ASO

ADMINISTRACIÓN DE SISTEMAS OPERATIVOS

TEMA 4

Administración del servicio de directorio en Linux

Práctica 1:
“Instalación y configuración básica del servidor openLDAP”
+
Práctica 2:
“Creación de usuarios y grupos OpenLDAP”

2CFSH

GERARDO CANO

Por si cabe la posibilidad de subir ese 'regular' de la práctica 1 (espero que sí) presento en esta memoria la práctica 1 y la 2 concatenadas. Estaría genial que reconsiderases, porfi, la nota de la 1 y lo tomes en cuenta. Muchas gracias!!!

Empiezo de cero instalando nuevas máquinas virtuales:

TAREA 1:

Se debe realizar una memoria de toda la instalación y configuración del sistema. El nombre del dominio debe ser: nombreApellidos.ldap

SOLUCIÓN 1:

1. Antes de iniciar la instalación de Open LDAP se debe asignar una dirección IP fija en el servidor. Para ello editamos el fichero 90-NM-1eef7e45-369d-3043-bee3-fc5925c90273.yaml

~$ sudo nano /etc/netplan/90-NM-1eef7e45-369d-3043-bee3-fc5925c90273.yaml

```
administrador@Srvbnt:/etc/netplan$ sudo cat 90-NM-1eef7e45-3b9d-3043-bee3-fc5925c90273.yaml
network:
  version: 2
  ethernets:
    enp0s3:
      renderer: NetworkManager
      match: {}
      addresses:
      - "192.168.1.106/24"
      nameservers:
        addresses:
        - 8.8.8.8
        - 8.8.4.4
      networkmanager:
        uuid: "1eef7e45-3b9d-3043-bee3-fc5925c90273"
        name: "netplan-enp0s3"
        passthrough:
          connection.timestamp: "1766830275"
          ipv4.address1: "192.168.1.106/24,192.168.1.1"
          ipv4.method: "manual"
          ipv6.method: "disabled"
          ipv6.ip6-privacy: "-1"
          proxy._: ""
```

Le doy la ip fija 192.168.1.106 tras comprobar que la tengo libre

```
administrador@Srvbnt:~$ sudo netpla apply
[sudo] contraseña para administrador:
sudo: netpla: orden no encontrada
administrador@Srvbnt:~$ sudo netplan apply
administrador@Srvbnt:~$
```

2. Modifico el contenido del fichero /etc/hosts para indicar un FQDN (fully qualified domain name) a nuestro servidor.

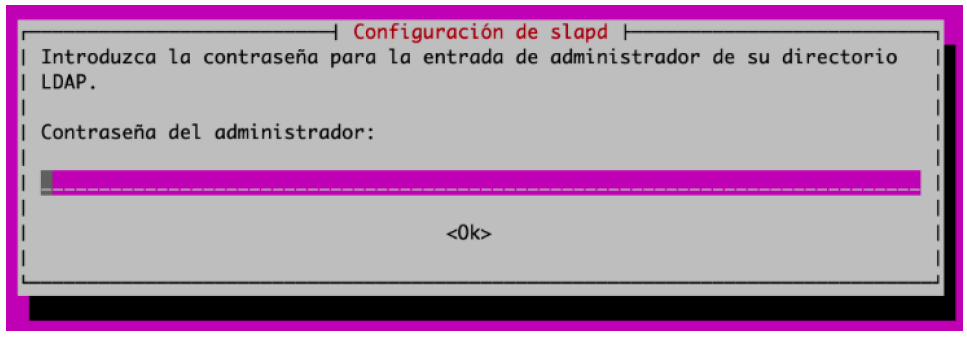
```
administrador@Srvbnt:~$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 gerardocanobustos.ldap Srvbnt

# 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
administrador@Srvbnt:~$
```

3. Actualizo la lista de paquetes de software disponibles en los repositorios oficiales, e instalar los paquetes necesarios en el servidor. Para ello ejecutamos el siguiente comando:

```
sudo apt update && sudo apt install slapd
```

Automáticamente nos aparecerá una ventana donde introduciremos la contraseña de administrador para el directorio LDAP. (Yo he usado ‘123456’) y seguidamente terminará el proceso de instalación.



