CENTRE ESPECÍFIC
D´EDUCACIÓ A DISTÀNCIA DE
LA COMUNITAT VALENCIANA

UNIT 4.
ACTIVITY

Web Applications Deployment
CFGS DAW

Important: this activity is not mandatory and does not compute for the final grade.

Importante: esta actividad no es obligatoria y no cuenta para la nota final.

Author: Carlos Cacho López

Reviewed by: Lionel Tarazón Alcocer
lionel.tarazon@ceedcv.es

2019/2020

License

Nomenclature

During this unit we are going to use special symbols to distinct some important elements.

This symbols are:

Important

Attention

Interesting

INDEX

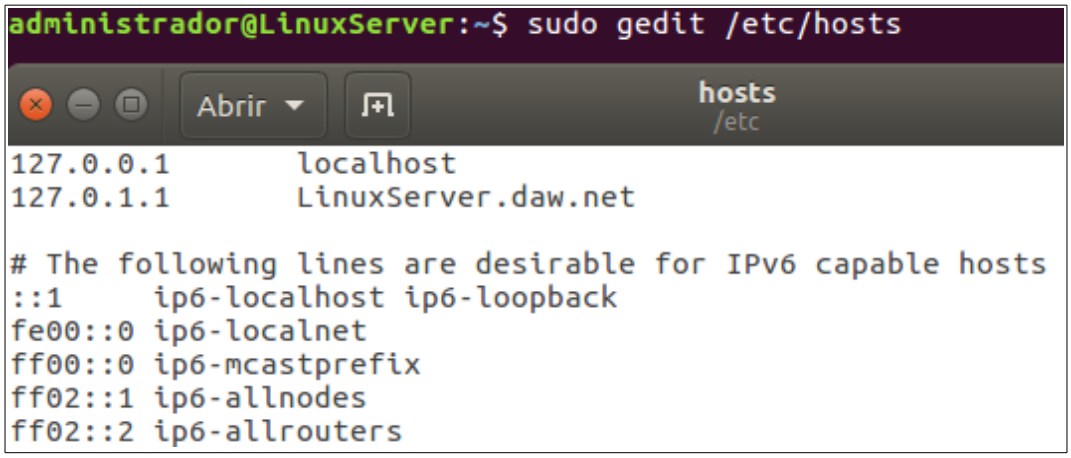
UT04. DIRECTORY SERVICE

1. INTRODUCTION

In this activity we are going to install and manage the directory server OpenLDAP in our virtual machine *linuxserver*. **First, we have to stop the Nginx server and start the Apache sever.**

2. INSTALLING OPENLDAP

First of all, we need to modify the file /etc/hosts and include this:

