulab:~$ _
```

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:xfMvk4f1SPGCKEWBwLgiu0+wThfbdE1mpd0F9nR8/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.