

AUTENTICACIÓN CENTRALIZADA CON OPENLDAP, SERVICIO DE DIRECTORIO

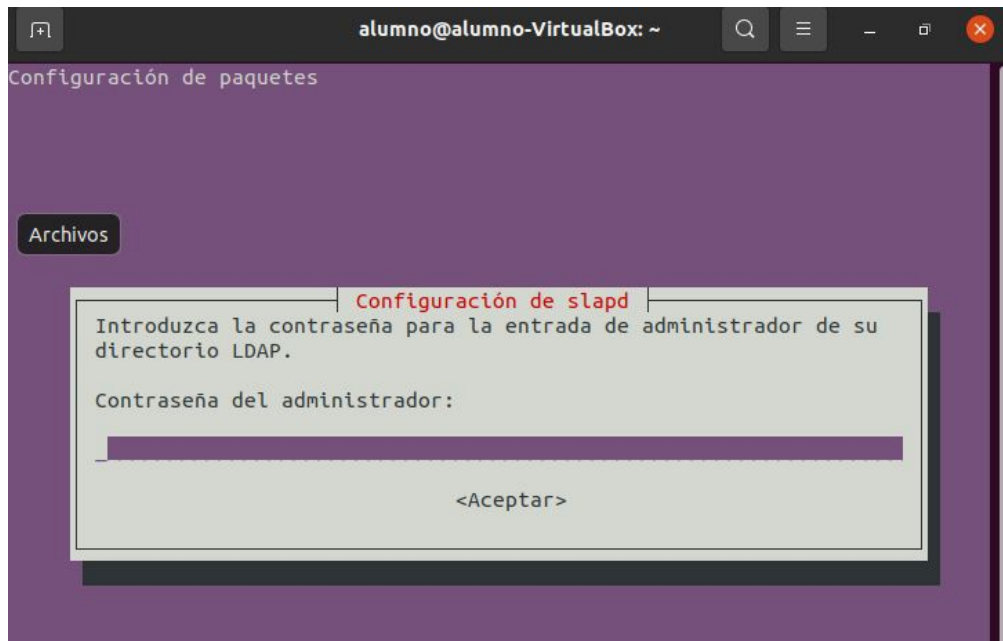
LDAP es un tipo de servicio de directorio. El servicio de directorio es una forma de autenticación centralizada, que nos permite tener un servidor con la configuración de usuarios y contraseñas, y tener diversas aplicaciones en diversos ordenadores que puedan utilizar esta autenticación para entrar.

Hay que ver dos partes: la parte del servidor (LDAP) y la parte del cliente, que puede tener muchas variantes. Cliente puede ser el sistema operativo, el servidor FTP, el acceso a un host virtual de apache, etc. Cualquier cosa que necesite autenticación se podrá conectar con un servidor de directorio, con OpenLDAP.

La configuración de OpenLDAP la vamos a hacer mediante terminal y editor de texto. OpenLDAP va a crear una estructura, que tendrá forma de árbol, y a partir de los primeros nodos, será cuando iremos introduciendo los otros nodos, que pueden ser grupos, usuarios, etc.

LDAP como servidor del SO

- Instalamos slapd: **sudo apt-get install slapd ldap-utils -y**
- Contraseña del administrador del LDAP. Se podrá reconfigurar después, pero hay que tenerla muy presente, para las tareas del lado del servidor como las tareas de preparación de los supuestos clientes. (123456)



- Antes se configuraba al instalar, pero ahora hay que configurar con **sudo dpkg-reconfigure slapd**
 - desea omitir: no
 - introduzca el nombre de dominio DNS: **servidor.DAW05.es**
 - nombre de la organización: servidor (no tiene correspondencia con el paso anterior)
 - contraseña del administrador. La que ponga aquí sustituirá a la que puse en principio.
 - desea que se borre la BD cuando se purgue el paquete: SI
 - desea mover la base de datos antigua: SI
- La forma de almacenar la información que tiene el OpenLDAP es en forma de árbol. Lo que hemos hecho es crear los dos primeros nodos: el nodo raíz y el nodo administrador.
Para ver el contenido de nuestro OpenLDAP: **sudo slapcat**
Se ven los dos nodos.