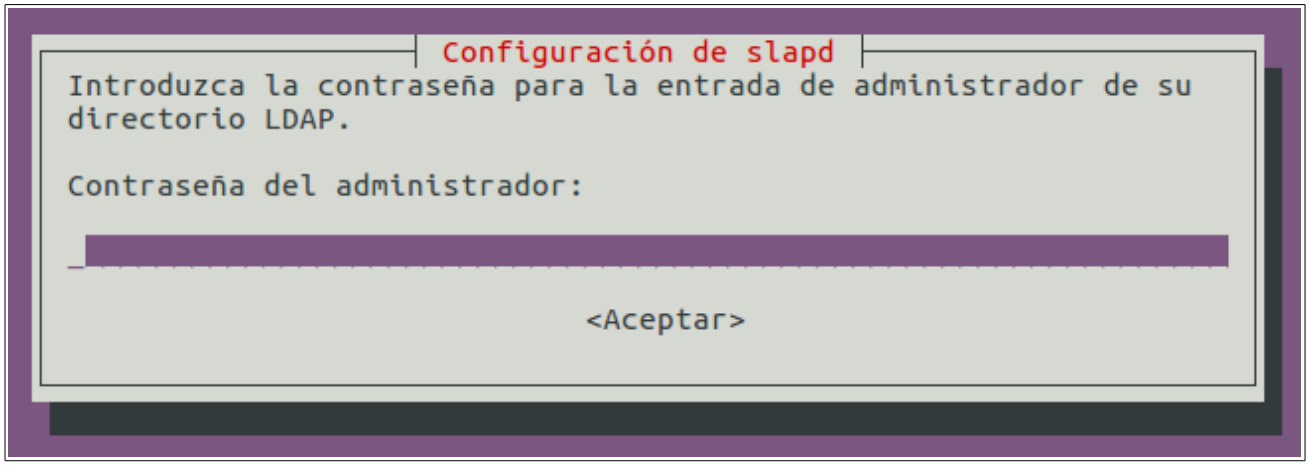


Also, open the network configuration and use a default (automatic) DNS or a public DNS such as Google's 8.8.8.8. Do not forget restart the service networking.

Now, install the OpenLDAP server. To do so write in the terminal:

sudo apt-get install slapd

During the installation we will have to write the administrator password twice:



Once installed, we can check if the server is running and listening in port 389/TCP. We have to write **ps -ef | grep slapd** and then **netstat -ltn**

```
administrador@LinuxServer:~$ ps -ef | grep slapd
openldap  2775     1  0 09:27 ?        00:00:00 /usr/sbin/slapd -h ldap:/// ldap
i:/// -g openldap -u openldap -F /etc/ldap/slapd.d
adminis+  2840  1919  0 09:28 pts/4    00:00:00 grep --color=auto slapd
administrador@LinuxServer:~$ netstat -ltn
Conexiones activas de Internet (solo servidores)
Proto  Recib Enviad Dirección local          Dirección remota        Estado
tcp        0      0 0.0.0.0:389             0.0.0.0:*               ESCUCHAR
tcp        0      0 192.168.1.2:53          0.0.0.0:*               ESCUCHAR
tcp        0      0 127.0.0.1:53            0.0.0.0:*               ESCUCHAR
tcp        0      0 0.0.0.0:22              0.0.0.0:*               ESCUCHAR
tcp        0      0 127.0.0.1:953           0.0.0.0:*               ESCUCHAR
tcp6       0      0 :::389                  :::*                    ESCUCHAR
tcp6       0      0 127.0.0.1:8005          :::*                    ESCUCHAR
tcp6       0      0 :::8009                 :::*                    ESCUCHAR
tcp6       0      0 :::8080                 :::*                    ESCUCHAR
tcp6       0      0 :::80                   :::*                    ESCUCHAR
tcp6       0      0 :::53                   :::*                    ESCUCHAR
tcp6       0      0 :::21                   :::*                    ESCUCHAR
tcp6       0      0 :::22                   :::*                    ESCUCHAR
tcp6       0      0 ::1:953                 :::*                    ESCUCHAR
tcp6       0      0 :::443                  :::*                    ESCUCHAR
```

Now we are going to install the OpenLDAP packet with utilities, for that we write in the terminal:

sudo apt-get install ldap-utils

Then, we will check the directories **/etc/ldap**, **/etc/ldap/slapd.d** (with the DIT with the server configuration) and **/etc/ldap/schema** (with the server schemes in *ldif* format)

```
administrador@LinuxServer:~$ ls /etc/ldap
ldap.conf  sasl2  schema  slapd.d
administrador@LinuxServer:~$ sudo ls /etc/ldap/slapd.d
cn=config  cn=config.ldif
```

```
administrador@LinuxServer:~$ ls /etc/ldap/schema/
collective.ldif    cosine.schema         java.ldif      openldap.ldif
collective.schema  duaconf.ldif          java.schema    openldap.schema
corba.ldif         duaconf.schema        ldapns.schema  pmi.ldif
corba.schema       dyngroup.ldif         misc.ldif      pmi.schema
core.ldif          dyngroup.schema       misc.schema    ppolicy.ldif
core.schema        inetorgperson.ldif    nis.ldif       ppolicy.schema
cosine.ldif        inetorgperson.schema  nis.schema     README
```

