

Documentación de Openldap

-Luis Piqueras López-

Teoría.....	3
NSS.....	3
PAM.....	3
LDAP.....	3
Open LDAP.....	3
Configuración de red del entorno de pruebas.....	4
1 Instalar en un servidor.....	5
Configuración inicial.....	6
Comprobación de la instalación.....	8
Administración de openldap.....	8
Creación de una unidad organizativa.....	8
Creación grupo.....	9
Añadir a un usuario y encriptar contraseña.....	10
Ejemplo ldif de usuario:.....	11
Borrar.....	12
Búsquedas.....	12
1. Comando básico.....	12
2. Parámetros clave.....	12
3. Filtros de búsqueda.....	13
4. Ámbito de búsqueda.....	13
5. Resultados de la búsqueda.....	13
6. Ejemplos.....	13
Configurar manual para autenticar un cliente en el servidor.....	15
ajustes en los archivos de configuración.....	18
Comprobación.....	19
conexión desde el cliente.....	20
Interfaz gráfica web ldap.....	21
gestionar usuarios y grupos en el servidor desde la interfaz gráfica.....	26
Cuentas de grupo.....	28
nuevo grupo.....	29
Scripts.....	30
Script1 unir cliente (Comentado).....	30
Explicación script 1.....	32
Paquetes instalados:.....	32
/etc/nsswitch.conf.....	32
/etc/pam.d/common-password.....	33
/etc/pam.d/common-session.....	33
Script 2.....	33
Explicación de scripts de monitorización.....	38
Documentación de Scripts de Monitorización.....	38
Script de Instalación (instalar).....	38
Propósito.....	38

Pasos Principales.....	38
Script de Monitorización (monitoriza.sh).....	38
Propósito.....	38
Funcionalidades.....	39
Cómo Funciona Todo Junto.....	39
Configuración y Personalización.....	39
Archivos Clave.....	39
Personalización.....	40
Errores Comunes y Soluciones.....	40
Script monitorización.....	40
instalar (Este se ejecuta antes).....	42

Teoría

Existen diferentes formas de autenticar clientes en una red GNU/Linux, pero una de las más usadas es la combinación de PAM, NSS y LDAP. La idea es disponer de un servidor para la autenticación de clientes, de modo que estos recurren al servidor cada vez que un usuario necesite identificarse. De esta manera la cuenta de usuario no es específica de un equipo cliente sino que será válida en cualquier equipo de la red.

De hecho, este es el método que suele utilizarse en GNU/Linux para obtener una gestión de usuarios globales similar a la ofrecida en servidores Windows a través de la estructura de dominio.

NSS

NSS (Name Service Switch) es un servicio que permite la resolución de nombres de usuario, de grupos y contraseñas mediante el acceso a información con diferentes orígenes. En condiciones normales esta información está en archivos locales, en concreto `/etc/passwd`, `etc/shadow` y `etc/group`, pero puede proceder de otras fuentes como: LDAP, DNS, NIS o WINS.

PAM

PAM (Pluggable Authentication Modules) establece una interfaz entre los programas de usuario y distintos métodos de autenticación. De esta forma se hace transparente para los programas el método de autenticación. La idea se basa en la creación de métodos de autenticación reemplazables de modo que se transparente para el sistema el uso de métodos de autenticación lo que permite usar métodos muy distintos entre sí sin ningún problema.

PAM complementa en algunos aspectos a NSS ya que mientras éste se centra en la búsqueda y mapeo de los usuarios, PAM controla la autenticación, el inicio de sesión y su configuración.

LDAP

LDAP es el protocolo que ofrece el acceso a un servicio de directorio implementado sobre un entorno de red, con el objetivo de acceder a una determinada información. Puede ejecutarse sobre TCP/IP o cualquier otro servicio de transferencia orientado a conexión. LDAP son las siglas en inglés de Lightweight Directory Access Protocol (Protocolo Ligero de Acceso a Directorios) y podemos considerarlo como un sistema de almacenamiento de red (normalmente construido como una base de datos) al que se le pueden realizar consultas.

Open LDAP

Open LDAP es la implementación de software libre del protocolo LDAP. Como ocurría en el caso de LDAP, OpenLDAP está muy optimizado para ofrecer los mejores resultados en situaciones que requieran operaciones de lectura intensivas. De esta forma, un directorio OpenLDAP arrojará unos resultados muy superiores a los que ofrece una base de datos relacional optimizada, cuando realicemos operaciones de consulta intensivas sobre ambas. Por el contrario, si utilizáramos un directorio OpenLDAP para guardar datos que sean actualizados de manera frecuente, los resultados obtenidos serían muy inferiores a los ofrecidos por una base de datos relacional.

Funcionamiento de LDAP y Open LDAP

El modelo de información de LDAP se basa en entradas, una entrada es un conjunto de atributos identificados por un nombre global único (Distinguished Name - DN), que se utiliza para identificarla de forma específica. Las entradas se organizan de forma jerárquica mediante un esquema de directorio, que contiene la definición de los objetos que pueden formar parte del directorio. Cada entrada en el directorio representa un objeto, que a su vez puede ser abstracto o real. Cada atributo de una entrada tendrá un tipo y un valor (formato atributo/valor). Estos atributos tienen nombres que hacen referencia a su contenido y pueden ser de dos tipos:

- Normales: los atributos que identifican a un objeto.
- Operativos: son los atributos que utiliza el servidor para administrar el directorio (fecha de creación, tamaño, etc.)

Las entradas se indexan mediante el nombre completo (dn), que facilita la identificación singular a cada elemento del árbol. El nombre completo se formará con una serie de pares atributo/valor, separados por comas, que reflejan la ruta inversa desde la posición lógica del objeto hasta la raíz del árbol.

En la actualidad, las implementaciones de LDAP suelen utilizar DNS (Domain Name Service) para la estructura de los niveles superiores del árbol. En los niveles inferiores, sin embargo, las entradas representarán otro tipo de unidades organizativas, usuarios o recursos. Por otra parte, gracias al uso de un atributo especial llamado `objectClass`, podemos controlar qué atributos son válidos y cuáles imprescindibles en una entrada. Los valores de `objectClass` establecen las reglas que debe seguir el valor de una entrada. Como vemos, LDAP puede utilizarse para organizar de forma unificada el acceso a la información representativa de una red. Sin embargo, es muy frecuente que también almacene la información de autenticación para los usuarios y/o recursos. De esta forma, se facilita el control de acceso sobre los datos contenidos en el servidor. Por último, LDAP incluye servicios de integridad y confidencialidad de los datos que contiene.

Configuración de red del entorno de pruebas

El servidor tiene una tarjeta en NAT y otra en Red interna, editamos en `/etc/netplan` las interfaces de red, para asegurarnos que la red interna tiene asignada una ip fija.

```
root@luis: /home/alumno# cat /etc/netplan/50-cloud-init.yaml
# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  ethernets:
    enp0s3:
      dhcp4: true
    enp0s8:
      dhcp4: false
      addresses:
        - 192.168.20.1/24
    enp0s9:
      dhcp4: false
      addresses:
        - 192.168.56.3/24
  version: 2
root@luis: /home/alumno#
```

1 Instalar en un servidor

cambiar el nombre del servidor

```
root@luis: /home/alumno  × + ▾
root@luis:/home/alumno# sudo hostnamectl set-hostname luis.local
root@luis:/home/alumno# hostname
luis.local
root@luis:/home/alumno#
```

editar /etc/hosts

```
root@luis: /home/alumno  × + ▾
GNU nano 7.2 /etc/hosts *
127.0.0.1 localhost
127.0.1.1 luis.local
192.168.20.1 luis.local

# 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
```

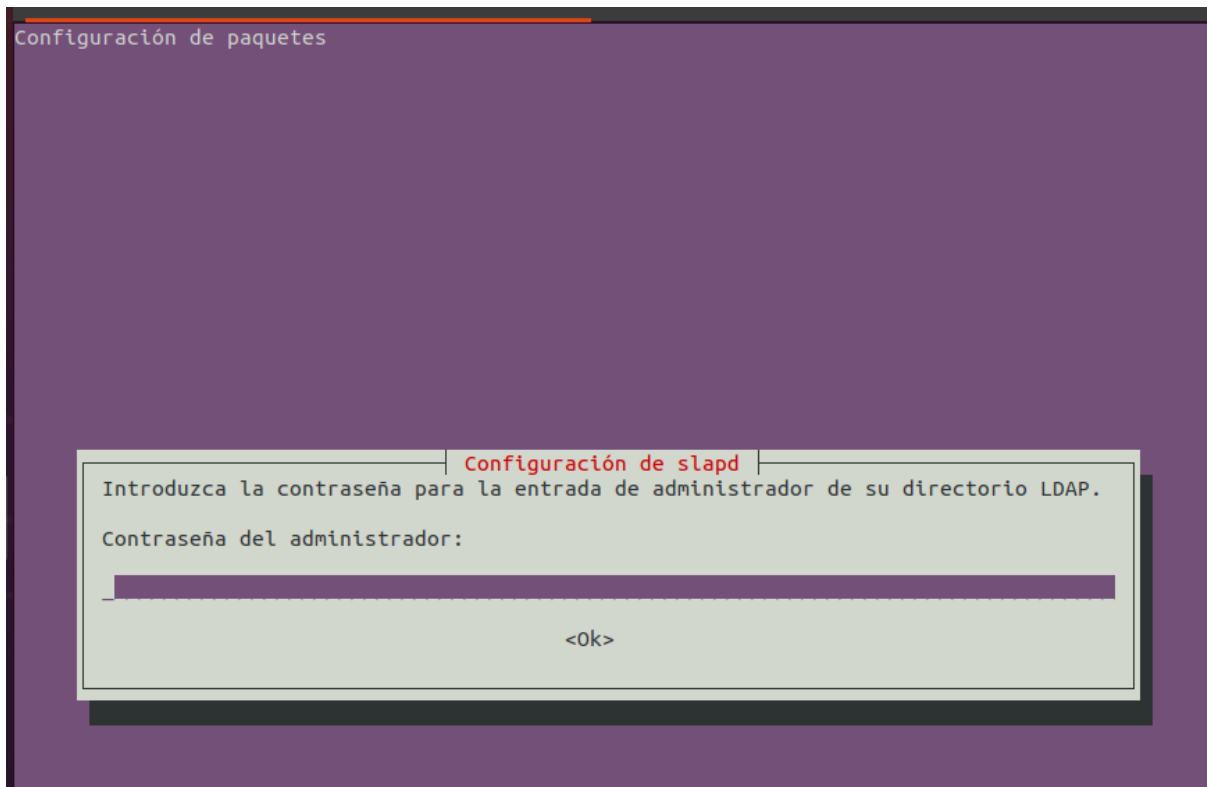
actualizar la máquina

```
alumno@ldaplk:~/Escritorio$ sudo apt update -y && upgrade -y && sudo apt dist-upgrade -y
```