Primer nodo, nodo raíz. Segundo nodo, nodo administrador.

```
alumno@alumno-VirtualBox:~$ sudo slapcat
dn: dc=servidor,dc=daw05,dc=es
o: Archivos
ss: top
objectClass: dcObject
objectClass: organization
o: servidor
dc: servidor
structuralObjectClass: organization
entryUUID: 28f63caa-040b-103b-92c8-51c64b0597e8
creatorsName: cn=admin,dc=servidor,dc=daw05,dc=es
createTimestamp: 20210215185547Z
entryCSN: 20210215185547.930452Z#000000#000#000000
modifiersName: cn=admin,dc=servidor,dc=daw05,dc=es
modifyTimestamp: 20210215185547Z

dn: cn=admin,dc=servidor,dc=daw05,dc=es
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9RkVwVURsYU1jR29GTmNJV0tyaFFeY1dVangrVmkyeGw=
structuralObjectClass: organizationalRole
entryUUID: 28f6fb9a-040b-103b-92c9-51c64b0597e8
creatorsName: cn=admin,dc=servidor,dc=daw05,dc=es
createTimestamp: 20210215185547Z
entryCSN: 20210215185547.935477Z#000000#000#000000
modifiersName: cn=admin,dc=servidor,dc=daw05,dc=es
modifyTimestamp: 20210215185547Z
```

Da muchos parámetros:

dn: nombre de dominio. Se describe por varios componentes

dc: componente de dominio. servidor, daw05 y es. Cuando me ha pedido el dns del servidor, puse servidor.daw05.es. No es dns como vimos en la práctica pasada, sino nombre de dominio.

ObjectClass: top. Objeto top. Nodo raíz.

o: organización (servidor le pusimos).

Y sobre el segundo nodo de nuestro árbol, que consiste en el dn que tenía el nodo anterior, añadiéndole el nombre del componente (cn), que es admin, que es el administrador.

cn: admin.

descripción: LDAP administrator

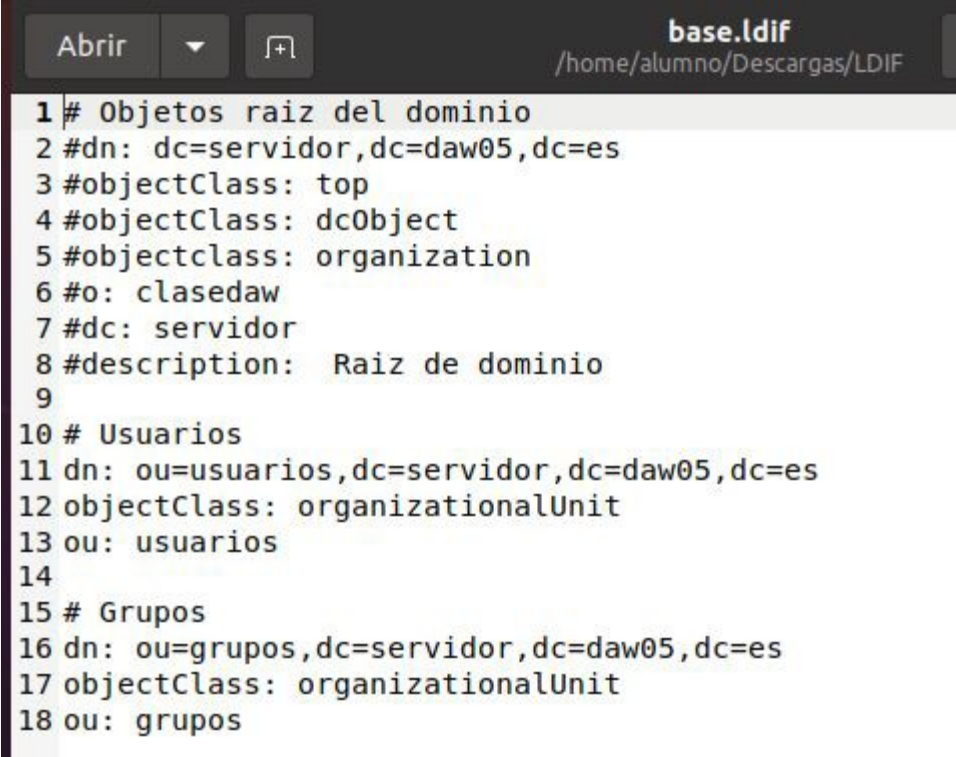
No es intuitivo y hay mucha información.

Lo que queremos es, a esta estructura que hemos creado, añadirle nuevos elementos. Crear un protocolo de autenticación mediante LDAP a nuestro sistema operativo. Ahora lo que necesito son unidades organizativas. Una unidad organizativa (ou) es la que puede admitir elementos.

Para ir añadiendo elementos a nuestro árbol, vamos a tener que ayudarnos de una serie de archivos con extensión ldif.

En el aulavirtual hay unos ejemplos: base.ldif y usuarios.ldif.