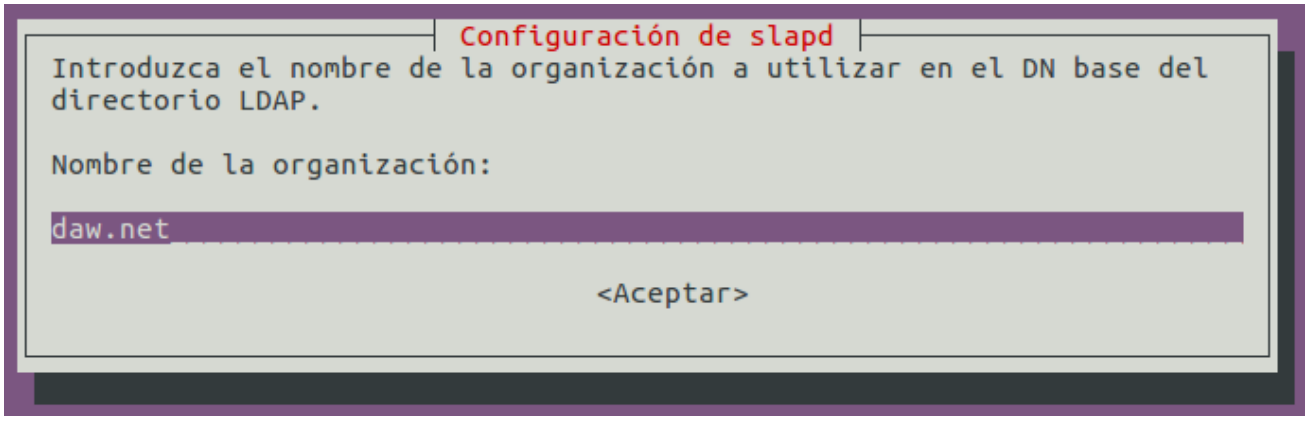
This is one way to install the server. Another way is to use the configuration wizard. We are going to work with it. For that, we write in the terminal:

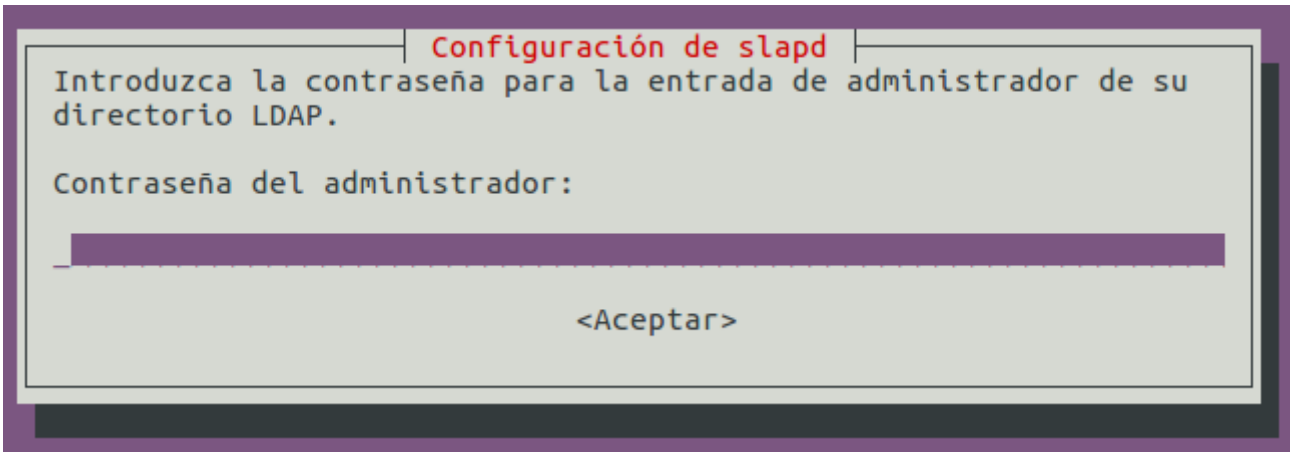
sudo dpkg-reconfigure slapd

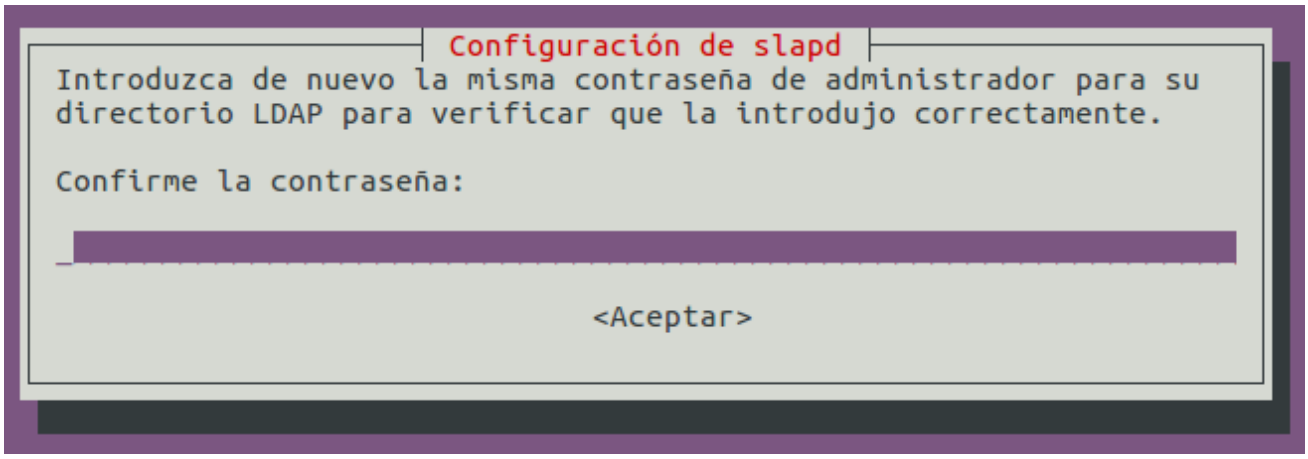
And follow these steps:

```
Configuración de slapd

No se creará la configuración ni la base de datos inicial si habilita
esta opción.

¿Desea omitir la configuración del servidor OpenLDAP?

                <Sí>                    <No>
```

```
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:

daw.net

                        <Aceptar>
```


Configuración de slapd
Introduzca el nombre de la organización a utilizar en el DN base del directorio LDAP.
Nombre de la organización:
daw.net
<Aceptar>

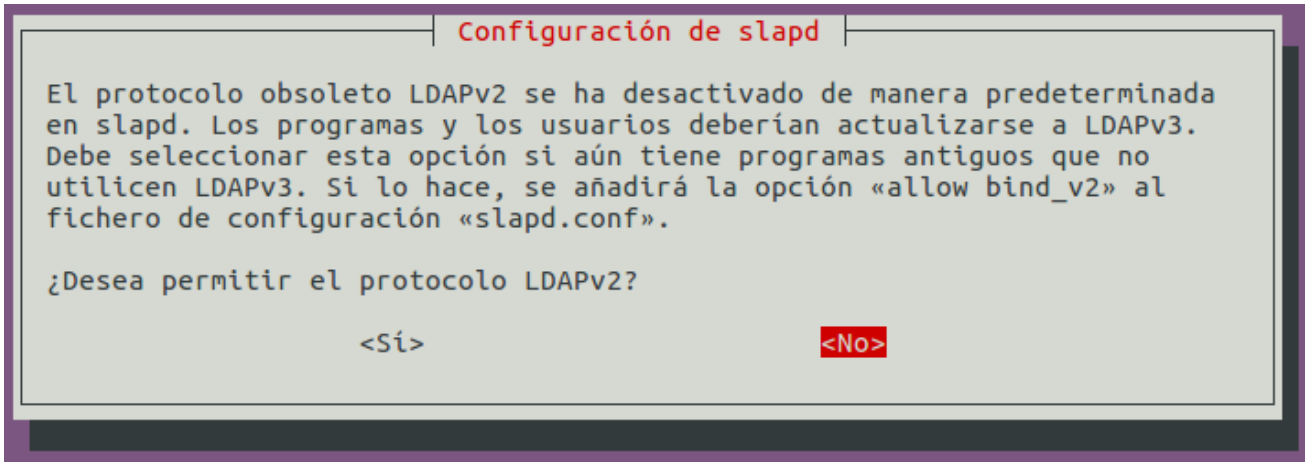

Configuración de slapd
Introduzca la contraseña para la entrada de administrador de su directorio LDAP.
Contraseña del administrador:
<Aceptar>


