10.1. Instalación de *OpenLDAP 2.4* en *Linux*

Instala el servidor *OpenLDAP* (`http://www.openldap.org/`) en la máquina **ServidorLinuxXX** y configúralo con las siguientes opciones:

- La entidad raíz de nuestro DIT usará como DN `dc=dawXX, dc=net`
- Establece la clave del usuario **admin** (`dn: cn=admin, dc=dawXX, dc=net`).

1. **Instalación**

   1.1. Inicia una sesión en **ServidorLinuxXX** con un usuario con privilegios de administración.

   1.2. Instala el servidor desde los repositorios oficiales de *Ubuntu*.

   ```
   sudo apt-get update
   sudo apt-get install slapd
   ```

   1.3. Introduce la contraseña del administrador (`dn: cn=admin, dc=dawXX, dc=net`) (usaremos **despliegue**), Figura 10.1.

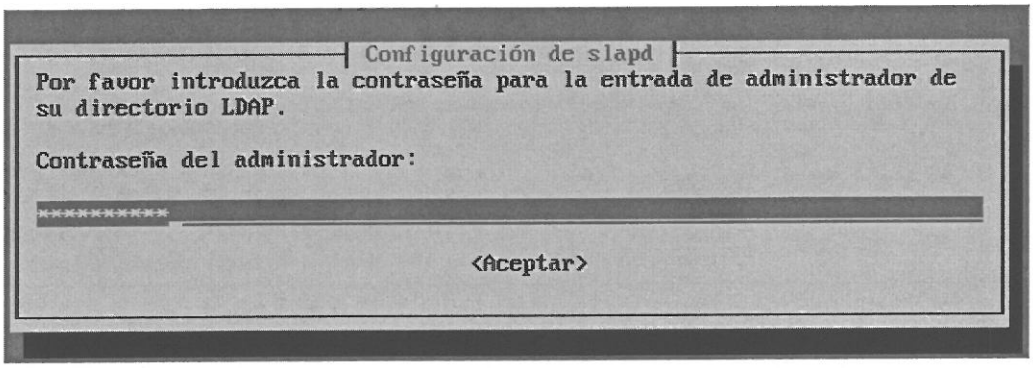

Figura 10.1: Contraseña del usuario admin

   1.4. Vuelve a introducir la contraseña.

   Al instalar el servidor se crean:

   - Los archivos de configuración.
   - Dos DIT
     - Uno con la configuración del servidor (*slapd-conf*).
     - Otro con nuestra configuración (`dc=dawXX dc=net`) (utiliza como **dawXX.net** porque está definido como nombre de dominio en el fichero **/etc/hosts** .
   - Esquemas usados por el servidor.

   1.5. Comprueba que el servidor está iniciado y escuchando peticiones en el puero 389/TCP.

   ```
   ps -ef | grep slapd
   netstat -ltn
   ```

2. **Utilidades *OpenLDAP***

   2.1. Instala el paquete **ldap-utils** que contiene un conjunto de utilidades cliente (`ldapadd, ldapsearch, ldapdelete, ldapmodify`, ...) y servidor (`slapcat, slaptest`).

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

3. **Configuración por defecto**

   3.1. Consulta el directorio **/etc/ldap** y observa los ficheros y directorios de configuración.

   3.2. Consulta el directorio **/etc/ldap/slapd.d** donde se almacena el DIT de configuración del servidor, Figura 10.2.

```
/etc/ldap/slapd.d/

├── cn=config
│   ├── cn=module{0}.ldif
│   ├── cn=schema
│   │   ├── cn={0}core.ldif
│   │   ├── cn={1}cosine.ldif
│   │   ├── cn={2}nis.ldif
│   │   └── cn={3}inetorgperson.ldif
│   ├── cn=schema.ldif
│   ├── olcBackend={0}hdb.ldif
│   ├── olcDatabase={0}config.ldif
│   ├── olcDatabase={-1}frontend.ldif
│   └── olcDatabase={1}hdb.ldif
└── cn=config.ldif
```

Figura 10.2: DIT de configuración del servidor

   3.3. Consulta el directorio **/etc/ldap/schema** que contiene los *schemas* del servidor (en formato LDIF), Figura 10.3

```
root@ServidorLinux01:/etc/ldap/schema# ls
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
root@ServidorLinux01:/etc/ldap/schema#
```

Figura 10.3: Directorio **/etc/ldap/schema**

   3.4. Utiliza el comando `ldapsearch` para mostrar el DIT `dc=dawXX, dc=net`, Figura 10.4.

   ```
   sudo ldapsearch -x -LLL -H ldap://localhost -b "dc=dawXX, dc=net"
   ```

   ```
   -x: Se usa autenticación simple en lugar SASL.
   -L : muestra la salida en formato LDIFv1.
   ```

```
-LL no muestra los comentarios LDIF.
-LLL no muestra la versión de LDIF.
 Si no se usa L muestra la versión extendida de LDIF.
-H: URL del servidor LDAP.Si se omite se usa localhosst.
-b: Entrada del DIT a partir de donde se empieza a buscar.
```

```
dn: dc=daw01,dc=net
objectClass: top
objectClass: dcObject
objectClass: organization
o: daw01.net
dc: daw01

dn: cn=admin,dc=daw01,dc=net
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
```

Figura 10.4: DIT dc=dawXX, dc=net

Prueba también

```
ldapsearch -x -H ldap://localhost -b "dc=dawXX, dc=net"
ldapsearch -x -H ldap:/// -b "dc=dawXX, dc=net"
ldapsearch -x -b "dc=dawXX, dc=net"
```

4. **Asistente de configuración**

   4.1. Puedes reconfigurar el servidor ldap ejecutando su asistente de configuración, vamos a probar.

   ```
   sudo dpkg-reconfigure slapd
   ```

   4.2. Selecciona que no quieres omitir la configuración.

   4.3. Como nombre de dominio dns introduce `daw01.net`.

   4.4. Como nombre de la organización introduce `daw01.net`.

   4.5. Introduce la contraseña del administrador (usaremos **despliegue**).

   4.6. Vuelve a introducir la contraseña.

   4.7. Selecciona el motor *HDB* (es el recomendado).

   4.8. Indica que no quieres que se borren los datos si se elimina el servidor.

   4.9. Indica que quieres borrar la base de datos antigua.

   4.10. No permitas el protocolo LDAPv2.

   4.11. Utiliza el comando `ldapsearch` para mostrar el DIT `dc=dawXX, dc=net`. Es igual que antes.

   ```
   ldapsearch -x -LLL -H ldap://localhost -b "dc=dawXX, dc=net"
   ```