Compruebo que se ha instalado correctamente ejecutando el comando slapcat. Dicho comando muestra en formato LDIF el contenido de las entradas existentes en el servicio de directorio.

sudo slapcat

```
administrador@Srvbnt:~$ sudo slapcat
dn: dc=ldap
objectClass: top
objectClass: dcObject
objectClass: organization
o: ldap
dc: ldap
structuralObjectClass: organization
entryUUID: cbf098f4-7767-1040-8ea5-83f8a2f4bfdd
creatorsName: cn=admin,dc=ldap
createTimestamp: 20251227120327Z
entryCSN: 20251227120327.136100Z#000000#000#000000
modifiersName: cn=admin,dc=ldap
modifyTimestamp: 20251227120327Z

administrador@Srvbnt:~$
```

4. Compruebo el estado con:

systemctl status slapd.service

```
administrador@Srvbnt:~$ systemctl status slapd.service
● 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 Sat 2025-12-27 13:03:28 CET; 32min ago
       Docs: man:systemd-sysv-generator(8)
      Tasks: 3 (limit: 4601)
     Memory: 3.5M (peak: 4.4M)
        CPU: 49ms
     CGroup: /system.slice/slapd.service
             └─2172 /usr/sbin/slapd -h "ldap:/// ldapi:///" -g openldap -u openldap -F /etc/ldap/slapd.d

dic 27 13:03:27 Srvbnt systemd[1]: Starting slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)...
dic 27 13:03:28 Srvbnt slapd[2165]:  * Starting OpenLDAP slapd
dic 27 13:03:28 Srvbnt slapd[2171]: @(#) $OpenLDAP: slapd 2.6.7+dfsg-1~exp1ubuntu8.2 (Dec  9 2024 02:50:18) $
                                    Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
dic 27 13:03:28 Srvbnt slapd[2172]: slapd starting
dic 27 13:03:28 Srvbnt slapd[2165]:    ...done.
dic 27 13:03:28 Srvbnt systemd[1]: Started slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol).
administrador@Srvbnt:~$
```

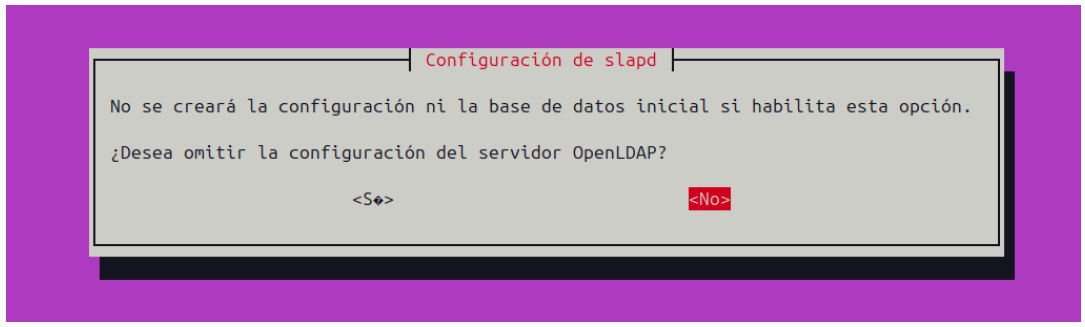
5. Compruebo si el servicio de directorio OpenLdap esta escuchando por el puerto 389.