Configuración de slapd
Introduzca de nuevo la misma contraseña de administrador para su directorio LDAP para verificar que la introdujo correctamente.
Confirme la contraseña:
<Aceptar>

```
Configuración de slapd
Los motores HDB y BDB utilizan formatos de almacenamiento semejantes,
pero HDB permite realizar cambios de nombre de subárboles («subtree
renames»). Los dos permiten las mismas opciones de configuración.

Se recomienda utilizar MDB. El motor MDB utiliza un nuevo formato de
almacenamiento y requiere menos configuración que BDB o HDB.

En cualquier caso, debe revisar la configuración de la base de datos.
Consulte «/usr/share/doc/slapd/README.Debian.gz» para más detalles.

Motor de base de datos a utilizar:

                                  BDB
                                  HDB
                                  MDB

                                <Aceptar>
```

```
Configuración de slapd

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

                  <Sí>                        <No>
```

```
Configuración de slapd

Existen ficheros en «/var/lib/ldap» que probablemente interrumpan el
proceso de configuración. Si activa esta opción, se moverán los ficheros
de las bases de datos antiguas antes de crear una nueva base de datos.

¿Desea mover la base de datos antigua?

                  <Sí>                        <No>
```

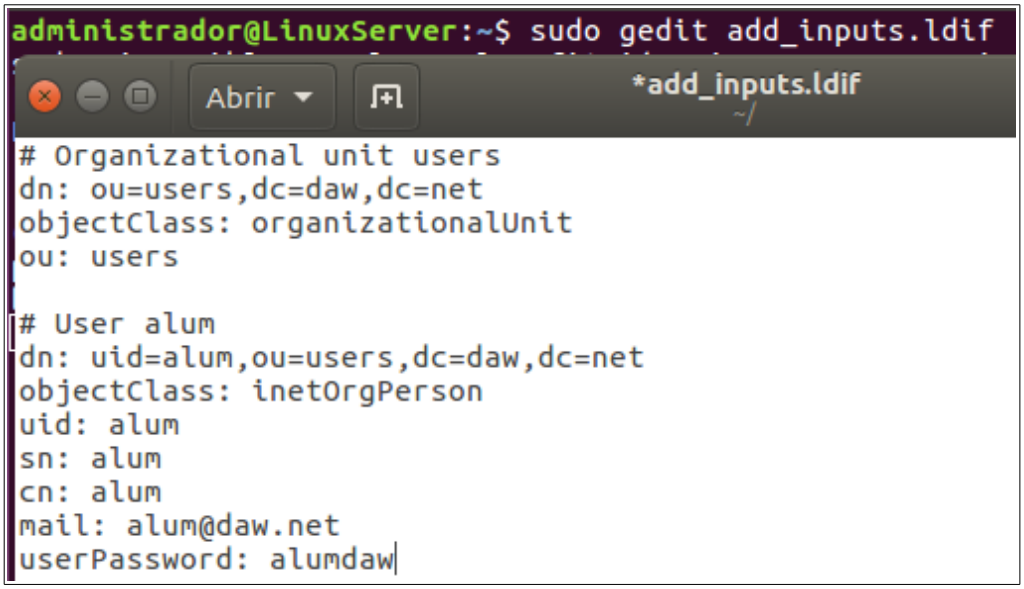


3. USING LDAP

Now we are going to see several functions in LDAP.

