

Instalar LDAP

```
# apt-get install slapd ldap-utils
```

Administrator Password:

Miramos estructura LDAP:

```
root@ldap1:~# slapcat
dn: dc=lobo99,dc=info
objectClass: top
objectClass: dcObject
objectClass: organization
o: lobo99.info
dc: lobo99
structuralObjectClass: organization
entryUUID: 2f9222aa-9998-1035-9dbc-0939660bb676
creatorsName: cn=admin,dc=lobo99,dc=info
createTimestamp: 20160418100055Z
entryCSN: 20160418100055.284922Z#000000#000#000000
modifiersName: cn=admin,dc=lobo99,dc=info
modifyTimestamp: 20160418100055Z

dn: cn=admin,dc=lobo99,dc=info
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9QUVqck5ZSGlJTnIzSnJPTGt2OG1adk1kVHliNEI2M2g=
structuralObjectClass: organizationalRole
entryUUID: 2f924adc-9998-1035-9dbd-0939660bb676
creatorsName: cn=admin,dc=lobo99,dc=info
createTimestamp: 20160418100055Z
entryCSN: 20160418100055.286000Z#000000#000#000000
modifiersName: cn=admin,dc=lobo99,dc=info
modifyTimestamp: 20160418100055Z
```

Creación usuario

Mas info:

[https://wiki.legido.com/doku.php?id=informatica:linux:ldap:instalacion&s\[\]=openldap](https://wiki.legido.com/doku.php?id=informatica:linux:ldap:instalacion&s[]=openldap)

Creamos ldif. **IMPORTANTE** Tiene que ser inetorgperson para que tenga uid y posixAccount hay que meter todos los campos:

```
dn: cn=jur,dc=lobo99,dc=info
objectClass: simpleSecurityObject
objectClass: inetorgperson
objectClass: posixAccount
cn: jur
sn: legido
uid: jur
uidnumber: 1001
gidNumber: 1001
homeDirectory: /home/jur
loginshell: /bin/bash
description: Jose
userPassword: 12345
```

```
# ldapadd -x -w ***** -D "cn=admin,dc=lobo99,dc=info" -f jose.ldif
```

Cliente LDAP

```
# apt-get install libnss-ldapd
```

Servidor:

```
ldap://ldap.lobo99.info
```

Base:

```
dc=lobo99,dc=info
```

Marcar Servicios:

```
group
passwd
shadow
```

Para hacer debug si no loga, en el servidor:

Si hacemos:

```
# getent passwd
```

Nos tienen que salir los usuarios que tiene en el ldap.

Si no aparece, arrancamos en modo debug:

```
# /etc/init.d/nscd stop
# /etc/init.d/nslcd stop
# nslcd -d
```

Por ejemplo podemos ver que el filtro no saca ningún usuario:

```
nsldap: [8b4567] <passwd="joseuid"> DEBUG:
myldap_search(base="dc=lobo99,dc=info",
filter="(&(objectClass=posixAccount)(uid=joseuid))")
.....
nsldap: [8b4567] <passwd="joseuid"> DEBUG: ldap_result(): end of results (0
total)
```

Puede ser que por ejemplo no tenga la clase posixAccount

Si funciona bien sale:

```
nsldap: [7b23c6] <passwd="jur"> DEBUG: ldap_simple_bind_s(NULL,NULL)
(uri="ldap://192.168.2.101:389")
nsldap: [7b23c6] <passwd="jur"> DEBUG: ldap_result():
cn=jur,dc=lobo99,dc=info
nsldap: [7b23c6] <passwd="jur"> DEBUG: ldap_result(): end of results (1
total)
```

Crear directorio home en el primer login

Requisito: tener instalado el paquete libpam-ldapd

Añadir la siguiente línea a:

```
/etc/pam.d/common-session
```

```
session      required      pam_mkhomedir.so skel=/etc/skel umask=0022
```

Hacer sudo a un grupo

Creamos el grupo de sudos en ldap grupoldapsudo.ldif:

```
dn: ou=groups,dc=lobo99,dc=info
objectclass: organizationalUnit
objectclass: top
ou: groups

dn: cn=grupoldapsudo,ou=groups,dc=lobo99,dc=info
cn: grupoldapsudo
gidnumber: 1001
objectclass: posixGroup
objectclass: top
```

```
ldapadd -x -w ***** -D "cn=admin,dc=lobo99,dc=info" -f grupoldapsudo.ldif
```

Para añadir usuarios:

```
dn: cn=grupoldapsudo,ou=groups,dc=lobo99,dc=info
changetype: modify
add: memberuid
memberuid: jur
```

```
ldapmodify -x -w ***** -D "cn=admin,dc=lobo99,dc=info" -f
grupoldapsudo_add.ldif
```

En el cliente, instalar el paquete:

```
apt-get install sudo-ldap
```

Crear el fichero:

```
/etc/sudoers.d/ldap
```

```
%grupoldapsudo ALL=(ALL:ALL) ALL
```

From:

<http://wiki.legido.com/> - **Legido Wiki**

Permanent link:

<http://wiki.legido.com/doku.php?id=proxmox:proxmox4:ldap>

Last update: **2016/04/20 09:30**