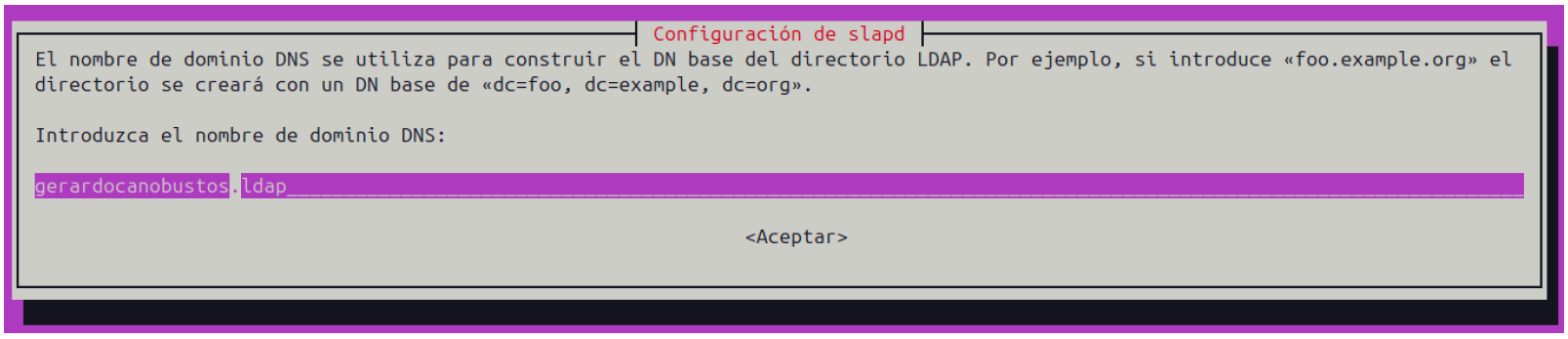
```
administrador@Srvbnt:~$ ss -nltp
State          Recv-Q         Send-Q                 Local Address:Port                  Peer Address:Port        Process
LISTEN         0              4096                   127.0.0.53%lo:53                         0.0.0.0:*
LISTEN         0              4096                       127.0.0.1:631                        0.0.0.0:*
LISTEN         0              2048                       0.0.0.0:389                          0.0.0.0:*
LISTEN         0              4096                       0.0.0.0:22                           0.0.0.0:*
LISTEN         0              4096                      127.0.0.54:53                         0.0.0.0:*
LISTEN         0              2048                          [::]:389                             [::]:*
LISTEN         0              4096                          [::]:22                              [::]:*
LISTEN         0              4096                         [::1]:631                             [::]:*
```

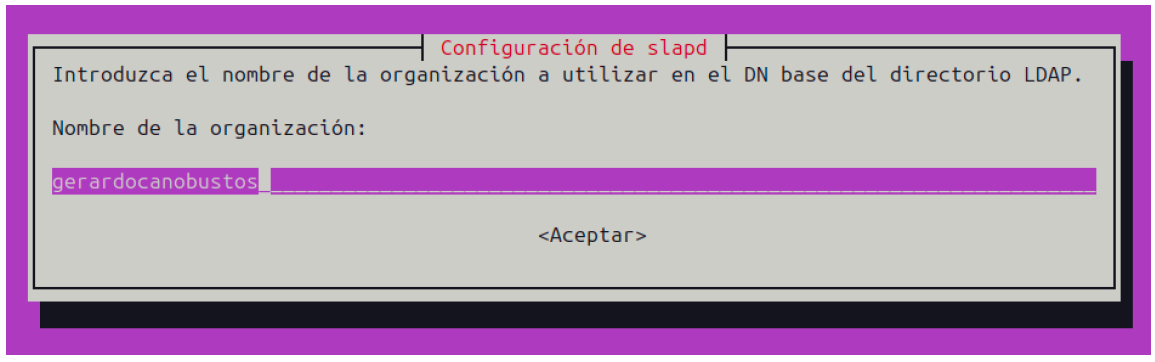
Efectivamente, será escuchado por cualquier IPv4 (0.0.0.0)

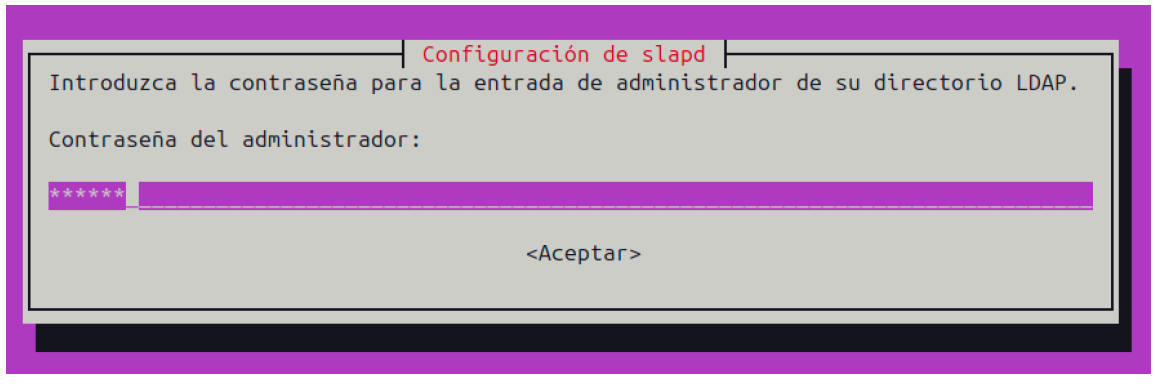
6. Configuro el servicio de directorio haciendo uso del comando:

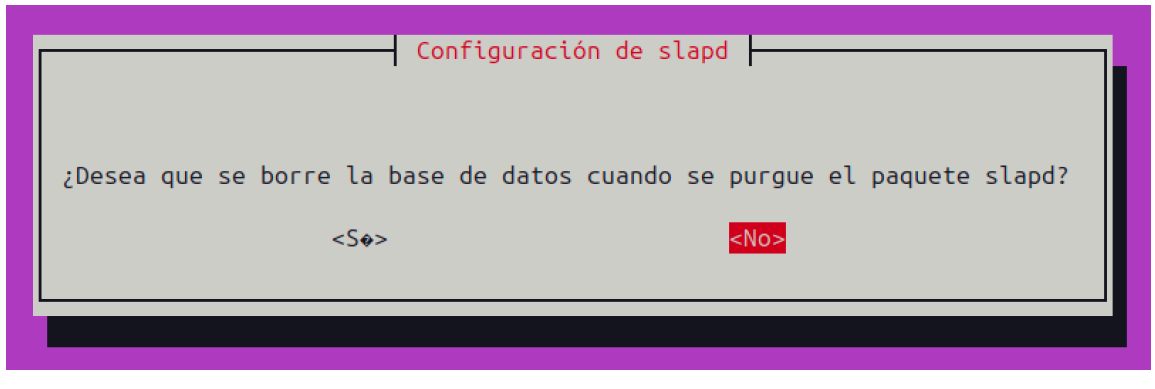
sudo dpkg-reconfigure slapd

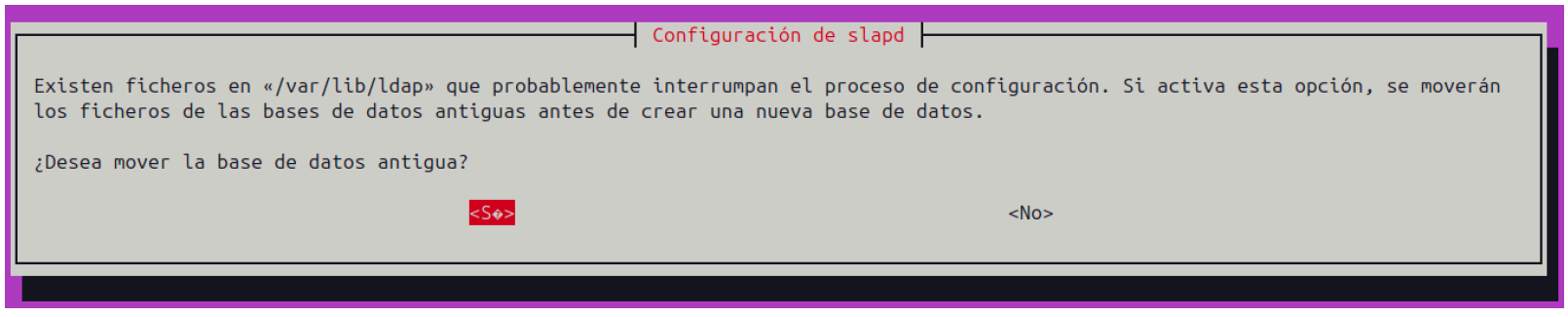













```
administrador@Srvbnt:~$ sudo dpkg-reconfigure slapd
  Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.6.7+dfsg-1~exp1ubuntu8.2... done.
  Moving old database directory to /var/backups:
  - directory unknown... done.
  Creating initial configuration... done.
  Creating LDAP directory... done.
administrador@Srvbnt:~$
```

7. Vuelvo a ejecutar el comando slapcat y se observa como se han modificado los valores de los atributos de las entradas, con los datos que se acaban de indicar.

sudo slapcat

```
dn: dc=gerardocanobustos,dc=ldap
objectClass: top
objectClass: dcObject
objectClass: organization
o: gerardocanobustos
dc: gerardocanobustos
structuralObjectClass: organization
entryUUID: 06ec8502-776e-1040-8e87-fbf1896ae71d
creatorsName: cn=admin,dc=gerardocanobustos,dc=ldap
createTimestamp: 20251227124803Z
entryCSN: 20251227124803.075318Z#000000#000#000000
modifiersName: cn=admin,dc=gerardocanobustos,dc=ldap
modifyTimestamp: 20251227124803Z
```

TAREA 2:

Se debe realizar un informe breve en pdf con las capturas:

- Captura del slapcat que confirme que se han creado y configurado los usuarios y grupos según el DIT que se aporta durante la guía.
- Captura del inicio de sesión con el usuario del cliente con CLI y GUI.