- `sudo gedit base.ldif`

A screenshot of a text editor window titled 'base.ldif' with the path '/home/alumno/Descargas/LDIF'. The editor contains 18 lines of LDIF code. Lines 1-9 define the root object (dc=servidor,dc=daw05,dc=es) with object classes top, dcObject, and organization, and a description 'Raiz de dominio'. Lines 10-14 define an organizational unit 'ou=usuarios'. Lines 15-18 define another organizational unit 'ou=grupos'.

```
1 # Objetos raiz del dominio
2 #dn: dc=servidor,dc=daw05,dc=es
3 #objectClass: top
4 #objectClass: dcObject
5 #objectclass: organization
6 #o: clasedaw
7 #dc: servidor
8 #description: Raiz de dominio
9
10 # Usuarios
11 dn: ou=usuarios,dc=servidor,dc=daw05,dc=es
12 objectClass: organizationalUnit
13 ou: usuarios
14
15 # Grupos
16 dn: ou=grupos,dc=servidor,dc=daw05,dc=es
17 objectClass: organizationalUnit
18 ou: grupos
```

Añade 2 unidades organizativas (ou), una para los grupos y otra para los usuarios. Lo que voy a añadir son usuarios del sistema operativo, por lo tanto necesitan pertenecer a algún grupo.

Primero se pone el tipo de nodo que se va a añadir, que será una unidad organizativa y después se pone la dirección del nodo del que va a depender, aquí el nodo raíz. Si no sabemos la dirección, en el terminal escribimos `sudoslappcat (dn:`

`ou=usuarios,dc=servidor,dc=daw05,dc=es)`

Creamos dos unidades organizativas. Una para crear usuarios y otra para crear grupos. Son contenedores. No contienen elementos autenticables. En estas unidades organizativas podremos meter esos elementos. Guardamos el archivo.

Vamos a usar la siguiente instrucción para añadir el archivo:

```
sudo ldapadd -x -D cn=admin,dc=servidor,dc=daw05,dc=es -W -f base.ldif
```

- `x` autenticarnos de la forma estándar
- `D` usuario que vamos a usar para ejecutar la acción, usando su dn completo, con los dc.

- W se autenticará mediante password
- f a ese usuario le vamos a añadir el archivo siguiente

(A veces pide primero la contraseña de sudo)

Pide la contraseña de LDAP, y muestra que ha añadido dos nuevas entradas a nuestro LDAP.

```
alumno@alumno-VirtualBox:~/Descargas/LDIF$ sudo ldapadd -x -D cn=admin,dc=servidor,dc=daw05,dc=es -W -f base.ldif
Enter LDAP Password:
adding new entry "ou=usuarios,dc=servidor,dc=daw05,dc=es"

adding new entry "ou=grupos,dc=servidor,dc=daw05,dc=es"
```

Sudo slapcat

nodo raíz, el administrador, unidad organizativa usuarios y unidad organizativa grupos.

Esto es un árbol, y en cada momento estamos diciendo de qué nodo depende cada uno. Cada uno indica cuál es el padre. En dn

Y en creatorsName, quién lo ha creado.

```
dn: ou=usuarios,dc=servidor,dc=daw05,dc=es
objectClass: organizationalUnit
ou: usuarios
structuralObjectClass: organizationalUnit
entryUUID: 40ad0d92-0410-103b-9ad9-a71bd6037331
creatorsName: cn=admin,dc=servidor,dc=daw05,dc=es
createTimestamp: 20210215193215Z
entryCSN: 20210215193215.199861Z#000000#000#000000
modifiersName: cn=admin,dc=servidor,dc=daw05,dc=es
modifyTimestamp: 20210215193215Z

dn: ou=grupos,dc=servidor,dc=daw05,dc=es
objectClass: organizationalUnit
ou: grupos
structuralObjectClass: organizationalUnit
entryUUID: 40aee5e0-0410-103b-9ada-a71bd6037331
creatorsName: cn=admin,dc=servidor,dc=daw05,dc=es
createTimestamp: 20210215193215Z
entryCSN: 20210215193215.212029Z#000000#000#000000
modifiersName: cn=admin,dc=servidor,dc=daw05,dc=es
modifyTimestamp: 20210215193215Z
```

Una vez que tenemos las unidades organizativas, podemos empezar a crear usuarios y grupos.

