

Tutorial: OpenLDAP

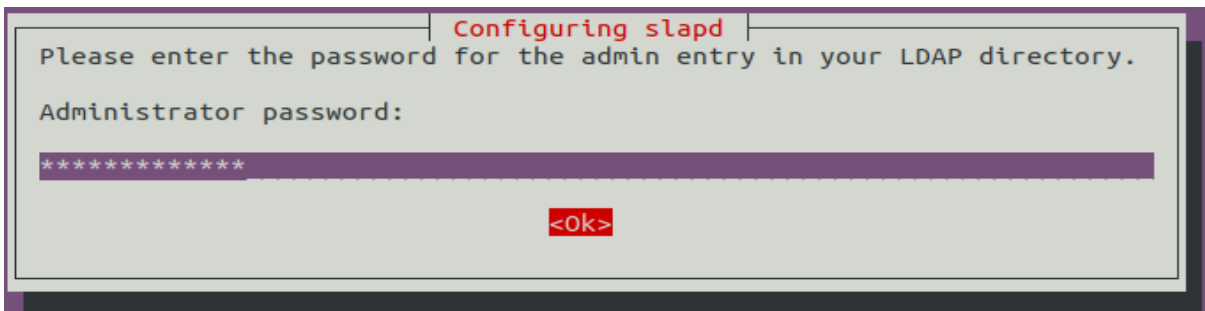
Ramon Caselles Ginestar

Instalamos *OpenLdap* con el siguiente comando

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

```
root@omen:/home/omen# sudo apt-get install slapd ldap-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-5.11.0-43-generic linux-hwe-5.11-headers-5.11.0-43
  linux-image-5.11.0-43-generic linux-modules-5.11.0-43-generic
  linux-modules-extra-5.11.0-43-generic
```

Durante la instalación, aparece en la consola un mensaje que nos solicita la contraseña de administración para *LDAP*. Pedirá una segunda confirmación. ramonopenldap



Tras confirmar, la instalación termina y pasamos a configurar el archivo `/etc/hosts`. Añadimos una nueva línea con los nombres de dominio para nuestro host.

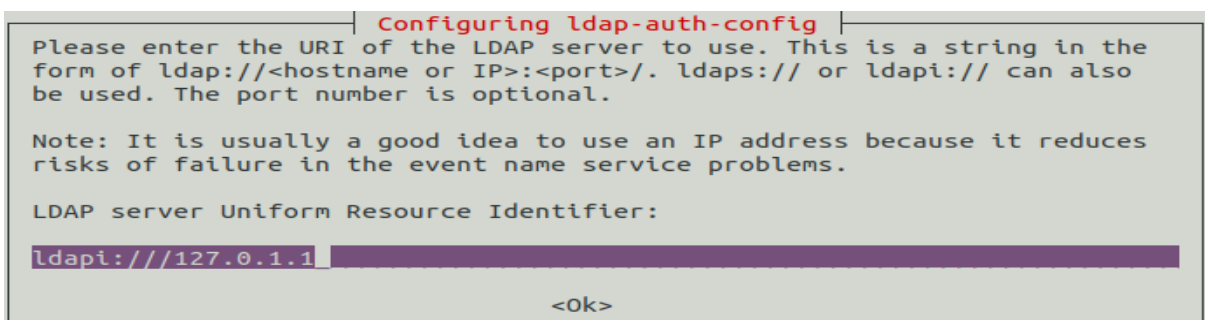
```
sudo nano /etc/hosts
```

```
GNU nano 4.8 /etc/hosts Modified
127.0.0.1    localhost
127.0.1.1    omen
127.0.1.1    proftpd.com
127.0.1.1    ldapserver.com www.ldapserver.com
```

A continuación, instalaremos la librería *NSS* para *LDAP*.

```
sudo apt-get install libnss-ldap -y
```

Durante la instalación se abrirá el asistente donde nos solicita la dirección URi del servidor *LDAP*. Dejando la primera parte tal cual escribimos la ip que establecimos anteriormente en `hosts`.



OpenLDAP

A continuación estableceremos el nombre global único.