SOLUCIÓN 2:

Una vez que tenemos el servicio instalado y configurado, pasamos a crear la estructura básica del directorio. Es decir, la estructura jerárquica del árbol (DIT -- Directory Information Tree).

1. Creamos mediante ficheros LDIF (LDAP Data Interchange Format).

Son ficheros de texto plano pero tienen un formato particular como 'netplan' - por ejemplo - y otros muchos que se debe prestar atención.

Creamos un fichero base con el formato básico siguiendo su formato peculiar de entrada que debería ser algo así en mi caso:

```
sudo nano base.ldif
```

- En el LDIF se crean dos entradas referentes a unidades organizativas: «usuarios» y «grupos».
- Las unidades organizativas, como su propio nombre indica, son atributos que nos van a servir para estructurar de forma idónea el árbol del directorio LDAP.
- Estas dos entradas serán la base del árbol ya que de ellas dependerán varias entradas más adelante.
- Se genera el base.ldif con las siguientes entradas, cambiando aso por dominio de cada alumna o alumno.

Algo como esto:

```
administrador@Srvbnt:~$ sudo nano base.ldif
[sudo] contraseña para administrador:
administrador@Srvbnt:~$ cat base.ldif
dn: ou=usuarios,dc=gerardocanobustos,dc=ldap
objectClass: organizationalUnit
objectClass: top
ou: usuarios
dn: ou=grupos,dc=gerardocanobustos,dc=ldap
objectClass: organizationalUnit
objectClass: top
ou: grupos
administrador@Srvbnt:~$
```

2. Cargamos en el directorio LDAP (en la BD de ldap). Para ello se ejecuta la siguiente instrucción:

sudo ldapadd -x -D cn=admin,dc=aso,dc=ldap -W -f base.ldif

```
administrador@Srvbnt:~$ sudo ldapadd -x -D cn=admin,dc=gerardocanobustos,dc=ldap -W -f base.ldif
Enter LDAP Password:
ldapadd: attributeDescription "dn": (possible missing newline after line 7, entry "ou=usuarios,dc=gerardocanobustos,dc=ldap"?)
adding new entry "ou=usuarios,dc=gerardocanobustos,dc=ldap"
ldap_add: Type or value exists (20)
        additional info: objectClass: value #0 provided more than once

administrador@Srvbnt:~$ cat -n base.ldif
     1  dn: ou=usuarios,dc=gerardocanobustos,dc=ldap
     2  objectClass: organizationalUnit
     3  objectClass: top
     4  ou: usuarios
     5  dn: ou=grupos,dc=gerardocanobustos,dc=ldap
     6  objectClass: organizationalUnit
     7  objectClass: top
     8  ou: grupos
administrador@Srvbnt:~$ sudo nano base.ldif
administrador@Srvbnt:~$ cat -n base.ldif
     1  dn: ou=usuarios,dc=gerardocanobustos,dc=ldap
     2  objectClass: organizationalUnit
     3  objectClass: top
     4  ou: usuarios
     5
     6  dn: ou=grupos,dc=gerardocanobustos,dc=ldap
     7  objectClass: organizationalUnit
     8  objectClass: top
     9  ou: grupos
administrador@Srvbnt:~$ sudo ldapadd -x -D cn=admin,dc=gerardocanobustos,dc=ldap -W -f base.ldif
Enter LDAP Password:
adding new entry "ou=usuarios,dc=gerardocanobustos,dc=ldap"

adding new entry "ou=grupos,dc=gerardocanobustos,dc=ldap"

administrador@Srvbnt:~$
```

Fig 1. Tiene un ancla apuntado en la sección de 'problemas'

3. Ahora, Como buena práctica de seguridad, se genera una contraseña cifrada para asignarlas a los usuarios en el fichero LDIF que se va a crear.
   Ejecutamos el siguiente comando:

slappasswd

Se escribe la contraseña dos veces y nos devolverá la misma cifrada por el algoritmo criptográfico SSHA.

```
administrador@Srvbnt:~$ vim slappasswd.txt
administrador@Srvbnt:~$ cat slappasswd.txt
# aquí voy copiar el SSHA que se genere con el comando 'slappasswd'
administrador@Srvbnt:~$ slappasswd
New password:
Re-enter new password:
{SSHA}yxzLIwYJDVWGyA5exdG+uTnZKm3w/gXe
administrador@Srvbnt:~$ vim slappasswd.txt
administrador@Srvbnt:~$ cat slappasswd.txt
# aquí voy copiar el SSHA que se genere con el comando 'slappasswd'

{SSHA}yxzLIwYJDVWGyA5exdG+uTnZKm3w/gXe


administrador@Srvbnt:~$
```