Los paquetes necesarios están en los repositorios oficiales así que solo ejecuta el siguiente comando

```
alumno@ldaplk:~/Escritorio$ sudo apt install slapd ldap-utils -y
Leyendo lista de paquetes... Hecho
```

Durante el proceso de instalación aparece el asistente de ldap y nos pide la contraseña de administrador

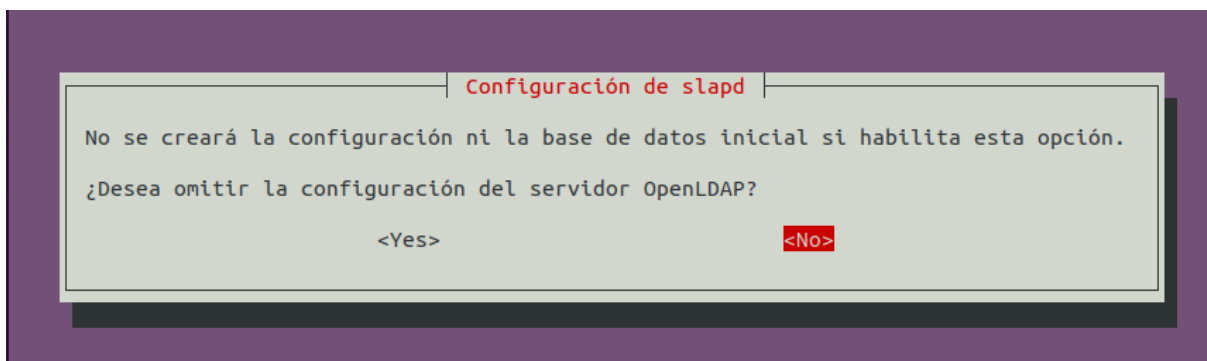


Configuración inicial

Para empezar con la configuración básica basta con el siguiente comando

```
alumno@ldaplk:/etc/netplan$ sudo dpkg-reconfigure slapd
```

tras su ejecución este asistente pregunta al usuario si desea omitir la configuración, en este caso se seleccionó “no”.



Ahora se debe escribir el nombre *DNS* del dominio que usaremos en nuestro directorio LDAP.

Configuración de slapd

El nombre de dominio DNS se utiliza para construir el DN base del directorio LDAP. Por ejemplo, si introduce «foo.example.org» el directorio se creará con un DN base de «dc=foo, dc=example, dc=org».

Introduzca el nombre de dominio DNS:

luis.local_____

<Ok>

Nombre de empresa o entidad

Configuración de slapd

Introduzca el nombre de la organización a utilizar en el DN base del directorio LDAP.

Nombre de la organización:

luis.local_____

<Ok>

y de nuevo la contraseña de administrador

Configuración de slapd

Introduzca la contraseña para la entrada de administrador de su directorio LDAP.

Contraseña del administrador:

*****_____

<Ok>

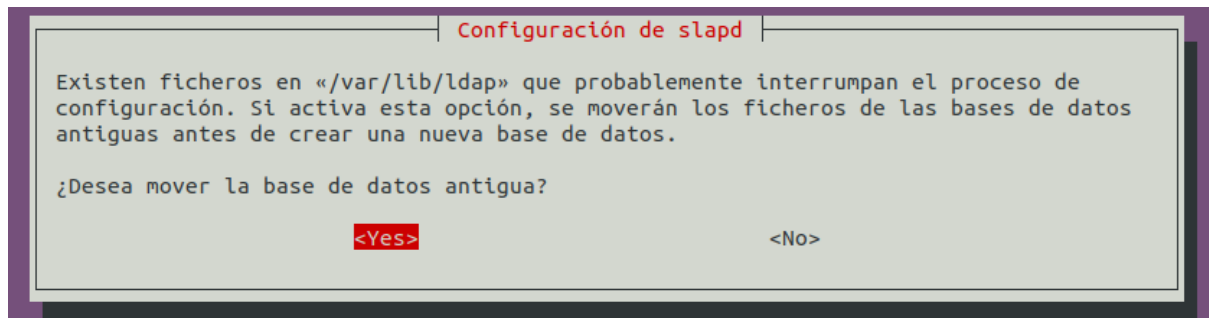
tras esto el asistente pregunta si se quiere eliminar la base de datos de configuración antigua.

Configuración de slapd

¿Desea que se borre la base de datos cuando se purgue el paquete slapd?

<Yes> <No>

Ahora el asistente avisa de que existen archivos que pueden estropear el proceso de configuración y pide permiso para eliminarlos.



Comprobación de la instalación

```
root@luis: /home/alumno  ×  +  ∨
root@luis:/home/alumno# sudo slapcat
dn: dc=luis,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: luis.local
dc: luis
structuralObjectClass: organization
entryUUID: d998bdd8-3fa5-103f-8a02-2f718d918a79
creatorsName: cn=admin,dc=luis,dc=local
createTimestamp: 20241125182136Z
entryCSN: 20241125182136.059049Z#000000#000#000000
modifiersName: cn=admin,dc=luis,dc=local
modifyTimestamp: 20241125182136Z

root@luis:/home/alumno#
```

Administración de openldap

Creación de una unidad organizativa

Ldap funciona con una estructura jerárquica en forma de árbol, para crear el primer elemento de esa estructura, en este caso una unidad organizativa, aunque este proceso es igual para el resto de elementos, creamos un archivo .ldif donde introducimos el tipo de objeto que estamos creando y los atributos del objeto en cuestión.

```
root@luis:~# cat AlumnosOU.ldif
dn: ou=Alumnos,dc=luis,dc=local
objectClass: top
objectClass: organizationalUnit
ou: Alumnos
root@luis:~#
```

Ahora con el comando ldapadd se va a añadir esta información a la BBDD ldap.

```
root@luis:~# ldapadd -x -D cn=admin,dc=luis,dc=local -W -f AlumnosOU.ldif  
Enter LDAP Password:  
adding new entry "ou=Alumnos,dc=luis,dc=local"
```

Las opciones que aparecen en este comando significan:

- **-x**: Esta opción indica que se debe usar el modo simple de autenticación
- **-D**: Después de esta opción se debe indicar el DN (Distinguished Name) del usuario que se está autenticando.
- **-W**: Esta opción solicita la contraseña del usuario especificado en el DN (El nombre por defecto si no se cambió durante la instalación de ldap debe ser “admin” **ejemplo:**
cn=admin,dc=luis,dc=local)
- **-f**: Esta opción indica que se debe leer las entradas LDAP desde un archivo, el nombre del archivo debe ser especificado a continuación de esta opción.

Para hacer una comprobación de la creación de la unidad organizativa, basta con slapcat

```
root@luis:~# sudo slapcat | tail -12  
dn: ou=Alumnos,dc=luis,dc=local  
objectClass: top  
objectClass: organizationalUnit  
ou: Alumnos  
structuralObjectClass: organizationalUnit  
entryUUID: a9b784ea-3fa6-103f-9988-7b25f16b8774  
creatorsName: cn=admin,dc=luis,dc=local  
createTimestamp: 20241125182725Z  
entryCSN: 20241125182725.226886Z#000000#000#000000  
modifiersName: cn=admin,dc=luis,dc=local  
modifyTimestamp: 20241125182725Z
```

Creación grupo

```
GNU nano 7.2 grupo.ldif *  
dn: cn=grupo1,ou=Alumnos,dc=luis,dc=local  
objectClass: top  
objectClass: posixGroup  
gidNumber: 10000  
cn: grupo
```

y se añade el grupo

```
root@luis:~# sudo ldapadd -x -D cn=admin,dc=luis,dc=local -W -f grupo.ldif  
Enter LDAP Password:  
adding new entry "cn=grupo1,ou=Alumnos,dc=luis,dc=local"
```

Añadir a un usuario y encriptar contraseña

mismo proceso pero esta vez hay que evitar que la contraseña del usuario se almacene en texto plano dentro del archivo ldif, para esto se usa slappasswd.

```
alumno@ldapserver:~/Escritorio$ sudo slappasswd
[sudo] password for alumno:
New password:
Re-enter new password:
{SSHA}qz6TglAxMxWKESMYo/vkTqR87P7wpPSe
alumno@ldapserver:~/Escritorio$
```

ahora se crea el archivo del nuevo usuario

```
{SSHA}qz6TglAxMxWKESMYo/vkTqR87P7wpPSe
alumno@ldapserver:~/Escritorio$ sudo nano usr.ldif
```

```
alumno@ldapserver: ~/Escritorio x alumno@ldapserver: ~/Escritorio x
GNU nano 4.8 usr.ldif Modified
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: lpiqueras
uid: lpiqueras
ou: grupo
uidNumber: 2000
gidNumber: 10000
homeDirectory: /home/pipqueras
loginShell: /bin/bash
userPassword: {SSHA}qz6TglAxMxWKESMYo/vkTqR87P7wpPSe
sn: Piqueras Lopez
mail: 13152527@goya.local
givenName: Luis
```

añadir al usuario

```
alumno@ldapserver:~/Escritorio$ sudo ldapadd -x -D cn=admin,dc=goya,dc=local -W -f usr.ldif
Enter LDAP Password:
adding new entry "uid=lpiqueras,ou=unidad,dc=goya,dc=local"

alumno@ldapserver:~/Escritorio$
```

y con sudo slapcat de nuevo se hace la comprobación

```
dn: uid=lpiqueras,ou=unidad,dc=goya,dc=local
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: lpiqueras
uid: lpiqueras
ou: grupo
uidNumber: 2000
gidNumber: 10000
homeDirectory: /home/pipqueras
loginShell: /bin/bash
userPassword:: e1NTSEF9cXo2VGdsQXhNeFdLRVNNWW8vdktUcVI4N1A3d3BQU2U=
sn: Piqueras Lopez
mail: 13152527@goya.local
givenName: Luis
structuralObjectClass: inetOrgPerson
entryUUID: 008e192e-a9b0-103e-853f-29d456a56a50
creatorsName: cn=admin,dc=goya,dc=local
createTimestamp: 20240518221621Z
entryCSN: 20240518221621.971135Z#000000#000#000000
modifiersName: cn=admin,dc=goya,dc=local
modifyTimestamp: 20240518221621Z
```

Ejemplo ldif de usuario:

```
dn: uid=jlopez,ou=usuarios,dc=servidor,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: jlopez
sn: Lopez
givenName: Juan
cn: Juan Lopez
displayName: Juan Lopez
uidNumber: 2000
gidNumber: 10000
userPassword: mi_password
gecos: Juan Lopez
loginShell: /bin/bash
homeDirectory: /home/jlopez
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: juan.lopez@servidor.com
postalCode: 29000
o: servidor
initials: JL
```

Borrar

La utilidad que permite eliminar entradas del directorio se llama `ldapdelete`. Para utilizarla, sólo tenemos que aportar los datos del objeto a borrar y los datos de la cuenta administrador que debe permitirlo. La sintaxis será como sigue:

```
Unset
ldapdelete -x -W -D cn=admin,dc=luís,dc=local
uid=lgomez,ou=usuarios,dc=luís,dc=local
```