3.1 Add

We are going to add inputs to the server. For that we create a file called *add_inputs.lidf* with this content:



Here we create an organizational unit (*objectClass: organizationalUnit*) called *users* and then a new user (*objectClass: inetOrgPerson*) called *alum* with the uid (User ID), sn (SurName) and cn (Common Name) *alum*, its mail and password.

And add it to the DIT:

```
administrador@LinuxServer:~$ ldapadd -x -D cn=admin,dc=daw,dc=net -W -f add_inputs.ldif

Enter LDAP Password:
adding new entry "ou=users,dc=daw,dc=net"

adding new entry "uid=alum,ou=users,dc=daw,dc=net"
```

The options used in the command ***ldapadd*** are:

-x Use simple authentication instead of SASL.

-D binddn Use the Distinguished Name binddn to bind to the LDAP directory.

-W Prompt for simple authentication.

-f file Read the entry modification information from *file*.

3.2 Find

Now, we will check all the DIT:

```
administrador@LinuxServer:~$ ldapsearch -x -b dc=daw,dc=net
# extended LDIF
#
# LDAPv3
# base <dc=daw,dc=net> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# daw.net
dn: dc=daw,dc=net
objectClass: top
objectClass: dcObject
objectClass: organization
o: daw.net
dc: daw

# admin, daw.net
dn: cn=admin,dc=daw,dc=net
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# users, daw.net
dn: ou=users,dc=daw,dc=net
objectClass: organizationalUnit
ou: users

# alum, users, daw.net
dn: uid=alum,ou=users,dc=daw,dc=net
objectClass: inetOrgPerson
uid: alum
sn: alum
cn: alum
mail: alum@daw.net

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
```

And check the attribute *mail*:

```
administrador@LinuxServer:~$ ldapsearch -x -b dc=daw,dc=net mail
# extended LDIF
#
# LDAPv3
# base <dc=daw,dc=net> with scope subtree
# filter: (objectclass=*)
# requesting: mail
#

# daw.net
dn: dc=daw,dc=net

# admin, daw.net
dn: cn=admin,dc=daw,dc=net

# users, daw.net
dn: ou=users,dc=daw,dc=net

# alum, users, daw.net
dn: uid=alum,ou=users,dc=daw,dc=net
mail: alum@daw.net

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
```

The options used in the command ***ldapsearch*** are:

-x Use simple authentication instead of SASL.

-b searchbase Use searchbase as the starting point for the search.

3.3 Modify

Now we are going to add the attribute *mobile* and modify the attribute *mail*. For that we create a file called *modify_inputs.ldif*:

```
administrador@LinuxServer:~$ gedit modify_inputs.ldif
```

modify_inputs.ldif (~/) - gedit

Abrir

```
dn: uid=alum,ou=users,dc=daw,dc=net
add:mobile
mobile:000000000

dn: uid=alum,ou=users,dc=daw,dc=net
changetype: modify
replace:mail
mail: alumnewmail@daw.net
```

```
administrador@LinuxServer:~$ ldapmodify -x -D cn=admin,dc=daw,dc=net -W -f modify_inputs.ldif
Enter LDAP Password:
modifying entry "uid=alum,ou=users,dc=daw,dc=net"

modifying entry "uid=alum,ou=users,dc=daw,dc=net"
```

The options used in the command ***ldapmodify*** are:

-x Use simple authentication instead of SASL.

-D binddn Use the Distinguished Name binddn to bind to the LDAP directory.

-W Prompt for simple authentication.

-f file Read the entry modification information from *file*.

And we check the DIT:

```
administrador@LinuxServer:~$ ldapsearch -x -b dc=daw,dc=net
```

```
# alum, users, daw.net
dn: uid=alum,ou=users,dc=daw,dc=net
objectClass: inetOrgPerson
uid: alum
sn: alum
cn: alum
mobile: 000000000
mail: alumnewmail@daw.net
```

3.4 Delete

Now we are going to delete the group and the user. We create a file again:

```
administrador@LinuxServer:~$ gedit delete_inputs.ldif
delete_inputs.ldif (~/) - gedit
Abrir
uid=alum,ou=users,dc=daw,dc=net
ou=users,dc=daw,dc=net
```

```
administrador@LinuxServer:~$ ldapdelete -x -D cn=admin,dc=daw,dc=net -W -f delete_inputs.ldif
Enter LDAP Password:
```

The options used in the command ***ldapdelete*** are:

-x Use simple authentication instead of SASL.