4. Creamos dos entradas en un fichero ‘content.ldif’ donde usaremos la la contraseña cifrada creada anteriormente:

- Un grupo llamado devops que colgará de la unidad organizativa grupos.
- Un usuario llamado mordecai que colgará de la unidad organizativa usuarios y a su vez pertenece al grupo devops.

nano content.ldif

```
administrador@Srvbnt:~$ sudo nano content.ldif
[sudo] contraseña para administrador:
administrador@Srvbnt:~$ cat content.ldif
dn: cn=devops,ou=grupos,dc=gerardocanobustos,dc=ldap
objectClass: posixGroup
cn: devops
gidNumber: 10000
memberUid: devops
dn: uid=mordecai,ou=usuarios,dc=gerardocanobustos,dc=ldap
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Mordecai
sn: Geek
userPassword: {SSHA}yxzLIwYJDVWGyA5exdG+uTnZKm3w/gXe
loginshell: /bin/bash
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/mordecai
administrador@Srvbnt:~$
```

5. Procedemos a cargar las entradas en el directorio LDAP ejecutando el siguiente comando:

sudo ldapadd -x -D cn=admin,dc=aso,dc=ldap -W -f content.ldif

```
administrador@Srvbnt:~$ sudo nano content.ldif
administrador@Srvbnt:~$ sudo ldapadd -x -D cn=admin,dc=gerardocanobustos,dc=ldap -W -f content.ldif
Enter LDAP Password:
adding new entry "cn=devops,ou=grupos,dc=gerardocanobustos,dc=ldap"
ldap_add: No such object (32)
        matched DN: dc=gerardocanobustos,dc=ldap

administrador@Srvbnt:~$
```

Ahora, desde el cliente comprobamos que todo está en su sitio con un búsqueda simple:

```
administrador@DesktopBnt:~$ ldapsearch -x -H ldap://192.168.1.106 -b "dc=gerardo
canobustos,dc=ldap"
# extended LDIF
#
# LDAPv3
# base <dc=gerardocanobustos,dc=ldap> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# gerardocanobustos.ldap
dn: dc=gerardocanobustos,dc=ldap
objectClass: top
objectClass: dcObject
objectClass: organization
o: gerardocanobustos.ldap
dc: gerardocanobustos

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
administrador@DesktopBnt:~$
```

Ahora reiniciamos el servicio y comprobamos que está ‘up’

```
administrador@DesktopBnt:~$ sudo systemctl restart nslcd
administrador@DesktopBnt:~$ sudo systemctl status nslcd
● nslcd.service - LSB: LDAP connection daemon
     Loaded: loaded (/etc/init.d/nslcd; generated)
     Active: active (running) since Thu 2026-01-01 16:52:02 CET; 9s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 20259 ExecStart=/etc/init.d/nslcd start (code=exited, status=0/SUC>
      Tasks: 6 (limit: 19095)
     Memory: 1.7M (peak: 2.7M)
        CPU: 33ms
     CGroup: /system.slice/nslcd.service
             └─20270 /usr/sbin/nslcd

ene 01 16:52:00 DesktopBnt systemd[1]: Starting nslcd.service - LSB: LDAP conne>
ene 01 16:52:00 DesktopBnt nslcd[20259]:  * Starting LDAP connection daemon nsl>
ene 01 16:52:00 DesktopBnt nslcd[20268]: nslcd: Warning: NSS_LDAP version missi>
ene 01 16:52:00 DesktopBnt nslcd[20268]: nslcd: Warning: /lib/x86_64-linux-gnu/>
ene 01 16:52:00 DesktopBnt nslcd[20270]: version 0.9.12 starting
ene 01 16:52:02 DesktopBnt nslcd[20270]: accepting connections
ene 01 16:52:02 DesktopBnt nslcd[20259]:    ...done.
ene 01 16:52:02 DesktopBnt systemd[1]: Started nslcd.service - LSB: LDAP connec>
lines 1-19/19 (END)
```

Le preguntamos al servidor si conoce a ‘mordecai´ con el comando:

Getent passwd mordecai

Y debería responder con una linea que termina en */home/mordecai*

Pero no funciona!!! De ninguna de las formas!!! No me responde eso.