Después de escribir la contraseña, parecerá que no ha ocurrido nada. Sin embargo, el objeto habrá sido eliminado. Para comprobar que la eliminación ha sido efectiva, podemos volver a utilizar la utilidad `ldapsearch`.

```
root@luís:~# sudo ldapdelete -x -W -D cn=admin,dc=luís,dc=local uid=Luis,ou=
Alumnos,dc=luís,dc=local
Enter LDAP Password:
```

Búsquedas

Las búsquedas en OpenLDAP se realizan utilizando el comando `ldapsearch`, que permite consultar el contenido del directorio LDAP. Aquí tienes una descripción general de cómo funcionan y algunos conceptos clave:

1. Comando básico

El comando básico para realizar una búsqueda en OpenLDAP es:

```
Unset
ldapsearch -x -D "cn=admin,dc=servidor,dc=local" -W -b
"dc=servidor,dc=local" "(objectClass=*)"
```

2. Parámetros clave

- `-x`: Indica que se usará una autenticación simple (en lugar de SASL).
- `-D "cn=admin,dc=servidor,dc=local"`: Especifica el DN del usuario que realiza la búsqueda (en este caso, el administrador).
- `-W`: Solicita la contraseña del usuario especificado con `-D`.
- `-b "dc=servidor,dc=local"`: Define la base de búsqueda (base DN). Es el punto de partida desde donde se realizan las búsquedas en la jerarquía LDAP.
- `"(objectClass=*)"`: Es un filtro de búsqueda que selecciona todas las entradas. Puedes modificar este filtro para buscar objetos específicos (por ejemplo, `"(uid=jdoe)"` para buscar un usuario con un UID específico).

3. Filtros de búsqueda

Los filtros permiten especificar criterios más detallados:

- Filtros simples: Pueden ser tan simples como "(cn=John)" para buscar una entrada con el nombre común "John".
- Operadores lógicos:
 - & (AND): (&(objectClass=person)(cn=John))
 - | (OR): (|(cn=John)(cn=Jane))
 - ! (NOT): (!(cn=John))

4. Ámbito de búsqueda

Puedes especificar el ámbito de búsqueda con el parámetro -s:

- sub: Busca en el DN base y en todos sus descendientes (el comportamiento predeterminado).
- one: Busca solo en el DN base, sin descendientes.
- base: Busca solo en el DN base, sin considerar el contenido.

5. Resultados de la búsqueda

Los resultados se muestran en formato LDIF. Cada entrada contiene varios atributos y sus valores. Puedes redirigir la salida a un archivo o procesarla con otras herramientas.

6. Ejemplos

Busca todos los usuarios en un dominio específico:

```
ldapsearch -x -D "cn=admin,dc=servidor,dc=local" -W -b "dc=servidor,dc=local" -s sub  
"(objectClass=inetOrgPerson)"
```

```
root@luis:~# ldapsearch -x -D "cn=admin,dc=luis,dc=local" -W -b "dc=luis,dc=local" -s sub "(objectClass=inetOrgPerson)"
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <dc=luis,dc=local> with scope subtree
# filter: (objectClass=inetOrgPerson)
# requesting: ALL
#
# luis, Alumnos, luis.local
dn: uid=luis,ou=Alumnos,dc=luis,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: Luis
sn: Piqueras Lopez
givenName: Luis
cn: Luis Piqueras Lopez
displayName: Luis Piqueras Lopez
uidNumber: 1000
gidNumber: 10000
userPassword:: bWlfcGFzc3dvcmQ=
gecos: Luis Piqueras Lopez
loginShell: /bin/bash
homeDirectory: L2hvbWUvTFAg
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: luis.piqueras@luis.local
postalCode: 29000
o: servidor
initials: LP
```

Búsqueda de un usuario específico por uid:

```
ldapsearch -xLLL -b "dc=luis,dc=local" uid=Luis
```

```

root@luis:~# ldapsearch -xLLL -b "dc=luis,dc=local" uid=Luis
dn: uid=luis,ou=Alumnos,dc=luis,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: Luis
sn: Piqueras Lopez
givenName: Luis
cn: Luis Piqueras Lopez
displayName: Luis Piqueras Lopez
uidNumber: 1000
gidNumber: 10000
gecos: Luis Piqueras Lopez
loginShell: /bin/bash
homeDirectory: L2hvbWUvTFAg
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: luis.piqueras@luis.local
postalCode: 29000
o: servidor
initials: LP

```

Que empiece por una letra

ldapsearch -x -D cn=admin,dc=luis,dc=local -W -b dc=luis,dc=local "(uid=L*)"

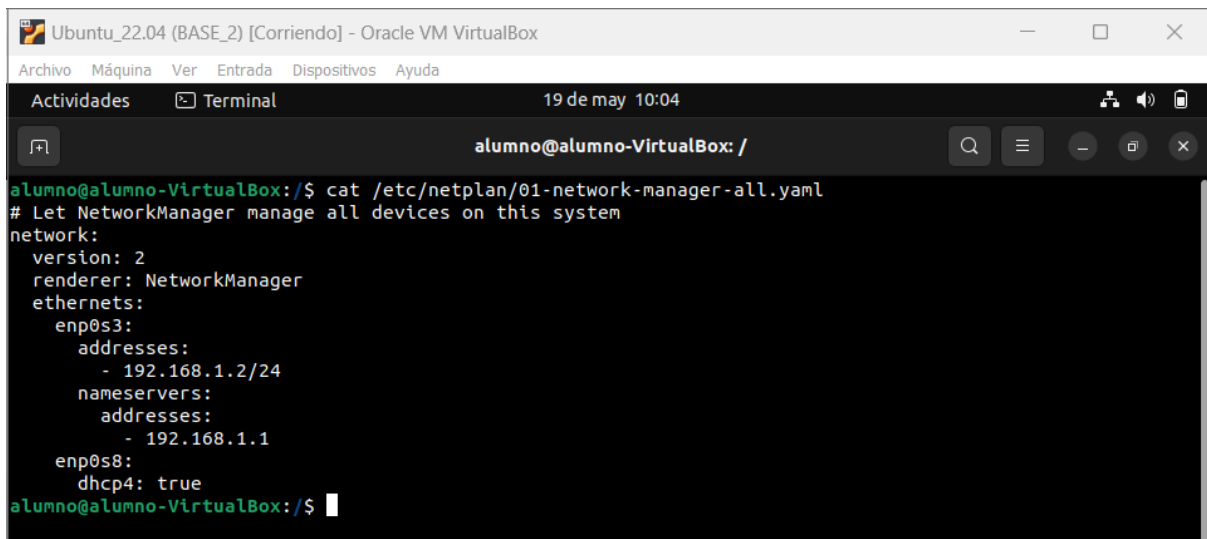
```

root@luis:~# ldapsearch -x -D cn=admin,dc=luis,dc=local -W -b dc=luis,dc=local "(uid=L*)"
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <dc=luis,dc=local> with scope subtree
# filter: (uid=L*)
# requesting: ALL
#
# Luis, Alumnos, luis.local
dn: uid=luis,ou=Alumnos,dc=luis,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: Luis
sn: Piqueras Lopez
givenName: Luis
cn: Luis Piqueras Lopez
displayName: Luis Piqueras Lopez
uidNumber: 1000
gidNumber: 10000
userPassword:: bWlfcGFzc3dvcmQ=
gecos: Luis Piqueras Lopez
loginShell: /bin/bash
homeDirectory: L2hvbWUvTFAg
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: luis.piqueras@luis.local
postalCode: 29000
o: servidor
initials: LP

```

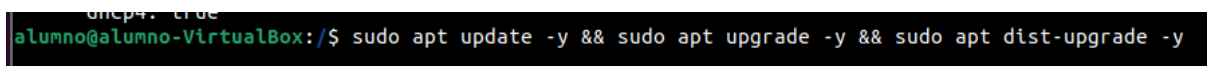
Configurar manual para autenticar un cliente en el servidor

En este caso el cliente es una máquina con Ubuntu, la máquina tiene un adaptador en red interna para verse con el servidor y otro adaptador en nat para salir a internet.



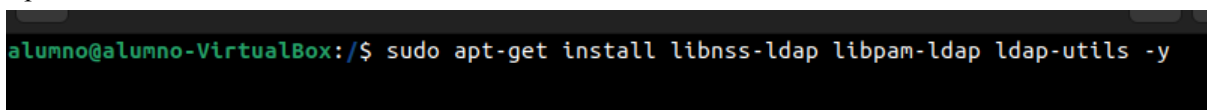
```
alumno@alumno-VirtualBox: /  
alumno@alumno-VirtualBox:/$ cat /etc/netplan/01-network-manager-all.yaml  
# Let NetworkManager manage all devices on this system  
network:  
  version: 2  
  renderer: NetworkManager  
  ethernets:  
    enp0s3:  
      addresses:  
        - 192.168.1.2/24  
      nameservers:  
        addresses:  
          - 192.168.1.1  
    enp0s8:  
      dhcp4: true  
alumno@alumno-VirtualBox:/$
```

ahora se actualiza el cliente



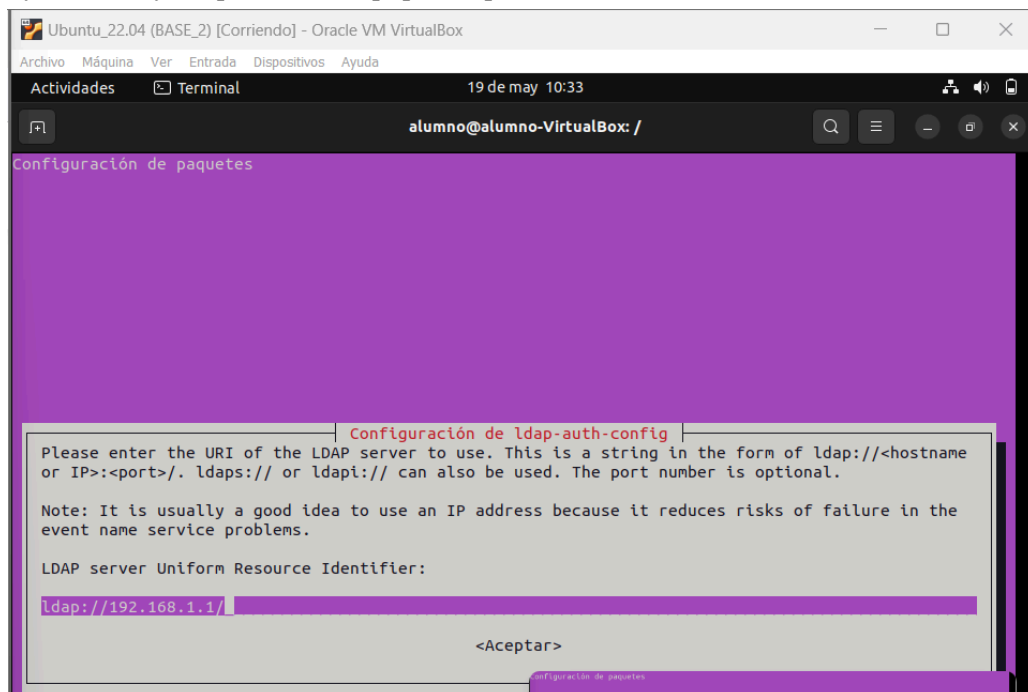
```
alumno@alumno-VirtualBox:/$ sudo apt update -y && sudo apt upgrade -y && sudo apt dist-upgrade -y
```

Ahora es hora de realizar la instalación de los paquetes necesarios, estos se encuentran en el repositorio oficial de ubuntu.



```
alumno@alumno-VirtualBox:/$ sudo apt-get install libnss-ldap libpam-ldap ldap-utils -y
```

Ahora solicita la dirección URi del servidor LDAP. En este caso, se introduce la dirección IP del servidor y se sustituye el protocolo ldapi por ldap.



```
Configuración de paquetes  
  
Configuración de ldap-auth-config  
Please enter the URI of the LDAP server to use. This is a string in the form of ldap://<hostname or IP>[:<port>/. ldaps:// or ldapi:// can also be used. The port number is optional.  
Note: It is usually a good idea to use an IP address because it reduces risks of failure in the event name service problems.  
LDAP server Uniform Resource Identifier:  
ldap://192.168.1.1/  
<Aceptar>
```

A continuación escribimos el nombre de nuestro dominio

Configuración de ldap-auth-config

Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.

