

## LDAP:

### Instalar:

Importante en el fichero de configuración de red de la maquina...

Nameservers:

addresses: [192.168.3.112]

search: [josue.local]

modificar el archivo hosts:

```
GNU nano 6.2 /etc/hosts
127.0.0.1 localhost
127.0.1.1 JMF-LDAP
127.0.0.1 JMF-LDAP.josue.local ldapserver
192.168.3.112 JMF-LDAP.josue.local ldapserver

GNU nano 6.2 /etc/hostname
JMF-LDAP.josue.local
```

**Sudo apt install slapd ldap-utils -y**

configuración:

**sudo dpkg-reconfigure slapd**

Nombre dominio -> josue.local

Organización -> josue

Password del administrador ldap

Eliminar la bbdd antigua, aceptando lo siguiente.

Probar la instalación:

**Sudo slapcat**

Crear la instalación de la unidad organizativa:

Crear un archivo llamado ou.ldif

```
dn: ou=OU_Jefes,dc=josue,dc=local
```

```
objectClass: top
```

```
objectClass: organizationalUnit
```

```
ou: OU_Jefes
```

```
dn: ou=OU_Curritos,dc=josue,dc=local
```

```
objectClass: top
```

```
objectClass: organizationalUnit
```

```
ou: OU_Curritos
```

Para ejecutar esto en la BBDD:

```
sudo ldapadd -x -D cn=admin,dc=josue,dc=local -W -f ou.ldif
```

para asegurarnos de que funciona:

```
sudo slapcat
```

Creación de grupos y usuarios:

Creamos un archivo...

```
sudo nano grp.ldif
```

Escribimos lo siguiente:

```
dn: cn=G_JEFES,ou=OU_Jefes,dc=josue,dc=local
```

```
objectClass: top
```

```
objectClass: posixGroup
```

```
gidNumber: 10000
```

```
cn: G_Jefes
```

```
dn: cn=G_Curritos,ou=OU_Curritos,dc=josue,dc=local
```

```
objectClass: top
```

```
objectClass: posixGroup
```

```
gidNumber: 10001
```

cn: G\_Curritos

Para ejecutar este fichero y crear los grupos...

```
sudo ldapadd -x -D cn=admin,dc=josue,dc=local -W -f grp.ldif
```

Para crear el usuario comenzamos creando la contraseña cifrada con el siguiente comando:

```
sudo slappasswd
```

introducimos la contraseña y copiamos el resultado para añadirlo al archivo de creación de usuarios:

```
sudo nano usr.ldif
```

Con contenido:

```
dn: uid=jefe1,ou=OU_Jefes,dc=josue,dc=local
```

```
objectClass: top
```

```
objectClass: posixAccount
```

```
objectClass: inetOrgPerson
```

```
objectClass: person
```

```
cn: jefe1
```

```
uid: jefe1
```

```
ou: G_Jefes
```

```
uidNumber: 2000
```

```
gidNumber: 10000
```

```
homeDirectory: /home/jefe1
```

```
loginShell: /bin/bash
```

```
userPassword: {SSHA}YbK3NVD0QJ42YNqLHakkwecRk1n3Ndyl
```

```
sn: 1
```

```
mail: jefe1@gmail.com
```

```
givenName: jefe
```

```
dn: uid=jefe2,ou=OU_Jefes,dc=josue,dc=local
```

```
objectClass: top
```

objectClass: posixAccount  
objectClass: inetOrgPerson  
objectClass: person  
cn: jefe2  
uid: jefe2  
ou: G\_Jefes  
uidNumber: 2001  
gidNumber: 10000  
homeDirectory: /home/jefe2  
loginShell: /bin/bash  
userPassword: {SSHA}Ybk3NVD0QJ42YNqLHakkwecRk1n3Ndyl  
sn: 2  
mail: jefe2@gmail.com  
givenName: jefe

dn: uid=currito1,ou=OU\_Curritos,dc=josue,dc=local  
objectClass: top  
objectClass: posixAccount  
objectClass: inetOrgPerson  
objectClass: person  
cn: currito1  
uid: currito1  
ou: G\_Curritos  
uidNumber: 2000  
gidNumber: 10001  
homeDirectory: /home/currito1  
loginShell: /bin/bash  
userPassword: {SSHA}Ybk3NVD0QJ42YNqLHakkwecRk1n3Ndyl  
sn: 1  
mail: currito1@gmail.com  
givenName: currito

dn: uid=currito2,ou=OU\_Curritos,dc=josue,dc=local  
objectClass: top  
objectClass: posixAccount  
objectClass: inetOrgPerson  
objectClass: person  
cn: currito2  
uid: currito2  
ou: G\_Curritos  
uidNumber: 2001  
gidNumber: 10001  
homeDirectory: /home/currito2  
loginShell: /bin/bash  
userPassword: {SSHA}YbK3NVD0QJ42YNqLHakkwecRk1n3Ndyl  
sn: 2  
mail: currito2@gmail.com  
givenName: currito

Para ejecutar esto...

```
sudo ldapadd -x -D cn=admin,dc=josue,dc=local -W -f usr.ldif
```

comprobamos con slapcat...

recuperar información de un usuario:

```
ldapsearch -xLLL -b "dc=josue,dc=local" uid=jefe1 sn givenName cn
```

Esto devuelve el sn, givenName, cn del usuario con uid=jefe1

Cambiar la información de un usuario:

```
sudo nano cambios.ldif
```

introducimos lo siguiente:

dn: uid=jefe1,ou=unidad,dc=josue,dc=local

changetype: modify

replace: mail

mail: [jefe1.modificado@josue.local](mailto:jefe1.modificado@josue.local)

para ejecutar:

```
ldapmodify -x -D cn=admin,dc=josue,dc=local -W -f cambios.ldif
```

Borrar un usuario:

```
ldapdelete -x -W -D 'cn=admin,dc=josue,dc=local' "uid=jefe1,ou=unidad,dc=josue,dc=local"
```

Autenticar usuarios ldap con apache:

Para autenticar un usuario con LDAP se debe habilitar el modulo authnz\_ldap

En el fichero .htaccess:

AuthType Basic

AuthBasicProvider ldap

AuthName "login...."

AuthLDAPURL "ldap://192.168.3.112/dc=josue,dc=local?uid?sub?(objectClass=\*)"

AuthLDAPBindDN "cn=admin,dc=josue,dc=local"

AuthLDAPBindPassword paso

Require ldap-user Currito1