Al final, y después de muchos días de documentación y frustraciones…. Encontré esta documentación. Y conseguí hacerlo funcionar. Lo detallo todo en la sección de ‘problemas’.

```
administrador@DesktopBnt: ~
administrador@DesktopBnt:~$ getent passwd mordecai
mordecai:x:5001:5000:Mordecai:/home/mordecai:/bin/bash
administrador@DesktopBnt:~$ su -mrodecai
su: opción incorrecta -- «r»
Escriba 'su --help' para obtener más información.
administrador@DesktopBnt:~$ su - mordecai
Contraseña:
```

PROBLEMAS:

1. Un fallo en la sintaxis del archivo base.ldif. Ya sabía que es un archivo muy ‘especializo’ e incluso poniendo especial atención lo hice mal y después me costó un ratito encontrar el error. Era problemas menores (pero que te pueden volver loco) de que no detectaba una separación y que el sistema leyó el segundo dn: (línea 5) como si fuera un atributo más.

2. No había forma de que el comando `Getent passwd mordecai` me respondiese con una linea que termina en `/home/mordecai`

   De esta forma, la práctica no estaba terminada. No iba a darme por vencido y prefería presentarla fuera de plazo pero acabada.

SOLUCIÓN A LOS PROBLEMAS:

1. Modificando el archivo ‘base.ldif’ con la sintaxis correcta.
2. Después de varios días de darle vueltas y buscar documentación, leerla y asimilarla, me Dao cuenta que el problema que estoy experimentando no es un "bug" (fallo de código) per se, sino un **conflicto de arquitectura de paquetes** que está documentado en las páginas de manual (man pages) y en el repositorio oficial de Debian/Ubuntu.

En el ecosistema Ubuntu, existen dos implementaciones del servicio de nombres para LDAP que son **incompatibles** entre sí si no se configuran con cuidado.

- **libnss-ldap (El paquete que tenía):** Desarrollado originalmente por **PADL Software**. Su documentación oficial indica que es una librería que se carga directamente en cada proceso que necesita buscar un usuario.

- **libnss-ldapd (La alternativa con "d"):** Desarrollado por **Arthur de Jong**. Esta versión no busca en LDAP directamente, sino que delega la búsqueda al demonio nslcd. *Enlace al Manual Oficial:* manpages.ubuntu.com - nslcd

Si estudiamos la descripción oficial del paquete nslcd en el repositorio de Ubuntu (Noble Numbat 24.04), veremos que dice:

"This package provides a daemon (nslcd) that does LDAP queries for name service lookups... It is a rewrite of the libnss-ldap and pam_ldap modules."

— Ubuntu Packages - nslcd (24.04 LTS)

El conflicto técnico: Tengo instalado el demonio nslcd, pero tu sistema está intentando usar la librería de PADL. Esta librería **no sabe hablar con el demonio nslcd**; intenta abrir su propio archivo de configuración en /etc/libnss-ldap.conf.

Como configuré /etc/nslcd.conf, el demonio tiene la información, pero la librería (libnss-ldap) está buscando en un archivo que no existe o está vacío. Por eso getent devuelve nada.

LA SOLUCIÓN DOCUMENTADA

La recomendación oficial para sistemas modernos (post-Ubuntu 20.04) es usar el stack de **nss-pam-ldapd**.

Para ver el "link oficial" de por qué se prefiere esto, puedes revisar el **Debian Wiki** (que es la base de Ubuntu) sobre LDAP:

- Wiki Debian - LDAP/NSS

CITA: "THERE ARE TWO DIFFERENT IMPLEMENTATIONS... NSS-PAM-LDAPD IS GENERALLY CONSIDERED MORE ROBUST BECAUSE IT USES A SEPARATE DAEMON (NSLCD).

Resumen del caso:

Para que getent funcione usando el demonio nslcd que ya tenía corriendo y configurado, **debo sustituir la librería**:

1. sudo apt remove libnss-ldap
2. sudo apt install libnss-ldapd (esta es la que se conecta al archivo /etc/nslcd.conf).

Lo he dejado explicado un poco mejor (creo) en mi Blog.

https://asir.gerardocano.com/autenticacion-centralizada-ldap-en-linux/