Distinguished name of the search base:

dc=goya,dc=local

<Aceptar>

Ahora el asistente solicita el número de versión de ldap, por defecto 3.

Configuración de ldap-auth-config

Please enter which version of the LDAP protocol should be used by ldapns. It is usually a good idea to set this to the highest available version.

LDAP version to use:

3
2

<Aceptar>

A continuación, se indicará si las utilidades que utilicen PAM deberán comportarse del mismo modo que cuando se cambian contraseñas locales. Esto implica que las contraseñas se guarden en un archivo independiente que solo podrá ser leído por el superusuario.

Configuración de ldap-auth-config

This option will allow you to make password utilities that use pam to behave like you would be changing local passwords.

The password will be stored in a separate file which will be made readable to root only.

If you are using NFS mounted /etc or any other custom setup, you should disable this.

Make local root Database admin:

<S> <No>

Después, el sistema preguntará si se desea que sea necesario identificarse para realizar consultas en la base de datos de LDAP.

Configuración de ldap-auth-config

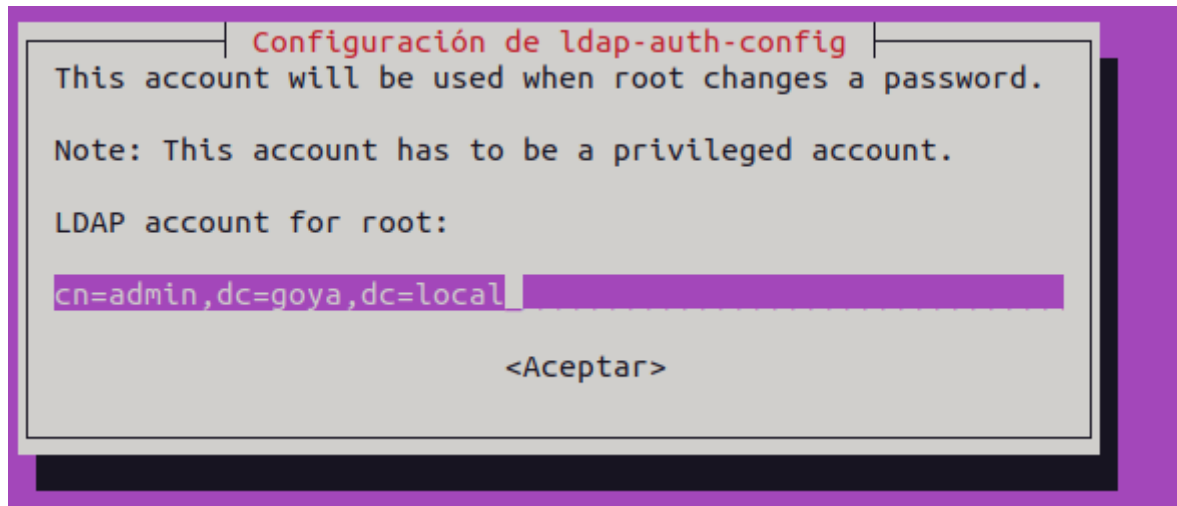
Choose this option if you are required to login to the database to retrieve entries.

Note: Under a normal setup, this is not needed.

Does the LDAP database require login?

<S> <No>

A continuación, solo queda indicar el nombre de la cuenta LDAP que tendrá privilegios para realizar cambios en las contraseñas. Como en los pasos anteriores, se debe escribir un nombre global único (Distinguished Name – DN), reemplazando el valor predeterminado ofrecido (cn=manager,dc=example,dc=net) por el utilizado en la configuración del servidor (cn=admin,dc=goya,dc=local).



Ahora solicita la contraseña de la cuenta que se indico en el paso anterior, tras escribirla y pulsar aceptar se volverá a la terminal.

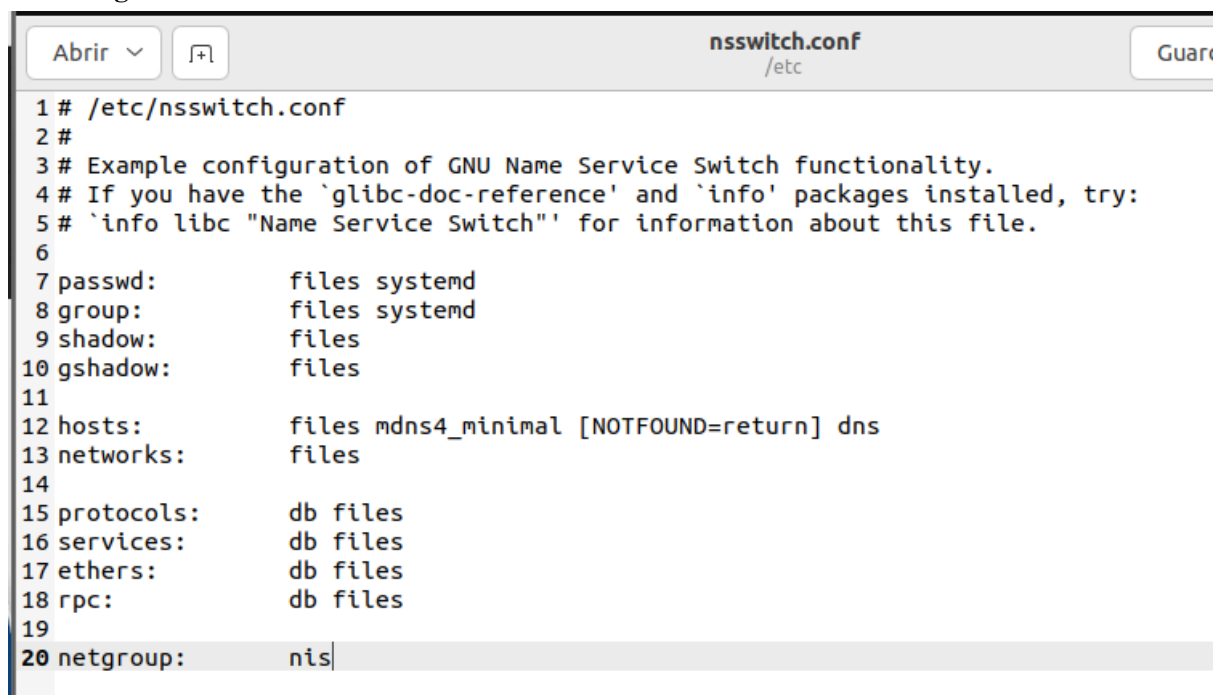
ajustes en los archivos de configuración

Se deben editar los siguientes archivos de configuración del cliente: **/etc/nsswitch.conf**, **/etc/pam.d/common-password** y **/etc/pam.d/common-session**.

En esta caso vamos a editar usando el editor gedit, empezamos **/etc/nsswitch.conf**

```
alumno@alumno-VirtualBox:/$ sudo gedit /etc/nsswitch.conf
```

Sin configurar:



Configurado:

```
1 # /etc/nsswitch.conf
2 #
3 # Example configuration of GNU Name Service Switch functionality.
4 # If you have the `glibc-doc-reference' and `info' packages installed, try:
5 # `info libc "Name Service Switch"' for information about this file.
6
7 passwd:         files ldap
8 group:          files ldap
9 shadow:         files ldap
10 gshadow:        files
11
12 hosts:          files mdns4_minimal [NOTFOUND=return] dns
13 networks:       files
14
15 protocols:      db files
16 services:       db files
17 ethers:         db files
18 rpc:            db files
19
20 netgroup:       nis
```

Para verificar si la configuración anterior funciona adecuadamente, se utilizará el comando `getent`. Este comando consultará el contenido del archivo `/etc/nsswitch.conf` para mostrar la lista de usuarios, grupos, equipos, etc., registrados en el sistema. Si la configuración realizada es correcta, también aparecerán las cuentas de usuario definidas en el servidor LDAP.

```
alumno@alumno-VirtualBox:/$ sudo getent passwd
```

Aquí esta la cuenta que creamos anteriormente:

```
lpiquerar:*:2000:10000:lpiquerar:/home/piquerar:/bin/bash
```

Ahora se editarán los archivos:

/etc/pam.d/common-password Se elimina `use_authok` de la línea 26 y 27 para permitir múltiples métodos de autenticación. **(Opcional, en algunas versiones es prescindible)**

/etc/pam.d/common-session en este paso indicamos que se debe crear un directorio home en el primer inicio de sesión, también en los usuarios autenticados mediante LDAP

```
alumno@alumno-VirtualBox:/$ sudo gedit /etc/pam.d/common-session
```

Ahora se añade la siguiente línea al final del archivo (línea 32)

```
31 session optional      pam_systemd.so
32 session optional      pam_mkhomedir.so skel=/etc/skel umask=077
33 # end of pam-auth-update config
```