Configuring 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=ldapserver,dc=local

<Ok>

Seguidamente elegimos la versión del protocolo *LDAP* que vamos a utilizar. Se recomienda la más alta.

Configuring 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

En el siguiente paso elegimos yes. Esto hará que las contraseñas se guarden en un archivo independiente que sólo podrá ser leído por el superusuario.

Configuring 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:

<Yes> <No>

A continuación nos da la opción de hacer consultas a la base de datos ldap solo con identificación, elegimos no.

Does the LDAP database require login?

<Yes> <No>

OpenLDAP

Indicamos el usuario que hará de manager y su contraseña.

LDAP account for root:

cn=admin,dc=ldapserver,dc=local

<Ok>

El último paso en la configuración del servidor LDAP será establecer algunos parámetros en la configuración de este demonio.

```
sudo dpkg-reconfigure slapd
```

Configuring slapd

If you enable this option, no initial configuration or database will be created for you.

Omit OpenLDAP server configuration?

<Yes>

<No>

Configuring slapd

The DNS domain name is used to construct the base DN of the LDAP directory. For example, 'foo.example.org' will create the directory with 'dc=foo, dc=example, dc=org' as base DN.

DNS domain name:

ldapserver.local

<Ok>

Configuring slapd

Please enter the name of the organization to use in the base DN of your LDAP directory.

Organization name:

OpenCorp

<Ok>

Configuring slapd

Please enter the password for the admin entry in your LDAP directory.

Administrator password:

<Ok>

Confirm password:

<Ok>

Tras seguir el asistente pasamos a crear la estructura del directorio.

OpenLDAP

```
sudo nano ~/base.ldif
```

```
dn: ou=usuarios,dc=ldapserver,dc=local
objectClass: organizationalUnit
ou: usuarios
```

```
dn: ou=grupos,dc=ldapserver,dc=local
objectClass: organizationalUnit
ou: grupos
```

```
GNU nano 4.8 /root/base.ldif Modified
dn: ou=usuarios,dc=ldapserver,dc=local
objectClass: organizationalUnit
ou: usuarios

dn: ou=grupos,dc=ldapserver,dc=local
objectClass: organizationalUnit
ou: grupos
```

A continuación, deberemos añadir la información a la base de datos *OpenLDAP*.

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

```
root@omen:~# sudo ldapadd -x -D cn=admin,dc=ldapserver,dc=local -W -f base.ldif
Enter LDAP Password:
adding new entry "ou=usuarios,dc=ldapserver,dc=local"

adding new entry "ou=grupos,dc=ldapserver,dc=local"
```

Finalmente podremos añadir usuarios y grupos.

```
sudo nano ~/usuario.ldif
```

```
dn: uid=ramon,ou=usuarios,dc=ldapserver,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: ramon
sn: ramon
givenName: ramon
cn: ramon
displayName: ramon
uidNumber: 1000
gidNumber: 10000
userPassword: password
gecos: ramon
loginShell: /bin/bash
homeDirectory: /home/omen
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: ramoncgcom@gmail.com
```

OpenLDAP

```
GNU nano 4.8 /root/usuario.ldif Modified
dn: uid=ramon,ou=usuarios,dc=ldapserver,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: ramon
sn: ramon
givenName: ramon
cn: ramon
displayName: ramon
uidNumber: 1000
gidNumber: 10000
userPassword: password
gecos: ramon
```

Faltaría cargar el usuario en el directorio.

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

```
root@omen:~# sudo ldapadd -x -D cn=admin,dc=ldapserver,dc=local -W -f usuario.ldif
Enter LDAP Password:
adding new entry "uid=ramon,ou=usuarios,dc=ldapserver,dc=local"
root@omen:~# █
```

Para comprobar el nuevo usuario podemos usar el siguiente comando

```
ldapsearch -xLLL -b "dc=ldapserver,dc=local" uid=ramon sn givenName cn
```

```
root@omen:~# ldapsearch -xLLL -b "dc=ldapserver,dc=local" uid=ramon sn givenName cn
dn: uid=ramon,ou=usuarios,dc=ldapserver,dc=local
sn: ramon
givenName: ramon
cn: ramon
```