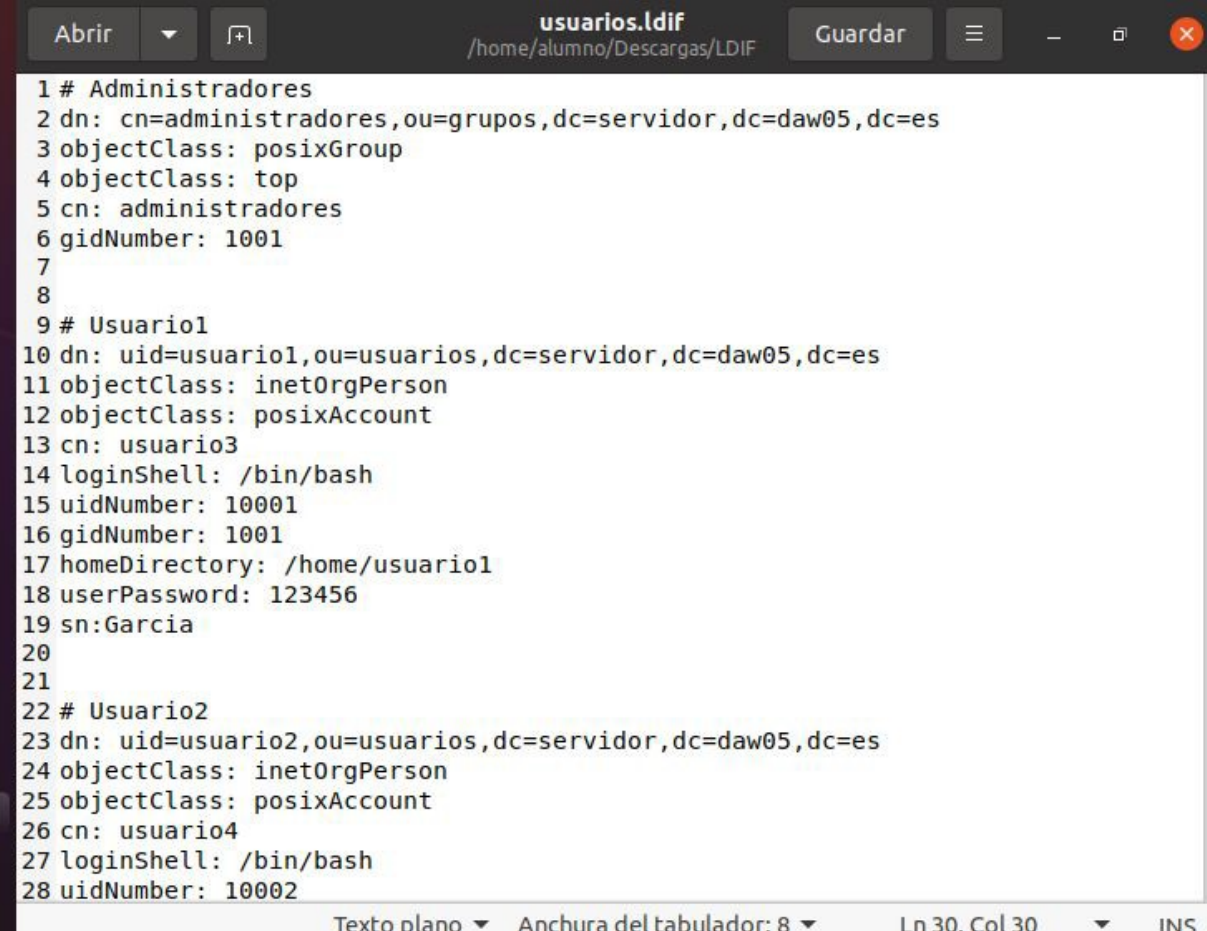
Abrimos el archivo para añadir usuarios: usuarios.ldif y añadimos un grupo Administradores, y los usuarios 1 y 2.

Nuevo componente de dominio (cn) que es administradores. Y tenemos que poner el dn, nombre de dominio de su nodo padre (ou=grupos,dc=servidor...)