Comprobación

Para asegurarnos de que todo funciona haremos una consulta en el directorio ldap desde el cliente

```

alumno@alumno-VirtualBox:/$ ldapsearch -x -H ldap://192.168.1.1 -b "dc=goya,dc=local"
# extended LDIF
#
# LDAPv3
# base <dc=goya,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# goya.local
dn: dc=goya,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: goya.local
dc: goya

# admin, goya.local
dn: cn=admin,dc=goya,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# unidad, goya.local
dn: ou=unidad,dc=goya,dc=local
ou: unidad
objectClass: top
objectClass: organizationalUnit

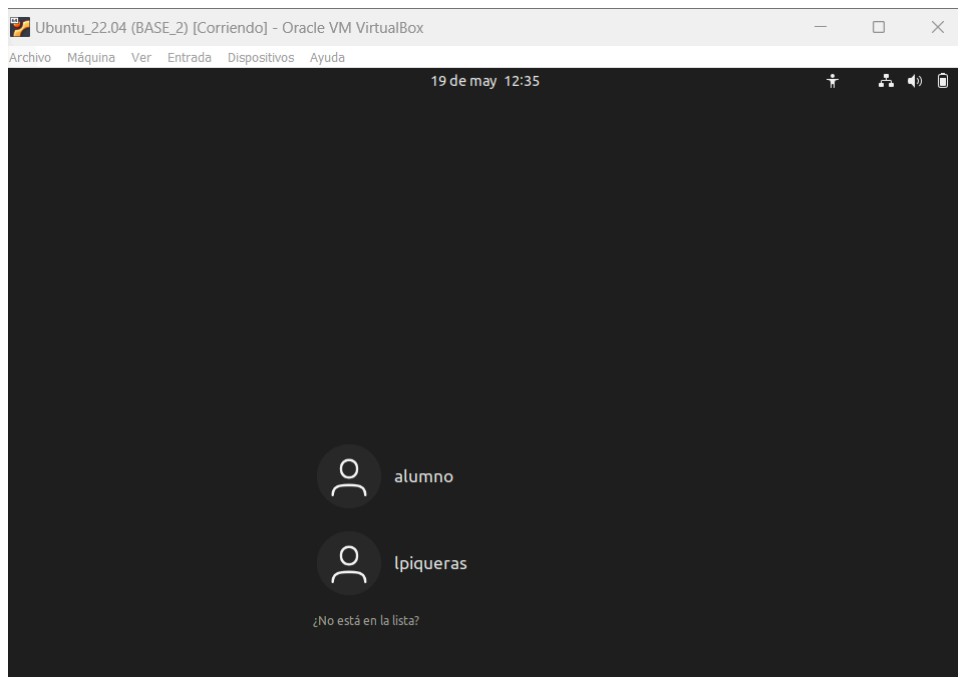
# grupo, unidad, goya.local
dn: cn=grupo,ou=unidad,dc=goya,dc=local

```

Como se puede ver se ha recibido una lista con los objetos de ldap, de esta forma se puede comprobar el correcto funcionamiento.

conexión desde el cliente

Para hacer la conexión desde el cliente vamos a instalar nsld con **sudo apt install nsld**, se introduce la ip del servidor y el nombre de dominio, después sudo reboot, pulsamos en ¿no está en la lista? y se introducen los datos del usuario, lpiqueras y su contraseña.



Interfaz gráfica web ldap

Instalar los paquetes necesarios

```
alumno@ldapserver:/etc/netplan$ sudo apt install apache2 php php-cgi libapache2-mod-php php-mbstring php-common php-pear -y
```

habilitar la extensión php-cgi.

```
alumno@ldapserver:/etc/netplan$ sudo a2enconf php7.4-cgi
Enabling conf php7.4-cgi.
To activate the new configuration, you need to run:
systemctl reload apache2
```

reiniciar el servicio

```
systemctl reload apache2
alumno@ldapserver:/etc/netplan$ sudo systemctl reload apache2
alumno@ldapserver:/etc/netplan$
```

instalar el account manager

```
alumno@ldapserver:/etc/netplan$ sudo systemctl reload apache2
alumno@ldapserver:/etc/netplan$ sudo apt install ldap-account-manager -y
```

restringir el acceso a la interfaz web de *LDAP Account Manager* únicamente para equipos de la red local.

```
p7.4-cgi (7.4.3-4ubuntu2.22) ...
sudo nano /etc/apache2/conf-enabled/ldap-account-manager.conf
```

y dejamos así el documento

```
alumno@ldapsrvr: /etc/netplan
GNU nano 4.8 /etc/apache2/conf-enabled/ldap-account-manager.conf Modified

Alias /lam /usr/share/ldap-account-manager

<Directory /usr/share/ldap-account-manager>
  Options +FollowSymLinks
  AllowOverride All
  Require ip 127.0.0.1 192.168.1.0/24
  DirectoryIndex index.html
</Directory>

<Directory /var/lib/ldap-account-manager/tmp>
  Options -Indexes
</Directory>

<Directory /var/lib/ldap-account-manager/tmp/internal>
  Options -Indexes
  Require all denied
</Directory>

<Directory /var/lib/ldap-account-manager/sess>
  Options -Indexes
  Require all denied
</Directory>

<Directory /var/lib/ldap-account-manager/config>
  Options -Indexes
  Require all denied
</Directory>

<Directory /usr/share/ldap-account-manager/lib>
  Options -Indexes
  Require all denied
</Directory>

<Directory /usr/share/ldap-account-manager/help>
  Options -Indexes
  Require all denied
</Directory>

<Directory /usr/share/ldap-account-manager/locale>
  Options -Indexes
  Require all denied
</Directory>

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos
^X Exit          ^R Read File    ^_ Replace      ^U Paste Text   ^T To Spell     ^_ Go To Line
```

y se vuelve a reiniciar el servicio, ahora para iniciar el servicio es desde el navegador con la url:
<http://192.168.1.1/lam>

← → ↻ 192.168.1.1/lam/templates/login.php ⚙️ ☆ 🔒 📱 ☰

LAM - 6.7 Want more features? Get LAM Pro! 🛠️ LAM configuration

User name

Password

Language

Login

LDAP server ldap://localhost:389

Server profile lam

ahora se puede editar la configuración en Lam configuration > edit general setting y nos pide la contraseña maestra, esta es la contraseña predeterminada de ldap account manager y es “lam”

Please enter the master password to change the general preferences:

Master password ?

Ok

LDAP Account Manager

General settings

Security settings

Session timeout

30

Allowed hosts

Encrypt session

☒

SSL certificates

Examinar...

No se ha seleccionado ningún archivo.

use system certificates

Upload

Import from server

ldaps://

Password policy

Minimum password length

0

Minimum lowercase characters

0

Minimum uppercase characters

0

Minimum numeric characters

0

Minimum symbolic characters

0

Minimum character classes

0

Number of rules that must match

all

Password must not contain user name

☐

Password must not contain part of user/first/last name

☐

External password check

Logging

Log level

Warning

Log destination

System logging

PHP error reporting

default

Change master password

New master password

Reenter password

Ok

Cancel

ahora se pueden editar los perfiles del servidor



Edit general settings




Edit server profiles

de nuevo pide la contraseña, sigue por defecto así que la meto de nuevo

Please enter your password to change the server preferences:

Profile name	lam
Password	<input type="password"/>

Ok

 Manage server profiles

adaptamos a nuestro dominio

General settings | Account types | Modules | Module settings

Server settings

Server address	ldap://localhost:389
Activate TLS	no
Tree suffix	dc=goya,dc=local
LDAP search limit	-

Advanced options

Language settings

Default language	Español (España)
Time zone	Europe/Madrid

Para este ejemplo, dentro de account types solo se va a escribir el sufijo para cada uno de los tipos de cuentas que vamos a manejar. qué son los siguientes:

Active account types

Users

User accounts (e.g. Unix, Samba and Kolab)

LDAP suffix	ou=unidad,dc=goya,dc=local
List attributes	#uid;#givenName;#sn;#uidNumber;#gidNumber
Custom label	
Additional LDAP filter	
Hidden	<input type="checkbox"/>

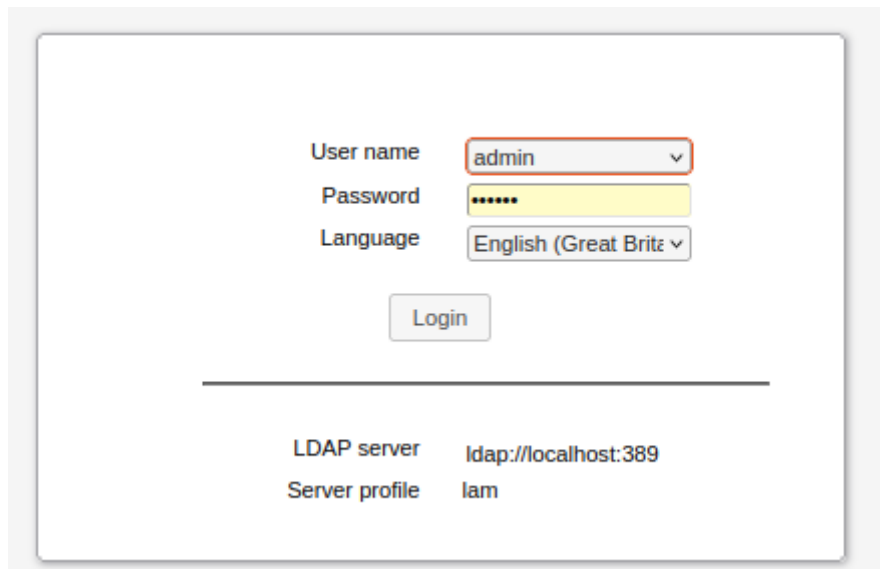
Groups

Group accounts (e.g. Unix and Samba)

LDAP suffix	ou=unidad,dc=goya,dc=local
List attributes	#cn;#gidNumber;#memberUID;#description
Custom label	
Additional LDAP filter	
Hidden	<input type="checkbox"/>

y le damos a guardar

gestionar usuarios y grupos en el servidor desde la interfaz gráfica
hacemos login

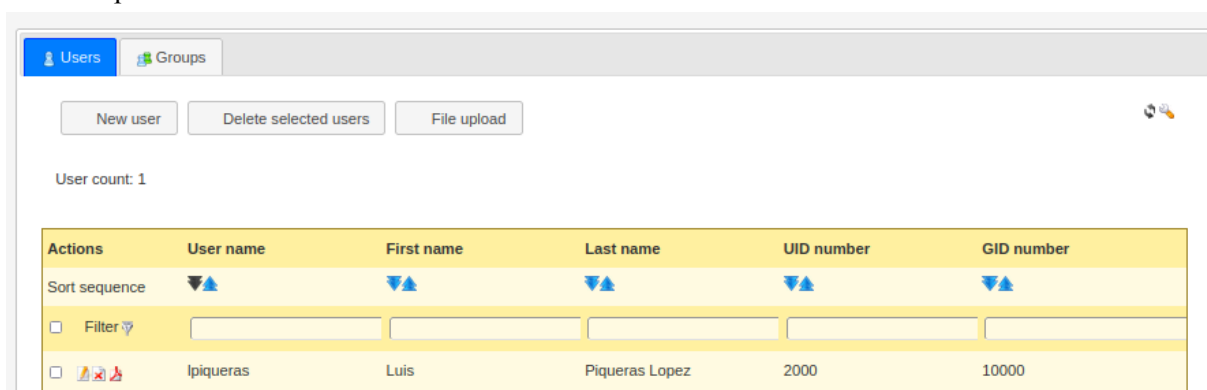


A login form with the following fields and values:

- User name: admin
- Password: masked with dots
- Language: English (Great Britz)

Below the fields is a "Login" button. At the bottom, the LDAP server is set to "ldap://localhost:389" and the server profile is "lam".

