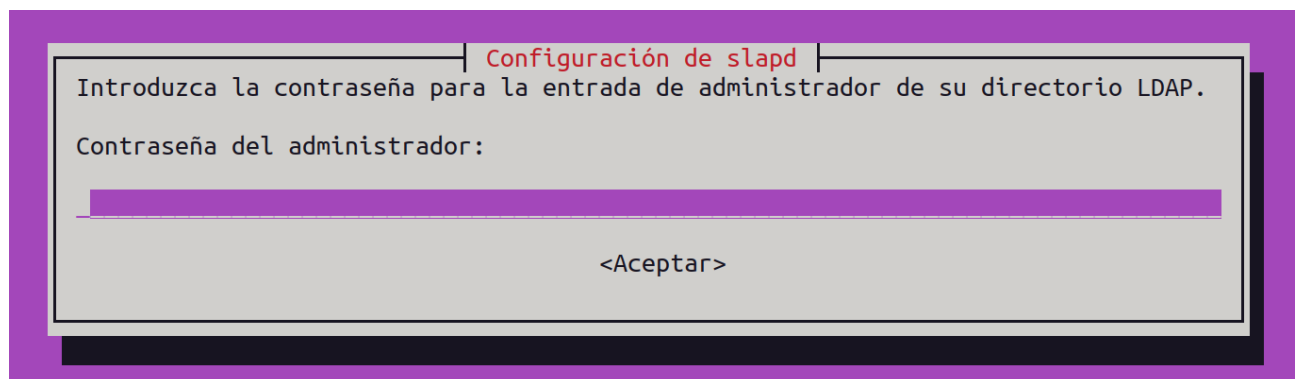


Práctica: Instalación y configuración de LDAP

Para instalar LDAP y sus utilidades, vamos a ejecutar “sudo apt install slapd ldap-utils”

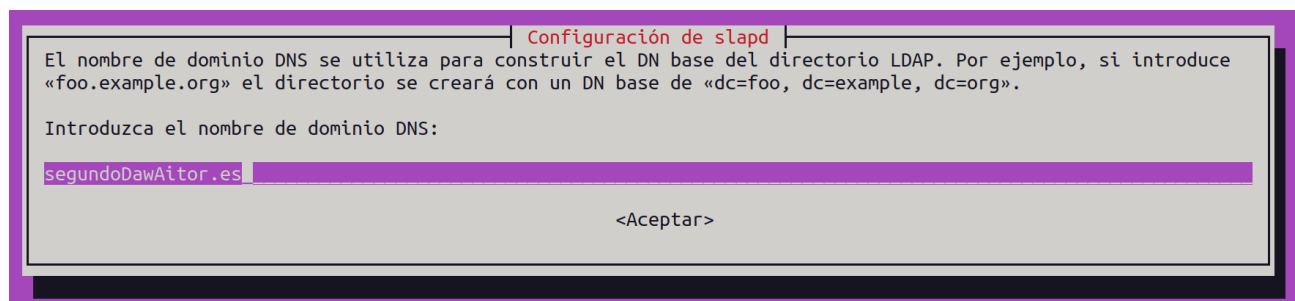
En la propia instalación nos van a pedir que definamos la contraseña de administrador.



The screenshot shows a terminal window titled "Configuración de slapd". The text inside reads: "Introduzca la contraseña para la entrada de administrador de su directorio LDAP." followed by "Contraseña del administrador:". Below this is a text input field containing a series of asterisks. At the bottom of the window is a button labeled "<Aceptar>".

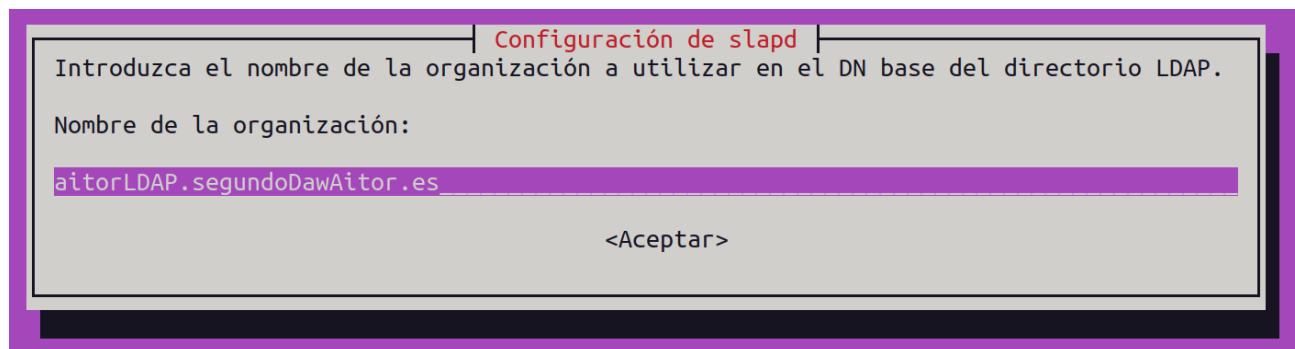
Si no nos pide nada más y finaliza la instalación, debemos ejecutar “sudo dpkg-reconfigure slapd”.