gidNumber: identificador de grupo

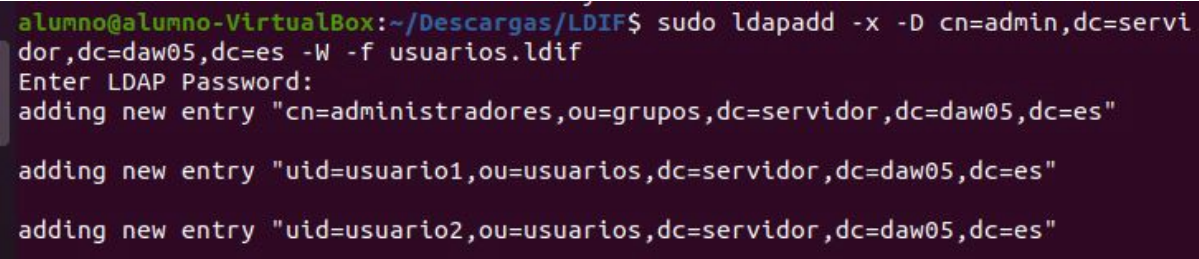
uidNumber: identificador de usuario

Añadimos dos usuarios nuevos, con el número del grupo y el número del usuario. Es una persona (inetOrgPerson) y hay que poner apellido también. Directorio y password.



```
1 # Administradores
2 dn: cn=administradores,ou=grupos,dc=servidor,dc=daw05,dc=es
3 objectClass: posixGroup
4 objectClass: top
5 cn: administradores
6 gidNumber: 1001
7
8
9 # Usuario1
10 dn: uid=usuario1,ou=usuarios,dc=servidor,dc=daw05,dc=es
11 objectClass: inetOrgPerson
12 objectClass: posixAccount
13 cn: usuario3
14 loginShell: /bin/bash
15 uidNumber: 10001
16 gidNumber: 1001
17 homeDirectory: /home/usuario1
18 userPassword: 123456
19 sn:Garcia
20
21
22 # Usuario2
23 dn: uid=usuario2,ou=usuarios,dc=servidor,dc=daw05,dc=es
24 objectClass: inetOrgPerson
25 objectClass: posixAccount
26 cn: usuario4
27 loginShell: /bin/bash
28 uidNumber: 10002
```

```
sudo ldapadd -x -D cn=admin,dc=servidor,dc=daw05,dc=es -W -f usuarios.ldif
```



```
alumno@alumno-VirtualBox:~/Descargas/LDIF$ sudo ldapadd -x -D cn=admin,dc=servidor,dc=daw05,dc=es -W -f usuarios.ldif
Enter LDAP Password:
adding new entry "cn=administradores,ou=grupos,dc=servidor,dc=daw05,dc=es"

adding new entry "uid=usuario1,ou=usuarios,dc=servidor,dc=daw05,dc=es"

adding new entry "uid=usuario2,ou=usuarios,dc=servidor,dc=daw05,dc=es"
```

```
sudo slapcat
```

Y aparecen los elementos añadidos al árbol del LDAP.

```
dn: en=adMinistradores,ou=grupos,de=servidor,de=daw05,de=es
objectClass: posixGroup
objectClass: top
en: adMinistradores
gidNumber: 1001
structuralObjectClass: posixGroup
entryUUID: eb8f56f0-0412-103b-9adb-a71bd6037331
creatorsName: en=adMin,de=servidor,de=daw05,de=es
createTimestamp: 20210215195120
entryCSN: 20210215195120.8890672#000000#000#000000
modifiersName: en=adMin,de=servidor,de=daw05,de=es
modifyTimestamp: 20210215195120
```

```
dn: uid=usuariol,ou=usuarios,de=servidor,dc=daw05,dc=es
objectClass: inetOrgPerson
objectClass: posixAccount
en: usuario3
loginShell: /bin/bash
uidNumber: 10001
gidNumber: 1001
homeDirectory: /home/usuariol
userPassword:: MTizNDU2
sn: Gareia
structuralObjectClass: inetOrgPerson
uid: usuariol
entryUUID: eb905e80-0412-103b-9ade-a71bd6037331
creatorsName: en=adMin,de=servidor,de=daw05,de=es
createTimestamp: 20210215195120
entryCSN: 20210215195120.8957642#000000#000#000000
modifiersName: en=adMin,dc=servidor,de=daw05,dc=es
modifyTimestamp: 20210215195120
```

```
dn: uid=usuario2,ou=usuarios,dc=servidor,de=daw05,dc=es
objectClass: inetOrgPerson
objectClass: posixAccount
en: usuario4
loginShell: /bin/bash
uidNumber: 10002
gidNumber: 1001
homeDirectory: /home/usuario2
userPassword:: MTizNDU2
sn: Perez
structuralObjectClass: inetOrgPerson
uid: usuario2
entryUUID: eb9188be-0412-103b-9add-a71bd6037331
creatorsName: en=adMin,de=servidor,dc=daw05,de=es
createTimestamp: 20210215195120
entryCSN: 20210215195120.903450z#000000#000#000000
modifiersName: en=adMin,de=servidor,de=daw05,de=es
modifyTimestamp: 20210215195120
```

De manera opcional se puede utilizar la aplicacion "jxplorer" de Ubuntu para revisar el árbol del servidor LDAP de una forma más visual.

```
sudo apt install jxplorer
```

Con esto tenemos completada la parte del servidor. Ahora tenemos que abordar la parte de cliente, que pueden ser de múltiples naturalezas. Vamos a utilizar el sistema operativo ahora.