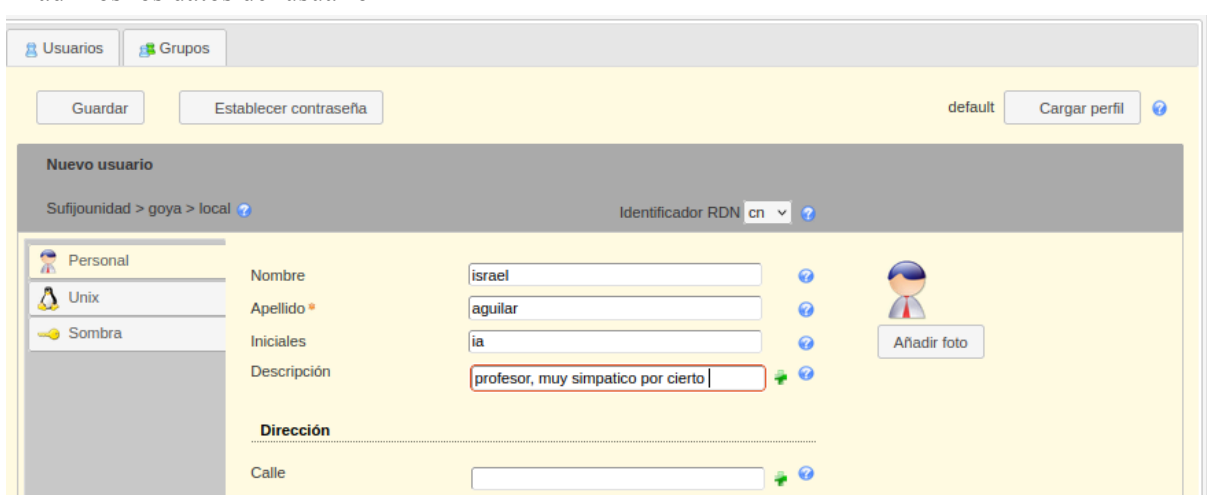
new user para añadir un nuevo usuario



The screenshot shows the 'Users' tab with a table of users. The table has columns for Actions, User name, First name, Last name, UID number, and GID number. There is one user listed: 'Ipiqueras' with first name 'Luis' and last name 'Piqueras Lopez'.

Actions	User name	First name	Last name	UID number	GID number
Sort sequence					
<input type="checkbox"/> Filter					
<input type="checkbox"/>	Ipiqueras	Luis	Piqueras Lopez	2000	10000

Añadimos los datos del usuario



The screenshot shows the 'Nuevo usuario' form. The form is for a user named 'israel aguilar' with the description 'profesor, muy simpatico por cierto'. The form includes fields for Name, Surname, Initials, Description, and Address. The 'Personal' tab is selected, and the 'Añadir foto' button is visible.

Form fields and values:

- Nombre: israel
- Apellido: aguilar
- Iniciales: ia
- Descripción: profesor, muy simpatico por cierto
- Dirección: Calle

Nombre del usuario *	<input type="text" value="iaguilar"/>	?
Nombre común	<input type="text" value="israel aguilar"/>	✗ + ?
Número UID	<input type="text" value="10000"/>	?
Gecos	<input type="text"/>	?
Grupo primario	grupo	?
Grupos adicionales	<input type="button" value="Editar grupos"/>	?
Directorio inicial *	<input type="text" value="/home/iaguilar"/>	?
Intérprete del inicio de sesión	<input type="text" value="/bin/bash"/>	?
Contraseña	<input type="button" value="Bloquear contraseña"/> <input type="button" value="Quitar contraseña"/>	

se pulsa guardar y el usuario se crea

UsuariosGrupos

Operación de LDAP exitosa.
La cuenta se creó exitosamente.

den ldap ou+grp+usr] [Corriendo] - Oracle VM VirtualBox

quina Ver Entrada Dispositivos Ayuda

Navegador web Firefox

may 19 14:48

LDAP Account Manager (1 x) +

← → ↺ 192.168.1.1/lam/templates/lists/list.php?type=user 70% ☆ 🔒 🔍 📄 ☰

LDAP Account Manager - 6.7 (Sesión iniciada como: admin)

UsuariosGrupos

Conteo de usuarios: 2

Acciones	Nombre del usuario	Nombre	Apellido	Número UID	Número GID
Secuencia de orde namiento	▼ ▲	▼ ▲	▼ ▲	▼ ▲	▼ ▲
<input type="checkbox"/> Filtrar ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	iaguilar	israel	aguilar	10000	10000
<input type="checkbox"/>	lpiqueras	Luis	Piqueras Lopez	2000	10000

Cuentas de grupo

Idap (open Idap ou+grp+usr) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Activities Navegador web Firefox may 19 14:50

LDAP Account Manager (x)

192.168.1.1/lam/templates/lists/list.php?type=group 70%

LDAP Account Manager - 6.7 (Sesión iniciada como: admin) Visor del árbol Herramientas Ayuda Cerrar sesión

Usuarios Grupos

Nuevo grupo Eliminar los grupos seleccionados

Enviar archivos

Conteo de grupos: 1

Acciones	Nombre del grupo	Número GID	Miembros del grupo	Descripción del grupo
Secuencia de ordenamiento				
<input type="checkbox"/> Filtrar				
<input type="checkbox"/> grupo	grupo	10000		

Show Applications

nuevo grupo

El proceso es el mismo, que con el usuario, nuevo grupo, establecer una contraseña

Usuarios

Grupos

Nuevo grupo

Eliminar los grupos seleccionados

Enviar archivos

Conteo de grupos: 1

Acciones	Nombre del grupo	Número GID	Miembros del grupo	Descripción del grupo
Secuencia de ordenamiento				
<input type="checkbox"/> Filtrar				
<input type="checkbox"/>	grupo	10000		

Usuarios

Grupos

La nueva contraseña será guardado en el directorio después que salve esta cuenta.

Guardar

Establecer contraseña

default

Cargar perfil

Nuevo grupo

Sufijounidad > goya > local

Identificador RDNcn

Unix

Nombre del grupo *

Número GID

Descripción

Miembros del grupo

alumnos

grupo de alumnos

Editar miembros

Pulsar guardar

Usuarios

Grupos

Operación de LDAP exitosa.

La cuenta se creó exitosamente.

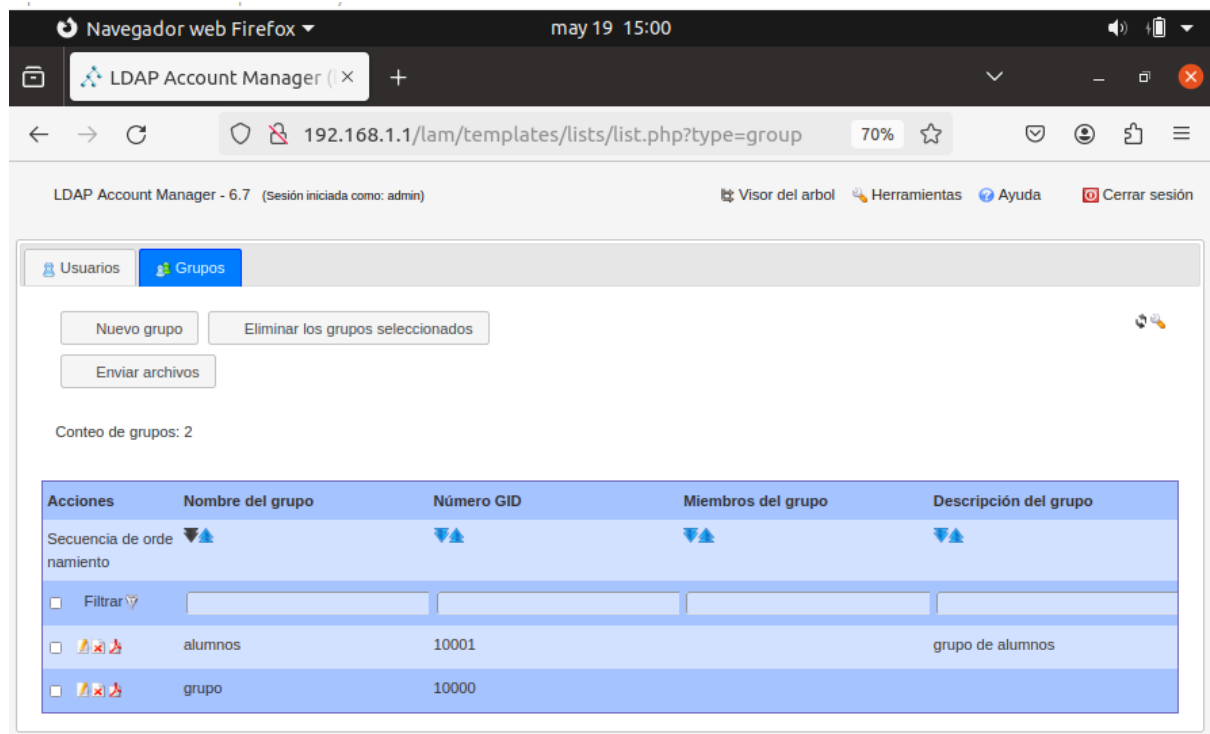
Crear un nuevo grupo

Crear PDF

Regresar a la lista de grupos

Editar nuevamente

ambos grupos creados



Scripts

Script1 unir cliente (Comentado)

```
Unset
#!/bin/bash

# Solicitar datos del servidor
read -p "Servidor LDAP (ldap://IP): " LDAP_SERVER
read -p "Base DN (ejemplo: dc=tu-dominio,dc=com): " BASE_DN
read -p "Bind DN (ejemplo: cn=admin,$BASE_DN): " BIND_DN

# Instalación desatendida y sin confirmación
apt update -y && DEBIAN_FRONTEND=noninteractive apt install -y
libnss-ldap libpam-ldap ldap-utils

# Configurar /etc/ldap/ldap.conf
# aquí se sobrescribe el archivo con el contenido de las
variables,
# tambien se usa heredoc que permite pasar múltiples
```

```
# líneas a un comando interactivo, en este caso cat.
cat <<EOF > /etc/ldap/ldap.conf
BASE $BASE_DN
URI $LDAP_SERVER
ldap_version 3
binddn $BIND_DN
EOF

# Configurar /etc/nsswitch.conf para usar LDAP
# con ^ se indica que estas buscando una cadena que empieza
una linea
# y con s/./ indicas que quieres sustituir toda la linea con
nuevo contenido
# . significa cualquier caracter y * que aparezca una o más
veces.
sed -i '/^passwd:/ s/./passwd: files ldap/'
/etc/nsswitch.conf
sed -i '/^group:/ s/./group: files ldap/' /etc/nsswitch.conf
sed -i '/^shadow:/ s/./shadow: files ldap/'
/etc/nsswitch.conf

# Modificar /etc/pam.d/common-password (remover use_auth tok)
# la g indica reemplazo global, se sustituye en este caso
use_auth tok por nada.
sed -i 's/use_auth tok//g' /etc/pam.d/common-password

# Habilitar creación de directorios home en
/etc/pam.d/common-session
# se comprueba si la linea existe con el -q (quiet) devuelve
el codigo de retorno
# (0 si encuentra coincidencia) se concatena con un echo y la
linea que se añade.
grep -q "pam_mkhomedir.so" /etc/pam.d/common-session || echo
"session optional pam_mkhomedir.so skel=/etc/skel umask=077"
>> /etc/pam.d/common-session

# Configurar autenticación PAM con LDAP
cat <<EOF > /etc/pam.d/common-auth
auth sufficient pam_unix.so nullok_secure
```



```

auth sufficient    pam_ldap.so use_first_pass
auth required     pam_deny.so
EOF

cat <<EOF > /etc/pam.d/common-account
account sufficient pam_unix.so
account sufficient pam_ldap.so
account required  pam_deny.so
EOF

# Reiniciar servicio nscd y probar conexión LDAP
ldapsearch -x -H $LDAP_SERVER -b $BASE_DN -D "$BIND_DN" -W

echo "Configuración completada. Cliente unido a OpenLDAP."