En el nombre de dominio asignamos el del DNS.



The screenshot shows a terminal window titled "Configuración de slapd". The text inside reads: "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»." followed by "Introduzca el nombre de dominio DNS:". Below this is a text input field containing "segundoDawAitor.es". At the bottom of the window is a button labeled "<Aceptar>".

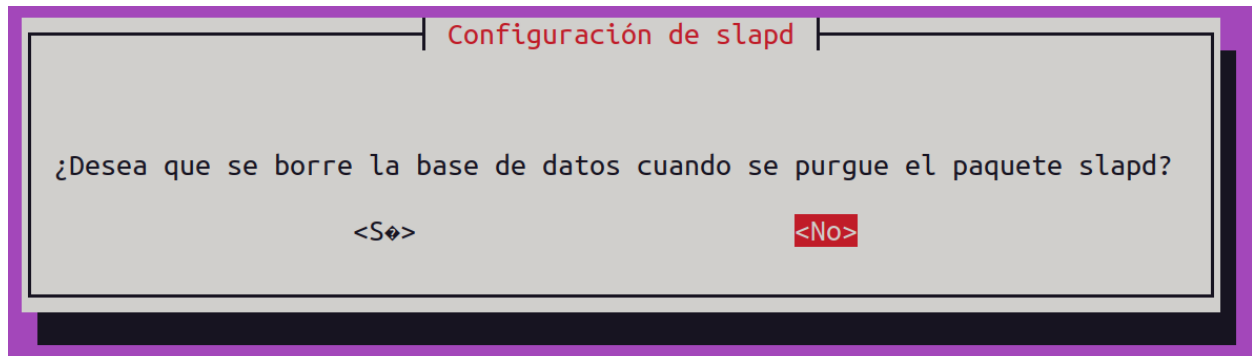
En el nombre de la organización DN base (distingue nuestro LDAP de otros) podemos poner el nombre que queramos aunque es común asignarle un nombre parecido al dominio.



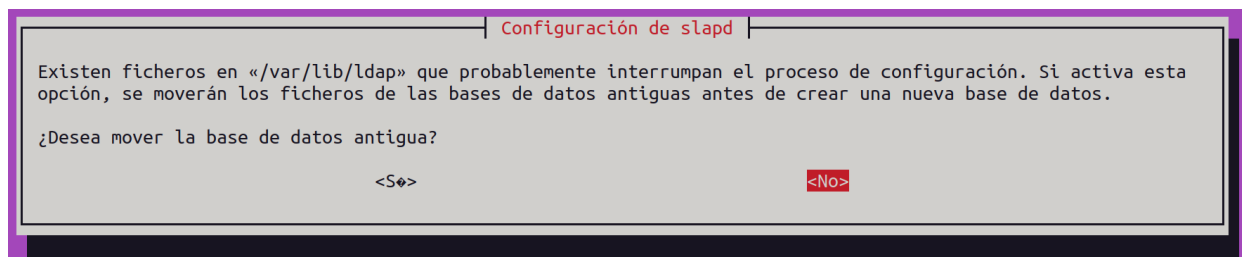
The screenshot shows a terminal window titled "Configuración de slapd". The text inside reads: "Introduzca el nombre de la organización a utilizar en el DN base del directorio LDAP." followed by "Nombre de la organización:". Below this is a text input field containing "aitorLDAP.segundoDawAitor.es". At the bottom of the window is a button labeled "<Aceptar>".

Aitor Pascual Jiménez
Despliegue de aplicaciones
2º Daw

No borramos la base de datos al purgar.



Aunque sea nuestra primera instalación, no vamos a mover los archivos de las bases de datos antiguas (aunque no tengan un uso en este momento).



Por defecto este servicio se encuentra apagado, debemos inicializarlo manualmente.

```
vboxuser@ubuntu-despliegue:~$ sudo systemctl start slapd
vboxuser@ubuntu-despliegue:~$ sudo systemctl status slapd
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
   Loaded: loaded (/etc/init.d/slapd; generated)
   Drop-In: /usr/lib/systemd/system/slapd.service.d
            └─slapd-remain-after-exit.conf
   Active: active (running) since Fri 2024-10-25 09:22:54 CEST; 1s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 4971 ExecStart=/etc/init.d/slapd start (code=exited, status=0/SUCCESS)
    Tasks: 3 (limit: 9438)
   Memory: 3.3M
      CPU: 38ms
   CGroup: /system.slice/slapd.service
            └─4978 /usr/sbin/slapd -h "ldap:/// ldapi:///" -g openldap -u openldap -F /etc/ldap/slapd.d
```