-D binddn Use the Distinguished Name binddn to bind to the LDAP directory.

-W Prompt for simple authentication.

-f file Read a series of lines from file, performing one LDAP search for each line.

And we check the DIT:

```
administrador@LinuxServer:~$ ldapsearch -x -b dc=daw,dc=net
# extended LDIF
#
# LDAPv3
# base <dc=daw,dc=net> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# daw.net
dn: dc=daw,dc=net
objectClass: top
objectClass: dcObject
objectClass: organization
o: daw.net
dc: daw

# admin, daw.net
dn: cn=admin,dc=daw,dc=net
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

We can see that the group *users* and the user *alum* are deleted.

4. INSTALLING LDAP CLIENT

Now we are going to install a LDAP client called **phpLDAPadmin**:

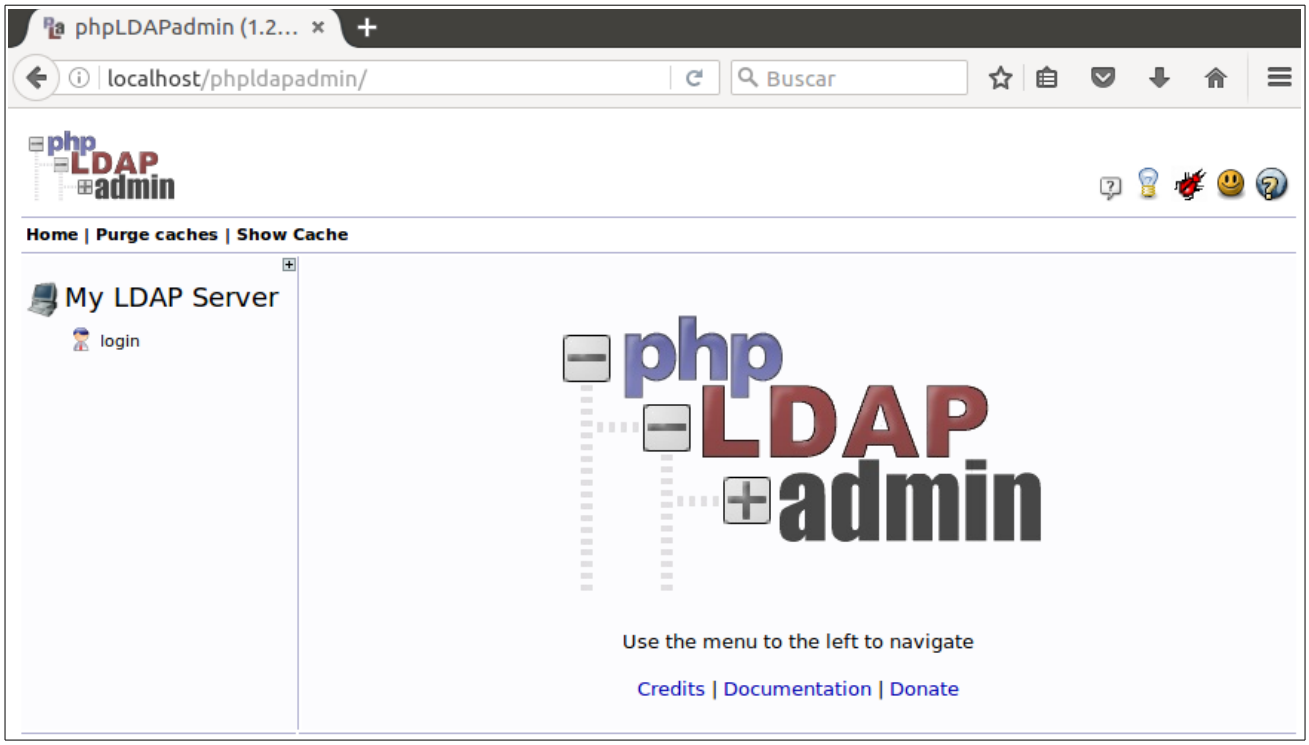
```
administrador@LinuxServer:~$ sudo apt-get install phpldapadmin
```

Then, we have to modify two lines of the file */etc/phpldapadmin/config.php*:

```
administrador@LinuxServer:~$ sudo gedit /etc/phpldapadmin/config.php
Abrir  *config.php  /etc/phpldapadmin
289     'ldap.example.com',
290     'ldaps://ldap.example.com/',
291     'ldapi://%2fusr%local%2fvar%2frun%2fldapi'
292             (Unix socket at /usr/local/var/run/ldap) */
293 $servers->setValue('server','host','127.0.0.1');
294
295 /* The port your LDAP server listens on (no quotes). 389 is standard. */
296 // $servers->setValue('server','port',389);
297
298 /* Array of base DNs of your LDAP server. Leave this blank to have
    phpLDAPadmin
299     auto-detect it for you. */
300 $servers->setValue('server','base',array('dc=daw,dc=net'));
```

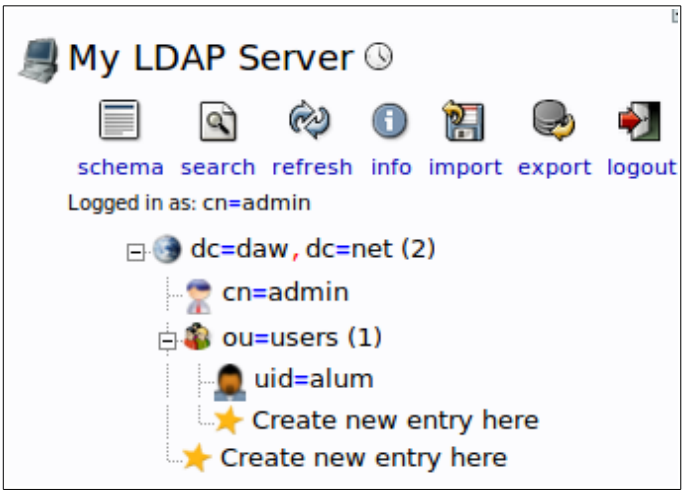
```
324     the directory for users (ie, if your LDAP server does not allow anonymous
325     binds. */
326 $servers->setValue('login','bind_id','cn=admin,dc=daw,dc=net');
327 #   $servers->setValue('login','bind_id','cn=Manager,dc=example,dc=com');
328
```

Next we are going to load the group and user of our *add_inputs.ldif* file. And we will run the client:



We click on ***LOGIN*** and write the admin password:

And we could see all the configuration, create new users and groups:



5. AUTHENTICATION AND AUTHORIZATION LDAP IN APACHE

Now, we are going to configure Apache for use the users of LADP. For that we have to enable the module ***mod_authnz_ldap***:

sudo a2enmod authnz_ldap

And restart Apache.

Now we, modify the default site and write the following: (if we have the configuration of the before activities we will have create the directory *alum* and the *index.html* file.)

```
administrador@LinuxServer:~$ sudo gedit /etc/apache2/sites-available/000-default.conf
Abrir   *000-default.conf   Guardar
/etc/apache2/sites-available

<Directory /var/www/html/alum>
    Options FollowSymLinks MultiViews
    AllowOverride None
    Order allow,deny
    allow from all
    AuthType Basic
    AuthBasicProvider ldap
    AuthName "Insert user and password"
    AuthLDAPURL "ldap://localhost/dc=daw,dc=net?uid?sub?(objectClass=*)"
    AuthLDAPBindDN "cn=admin,dc=daw,dc=net"
    AuthLDAPBindPassword daw
    Require valid-user
</Directory>
```

We restart Apache and try to access to *192.168.1.2/alum/index.html*: (we will write the password for the user define in LDAP)