```

Explicación script 1

Paquetes instalados:

- libnss-ldap: Permitirá que NSS obtenga de LDAP información administrativa de los usuarios (Información de las cuentas, de los grupos, información de la máquina, alias, etc)
- libpam-ldap: Facilita la autenticación con LDAP a los usuarios que usan PAM.
- ldap-utils: Facilita la interacción de LDAP desde cualquier máquina de la red.

Los parámetros que nos permiten configurar el comportamiento de ldap-auth-config:

- URi del servidor, en este caso la ip, con el formato ldap://
- Indicar el DN (nombre global único) en esta caso: dc=luis,dc=local
- El DN de la cuenta LDAP que tiene permisos para realizar cambios en las contraseñas (por defecto es admin) en este caso: cn=admin,dc=luis,dc=local
- El número de versión de LDAP no se solicita en el script, está dentro del EOF que modifica el /etc/ldap/ldap.conf y por defecto se indica el 3

/etc/nsswitch.conf

En este archivo se incluyen las fuentes desde las que se obtiene la información del servicio de nombres en diferentes categorías de orden. cada categoría de información se identifica bajo un nombre. El archivo formado en texto plano se divide en columnas separadas por espacios o tabulaciones. La primera columna indica el almacenamiento y, las restantes el orden de los orígenes a consultas.

localizamos las líneas que comienzan por passwd, group y shadow y les añadimos el texto ldap, para indicar el nuevo origen para autenticar las cuentas.

/etc/pam.d/common-password

Este archivo proporciona un conjunto común de reglas PAM para la comprobación de contraseñas. En particular en la línea 26 contiene la opción `use_authok`, que impide utilizar el segundo método de autenticación cuando ya se ha aplicado otro anteriormente incluso cuando este haya sido insatisfactorio. Para evitar esto se elimina `use_authok` del archivo.

/etc/pam.d/common-session

Este otro archivo ofrece un conjunto de reglas PAM para el inicio de sesión, tanto si este es o no interactivo. Aquí se indica dónde se ha de crear el directorio home durante el primer inicio de sesión, también para los usuarios autenticados mediante LDAP. Este comportamiento lo conseguiremos añadiendo al final del archivo la siguiente línea:

```
session optional      pam_mkhomedir.so skel=/etc/skel umask=077
```

Script 2

```
Unset
#!/bin/bash

BASE_DN=`slapcat | head -1`
BASE_DN=${BASE_DN/dn: /}
BIND_DN=`sudo slapcat | grep creatorsName | head -1`
BIND_DN=${BIND_DN/creatorsName: /}

read -sp "contraseña del administrador: " BIND_PW
echo ""

# Función para añadir una entrada LDAP
añadir() {
    echo "Seleccione el tipo de entrada a añadir:"
    echo "1) Usuario"
    echo "2) Unidad Organizativa (OU)"
    echo "3) Grupo"
    echo "4) Cancelar"
    read -p "Elija una opción [1-4]: " tipo_opcion

    case $tipo_opcion in
        1) # Usuario
            read -p "Ingrese la ruta DN donde desea crear el usuario (ej.
dc=luis,dc=local): " dn_base
            read -p "Ingrese UID: (ej:luisP) " uid
            read -p "Ingrese Nombre Común (CN): " cn
            read -p "Ingrese Apellido (SN): " sn
```

```

read -p "Ingrese UID Number: " uidNumber
read -p "Ingrese GID Number: " gidNumber
homeDirectory="/home/${cn// /}"
loginShell="/bin/bash"
mail="${cn// /}@gmail.com"
dn="uid=$uid,$dn_base"
cat <<EOF > /tmp/entrada.ldif

```

```

dn: $dn
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
cn: $cn
sn: $sn
uid: $uid
uidNumber: $uidNumber
gidNumber: $gidNumber
homeDirectory: $homeDirectory
loginShell: $loginShell
mail: $mail
EOF

```

```
;;
```

```
2) # OU
```

```

read -p "Ingrese la ruta DN donde desea crear la OU (ej.
$BASE_DN): " dn_base
read -p "Ingrese el nombre de la Unidad Organizativa (OU): " ou
dn="ou=$ou,$dn_base"
cat <<EOF > /tmp/entrada.ldif

```

```

dn: $dn
objectClass: organizationalUnit
ou: $ou
EOF

```

```
;;
```

```
3) # Grupo
```

```

read -p "Ingrese la ruta DN donde desea crear el grupo (ej.
ou=Groups,$BASE_DN): " dn_base
read -p "Ingrese el nombre del grupo: " cn
read -p "Ingrese la descripción del grupo: " description
read -p "Ingrese el GID Number para el grupo: " gidNumber
dn="cn=$cn,$dn_base"
cat <<EOF > /tmp/entrada.ldif

```

```

dn: $dn
objectClass: posixGroup
objectClass: top
cn: $cn
gidNumber: $gidNumber
description: $description
EOF

```

```

        ;;
    4) # Cancelar
        echo "Operación cancelada."
        return
        ;;
    *)
        echo "Opción inválida."
        return
        ;;
esac

if ldapadd -x -D "$BIND_DN" -w "$BIND_PW" -f /tmp/entrada.ldif; then
    echo "Entrada de tipo añadida correctamente."
else
    echo "Error al añadir la entrada." >&2
fi

rm -f /tmp/entrada.ldif
}

# Función para modificar una entrada LDAP usando un archivo LDIF

modificar() {
    echo "Modificar una entrada existente en LDAP"

    # Solicita el DN de la entrada que quieres modificar
    read -p "Introduce el DN de la entrada a modificar: " dn
    if [[ -z "$dn" ]]; then
        echo "El DN no puede estar vacío." >&2
        return
    fi

    # Solicita el nombre del atributo a modificar
    read -p "Introduce el atributo que deseas modificar (por ejemplo, mail,
cn): " atributo
    if [[ -z "$atributo" ]]; then
        echo "El atributo no puede estar vacío." >&2
        return
    fi

    # Solicita el nuevo valor para el atributo
    read -p "Introduce el nuevo valor para el atributo $atributo: "
nuevo_valor
    if [[ -z "$nuevo_valor" ]]; then
        echo "El nuevo valor no puede estar vacío." >&2
        return
    fi

```

```

# Genera un archivo LDIF temporal para la modificación
archivo_ldif=$(mktemp)
echo "dn: $dn" > "$archivo_ldif"
echo "changetype: modify" >> "$archivo_ldif"
echo "replace: $atributo" >> "$archivo_ldif"
echo "$atributo: $nuevo_valor" >> "$archivo_ldif"

# Aplica la modificación usando ldapmodify
if ldapmodify -x -D "$BIND_DN" -w "$BIND_PW" -f "$archivo_ldif"; then
    echo "La entrada LDAP ha sido modificada exitosamente."
else
    echo "Error al modificar la entrada LDAP." >&2
fi

# Elimina el archivo LDIF temporal
rm -f "$archivo_ldif"
}

# Función para eliminar una entrada LDAP mediante su DN
borrar() {
    echo "Seleccione el tipo de entrada a borrar:"
    echo "1) Usuario"
    echo "2) Unidad Organizativa (OU)"
    echo "3) Grupo"
    echo "4) Cancelar"
    read -p "Elija una opción [1-4]: " tipo_opcion

    case $tipo_opcion in
        1|2|3)
            read -p "Introduce el DN de la entrada para borrar: " dn
            if [[ -n "$dn" ]]; then
                if ldapdelete -x -D "$BIND_DN" -w "$BIND_PW" "$dn"; then
                    echo "Entrada con DN $dn borrada correctamente."
                else
                    echo "Error al borrar la entrada con DN $dn" >&2
                fi
            fi
            echo "El DN no puede estar vacío." >&2
            ;;
        4) # Cancelar
            echo "Operación cancelada."
            return
            ;;
        *)
            echo "Opción inválida."
            return
            ;;
    esac
}

```

```

        esac
    }

    # Función principal para el menú de opciones
    main() {
        echo "Elige una acción:"
        echo "1) Añadir"
        echo "2) Modificar"
        echo "3) Borrar"
        echo "4) Salir"
        read -p "Elija una opción [1-4]: " opcion

        case $opcion in
            1)
                añadir
                ;;
            2)
                modificar
                ;;
            3)
                borrar
                ;;
            4)
                echo "Saliendo..."
                return
                ;;
            *)
                echo "Opción inválida."
                ;;
        esac

        read -p "¿Desea realizar otra acción? (s/n): " continuar
        if [[ "$continuar" == "s" ]]; then
            main
        else
            echo "Saliendo..."
        fi
    }

    # Ejecutar la función principal
    main

```

Explicación de scripts de monitorización

Documentación de Scripts de Monitorización

Este conjunto de scripts se utiliza para configurar y operar un sistema de monitorización que recopila datos de uso de CPU, memoria y procesos principales en un servidor. Además, incluye un sistema para enviar correos electrónicos utilizando **msmtp** y automatiza la ejecución periódica de la monitorización.

Script de Instalación (instalar)

Propósito

Este script configura el entorno necesario para el funcionamiento del sistema de monitorización. Instala el cliente de correo **msmtp**, configura las credenciales de correo y establece un temporizador para la ejecución periódica del script de monitorización.