Con ldapsearch podemos comprobar la configuración del directorio.

ldapsearch -x -LLL -H ldap:/// -b dc=nombreDominio,dc=raiz

- -x Simple
- -H LDAP URI
- -b dn base a buscar
- -LLL para el formato

```
-L      print responses in LDIFv1 format
-LL     print responses in LDIF format without comments
-LLL    print responses in LDIF format without comments
        and version
```

Aitor Pascual Jiménez
Despliegue de aplicaciones
2º Daw

```
vboxuser@ubuntu-despliegue:~$ ldapsearch -x -LLL -H ldap:/// -b dc=segundoDawAitor,dc=es
dn: dc=segundoDawAitor,dc=es
objectClass: top
objectClass: dcObject
objectClass: organization
o: myguest.virtualbox.org
dc: segundoDawAitor
```

Para añadir usuarios y grupos, debemos crear unos ficheros específicos con extensión .ldif

Crearemos una unidad organizativa con esta sintaxis.

```
dn: ou=groups,dc=segundoDawAitor,dc=es
objectClass: organizationalUnit
ou: groups
```

La añadimos con este comando.

```
vboxuser@ubuntu-despliegue:/etc/ldap/groups$ sudo ldapadd -x -D cn=admin,dc=segundoDawAitor,dc=es -W -f ou_grupo.ldif
Enter LDAP Password:
adding new entry "ou=groups,dc=segundoDawAitor,dc=es"
```

Para crear un grupo.

```
dn: cn=alumnos,ou=groups,dc=segundoDawAitor,dc=es
objectClass: top
objectClass: posixGroup
gidNumber: 5000
cn: alumnos
```

Para añadirlo.

```
vboxuser@ubuntu-despliegue:/etc/ldap/groups$ sudo ldapadd -x -D cn=admin,dc=segundoDawAitor,dc=es -W -f grupo.ldif
Enter LDAP Password:
adding new entry "cn=alumnos,ou=groups,dc=segundoDawAitor,dc=es"
```

Puede ser que al insertar un oneliner tan largo, nos equivoquemos escribiendo, en ese caso siempre podemos consultar /var/log/syslog

```
vboxuser@ubuntu-despliegue:/etc/ldap/groups$ sudo ldapadd -x -D cd=admin,dc=segundoDawAitor,dc=es -W -f grupo.ldif
Enter LDAP Password:
ldap_bind: Invalid DN syntax (34)
additional info: invalid DN
```

```
Oct 28 09:29:09 ubuntu-despliegue slapd[2269]: conn=1002 op=0 do_bind: invalid dn (cd=admin,dc=segundoDawAitor,dc=es)
```

Aitor Pascual Jiménez
Despliegue de aplicaciones
2º Daw

Vamos a crear otra unidad organizativa.

```
vboxuser@ubuntu-despliegue:/etc/ldap/groups$ sudo cat ou_people.ldif
dn: ou=people,dc=segundoDawAitor,dc=es
objectClass: organizationalUnit
ou: people
vboxuser@ubuntu-despliegue:/etc/ldap/groups$ sudo ldapadd -x -D cn=admin,dc=segundoDawAitor,dc=es -W -f ou_people.ldif
Enter LDAP Password:
adding new entry "ou=people,dc=segundoDawAitor,dc=es"
```

y un usuario.

```
dn: uid=Aitor,ou=groups,dc=segundoDawAitor,dc=es
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
cn: Aitor
sn: Usuario
uid: Aitor
uidNumber: 10001
gidNumber: 10000
homeDirectory: /home/aitor
loginShell: /bin/bash
userPassword: {SSHA}gkpRG6bu6WSJXAk3Mt2jRu97m7Mk7aji
```

Id del grupo que hemos creado antes

usaremos slappasswd para generar el hash de la contraseña

Lo añadimos.

```
vboxuser@ubuntu-despliegue:/etc/ldap/groups$ sudo ldapadd -x -D cn=admin,dc=segundoDawAitor,dc=es -W -f usuario.ldif
Enter LDAP Password:
adding new entry "uid=Aitor,ou=groups,dc=segundoDawAitor,dc=es"
```

Para agregar el usuario al grupo alumnos, debemos crear otro fichero y usar ldapmodify.

```
dn: cn=alumnos,ou=groups,dc=segundoDawAitor,dc=es
changetype: modify
add: memberUid
memberUid: Aitor
```

De esta manera añadimos el usuario al grupo.

```
vboxuser@ubuntu-despliegue:/etc/ldap/groups$ sudo ldapmodify -x -D "cn=admin,dc=segundoDawAitor,dc=es" -W -f aitorAlumnos.ldif
Enter LDAP Password:
modifying entry "cn=alumnos,ou=groups,dc=segundoDawAitor,dc=es"
```