Pasos Principales

- 1. Instalación de Dependencias:**
 - Se actualizan los paquetes y se instala **msmtp** para enviar correos electrónicos.
- 2. Configuración de Correo:**
 - Solicita al usuario un correo electrónico y su contraseña.
 - Valida que la entrada sea correcta.
 - Crea el archivo `/etc/msmtp.rc` con los datos proporcionados, asegurando que tenga los permisos necesarios para proteger las credenciales.
- 3. Configuración del Servicio y Temporizador:**
 - Crea un archivo de servicio `systemd` (`monitorizacion.service`) que ejecuta el script de monitorización (`/etc/monitoriza.sh`).
 - Crea un temporizador (`monitorizacion.timer`) para activar el servicio cada 15 minutos.
 - Habilita y activa el temporizador.
- 4. Validación de Existencia del Script:**
 - Verifica si el script principal de monitorización (`/etc/monitoriza.sh`) existe.
- 5. Prueba de Envío de Correo:**
 - Envía un correo de prueba para confirmar que la configuración de **msmtp** funciona correctamente.

Script de Monitorización (monitoriza.sh)

Propósito

Este script recopila métricas del sistema y las registra en un archivo de log (`/var/log/monitorizacion.log`). También puede configurarse para enviar estas métricas por correo electrónico utilizando las credenciales configuradas en el script de instalación.

Funcionalidades

1. **Inicialización:**
 - Configura colores para salida en consola.
 - Garantiza la existencia del archivo de log con permisos adecuados.
 - Redirige la salida estándar y errores al log, manteniendo también la salida en consola.
2. **Carga de Credenciales:**
 - Extrae la dirección de correo y contraseña desde el archivo `/etc/msmtprc`.
3. **Monitorización del Sistema:**
 - **CPU:**
 - Usa `mpstat` para calcular el uso de CPU.
 - **RAM:**
 - Usa `free` para obtener la memoria total, usada y libre.
 - **Procesos Principales:**
 - Usa `ps` para listar los procesos que más memoria y CPU consumen.
 - Si alguna métrica no se obtiene, registra un mensaje de error.
4. **Registro de Métricas:**
 - Muestra las métricas en consola y las registra en el log.
5. **Finalización:**
 - Imprime un mensaje de finalización en consola y log.

Cómo Funciona Todo Junto

1. **Ejecución del Script de Instalación:**
 - Configura las dependencias necesarias (`msmtp`) y establece el temporizador para ejecutar el script de monitorización de forma automática cada 15 minutos.
2. **Ejecución Automática de Monitorización:**
 - El temporizador activa el script de monitorización, que recopila datos del sistema y los guarda en un archivo de log.
3. **Envío de Correos (opcional):**
 - El script puede enviar las métricas por correo utilizando la configuración de `msmtp`.

Configuración y Personalización

Archivos Clave

- **`/etc/msmtprc`:** Contiene las credenciales de correo electrónico y configuración de envío.
- **`/etc/monitoriza.sh`:** Script principal de monitorización.
- **`/var/log/monitorizacion.log`:** Log donde se almacenan las métricas.

Personalización

- **Frecuencia de Ejecución:**
 - Modificar el intervalo en `OnUnitActiveSec` en el archivo `monitorizacion.timer`.
- **Métricas Monitoreadas:**

- Ampliar o modificar los comandos en `monitoriza.sh` para incluir otras métricas (e.g., temperatura del sistema, disco).
- **Alerta por Correo:**
 - Implementar lógica para enviar correos automáticos si se detectan anomalías.

Errores Comunes y Soluciones

1. **msmtp No Envía Correos:**
 - Verificar configuración en `/etc/msmtprc`.
 - Confirmar acceso al servidor SMTP.
2. **El Temporizador No Funciona:**
 - Comprobar estado con `systemctl status monitorizacion.timer`.
 - Verificar errores en `journalctl -u monitorizacion.timer`.
3. **Permisos Denegados:**
 - Asegurar que los permisos de `/etc/msmtprc` sean 600 y el script tenga permisos de ejecución (`chmod +x`).

Script monitorización

```
Unset
#!/bin/bash

# Colores
GREEN='\033[0;32m'
YELLOW='\033[1;33m'
RED='\033[0;31m'
BLUE='\033[0;34m'
NC='\033[0m' # Sin color

# Archivo de log
LOG_FILE="/var/log/monitorizacion.log"

# Crear el archivo de log si no existe y establecer permisos adecuados
if [[ ! -f "$LOG_FILE" ]]; then
    sudo touch "$LOG_FILE" || { printf "${RED}Error al crear el archivo de log en $LOG_FILE.${NC}\n" >&2; exit 1; }
    sudo chmod 640 "$LOG_FILE" || { printf "${RED}Error al establecer permisos del archivo de log.${NC}\n" >&2; exit 1; }
fi

# Redirigir stdout y stderr al log (mantener la salida a consola también)
exec >>(tee -a "$LOG_FILE") 2>&1

# Obtener la dirección de correo y la contraseña desde /etc/msmtprc
recipient_email=$(grep -i "^from" /etc/msmtprc | awk '{print $2}')
```

```

user_email=$(grep -i "^user" /etc/msmtprc | awk '{print $2}')
user_password=$(grep -i "^password" /etc/msmtprc | awk '{print $2}')

# Comprobamos si se obtuvo el correo y la contraseña correctamente
if [[ -z "$recipient_email" || -z "$user_password" ]]; then
    printf "${RED}No se encontró el correo electrónico o la contraseña en la
configuración de msmtprc. Asegúrate de que el archivo /etc/msmtprc esté
correctamente configurado.${NC}\n"
    exit 1
fi

# Inicio del script
printf "${GREEN}==== Inicio de Monitorización =====${NC}\n"

# Obtener el uso de CPU
cpu_usage=$(mpstat 1 1 | awk '/all/ {print "CPU Load: " 100 - $12 "%
used"}')
if [[ -z "$cpu_usage" ]]; then
    printf "${RED>Error al obtener el uso de CPU.${NC}\n"
    cpu_usage="No disponible"
fi

# Obtener el uso de RAM
ram_usage=$(free -h | awk '/Mem/ {print "Total Memory: " $2 "\nUsed: " $3
"\nFree: " $4}')
swap_usage=$(free -h | awk '/Swap/ {print "Swap - Total: " $2 ", Used: " $3
", Free: " $4}')
if [[ -z "$ram_usage" || -z "$swap_usage" ]]; then
    printf "${RED>Error al obtener el uso de RAM.${NC}\n"
    ram_usage="No disponible"
    swap_usage="No disponible"
fi

# Obtener los procesos que más RAM consumen
ram_processes=$(ps -eo pid,ppid,cmd,%mem,%cpu --sort=-%mem | head -n 6)
if [[ -z "$ram_processes" ]]; then
    printf "${RED>Error al obtener los procesos que consumen más
RAM.${NC}\n"
    ram_processes="No disponible"
fi

# Obtener los procesos que más CPU consumen
cpu_processes=$(ps -eo pid,ppid,cmd,%mem,%cpu --sort=-%cpu | head -n 6)
if [[ -z "$cpu_processes" ]]; then
    printf "${RED>Error al obtener los procesos que consumen más
CPU.${NC}\n"
    cpu_processes="No disponible"
fi

```

```

# Imprimir la información de uso de CPU, RAM y procesos
printf "${YELLOW}>> Uso de CPU:${NC}\n"
printf "%s\n" "$cpu_usage"

printf "${YELLOW}>> Uso de RAM:${NC}\n"
printf "%s\n%s\n" "$ram_usage" "$swap_usage"

printf "${YELLOW}>> Procesos que más RAM están consumiendo:${NC}\n"
printf "%s\n" "$ram_processes"

printf "${YELLOW}>> Procesos que más CPU están consumiendo:${NC}\n"
printf "%s\n" "$cpu_processes"

# Fin del script
printf "${GREEN}==== Monitorización Completa =====${NC}\n"
printf "$(date '+%Y-%m-%d %H:%M:%S') - Monitorización completa\n"
# Fin del script
echo -e "${GREEN}==== Monitorización Completa =====${NC}" | tee -a
$LOG_FILE
echo "$(date '+%Y-%m-%d %H:%M:%S') - Monitorización completa" >> $LOG_FILE

```

instalar (Este se ejecuta antes)

```

Unset
#!/bin/bash

# Actualizar paquetes e instalar msmtplib
sudo apt update && sudo apt install -y msmtplib || { printf "Error al instalar
msmtplib\n" >&2; exit 1; }

# Solicitar correo electrónico y contraseña
read -p "Introduce tu correo electrónico: " email
while [[ ! "$email" =~ ^[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}$ ]];
do
    printf "Correo inválido. Inténtalo nuevamente.\n"
    read -p "Introduce tu correo electrónico: " email
done

read -s -p "Introduce tu contraseña de correo: " password
printf "\n"

# Validar correo y contraseña
if [[ -z "$email" || -z "$password" ]]; then

```

```

        printf "El correo y la contraseña no pueden estar vacíos.\n" >&2
        exit 1
    fi

    # Crear y configurar msmtprc
    sudo tee /etc/msmtprc > /dev/null <<EOL
    account default
    host smtp.gmail.com
    port 587
    from $email
    user $email
    password $password
    tls on
    tls_starttls on
    auth on
    logfile /var/log/msmtp.log
    EOL

    sudo chmod 600 /etc/msmtprc || { printf "Error al configurar permisos de
    /etc/msmtprc\n" >&2; exit 1; }

    # Configurar el servicio systemd
    sudo tee /etc/systemd/system/monitorizacion.service > /dev/null <<EOL
    [Unit]
    Description=Servicio de supervisión del sistema
    After=network.target

    [Service]
    ExecStart=/bin/bash /etc/monitoriza.sh
    Type=oneshot
    EOL

    sudo tee /etc/systemd/system/monitorizacion.timer > /dev/null <<EOL
    [Unit]
    Description=Temporizador para el servicio de supervisión cada 15 minutos

    [Timer]
    OnBootSec=15min
    OnUnitActiveSec=15min

    [Install]
    WantedBy=timers.target
    EOL

    sudo systemctl daemon-reload || { printf "Error al recargar systemd\n" >&2;
    exit 1; }
    sudo systemctl enable --now monitorizacion.timer || { printf "Error al
    habilitar o iniciar el temporizador\n" >&2; exit 1; }

```

```
# Validar existencia del script monitoriza.sh
if [[ ! -f /etc/monitoriza.sh ]]; then
    printf "El archivo /etc/monitoriza.sh no existe. Crea este archivo para
completar la configuración.\n" >&2
    exit 1
fi

# Crear entrada en crontab (opcional, ya que se usa un timer)
if ! grep -q "/etc/monitoriza.sh" /etc/crontab; then
    echo "*/5 * * * * root /bin/bash /etc/monitoriza.sh" | sudo tee -a
/etc/crontab > /dev/null || { printf "Error al configurar crontab\n" >&2;
exit 1; }
fi

# Enviar un correo de prueba
printf "Enviando correo de prueba...\n"
if ! echo -e "Subject: prueba\n\nHola" | msmtplib --account=default "$email";
then
    printf "Error al enviar el correo de prueba\n" >&2
    exit 1
fi

printf "Configuración completa y correo de prueba enviado a %s\n" "$email"
```