LDAP

Introducción

¿Qué es LDAP?

- **LDAP** (Lighweight Directory Access Protocol): Protocolo ligero de acceso a directorios.
- LDAP es un protocolo para **consultar y modificar un servicio de directorio** basado en X.500 que se ejecuta sobre **TCP/IP**.
- LDAP fue creado por la **Universidad de Michigan** en 1992.
- Por sí mismo LDAP no define el servicio de directorios. En vez de ello, define el transporte y formato de mensajes utilizado para que un cliente acceda a los datos de un directorio.
- **OpenLDAP** es un conjunto abierto de LDAP.

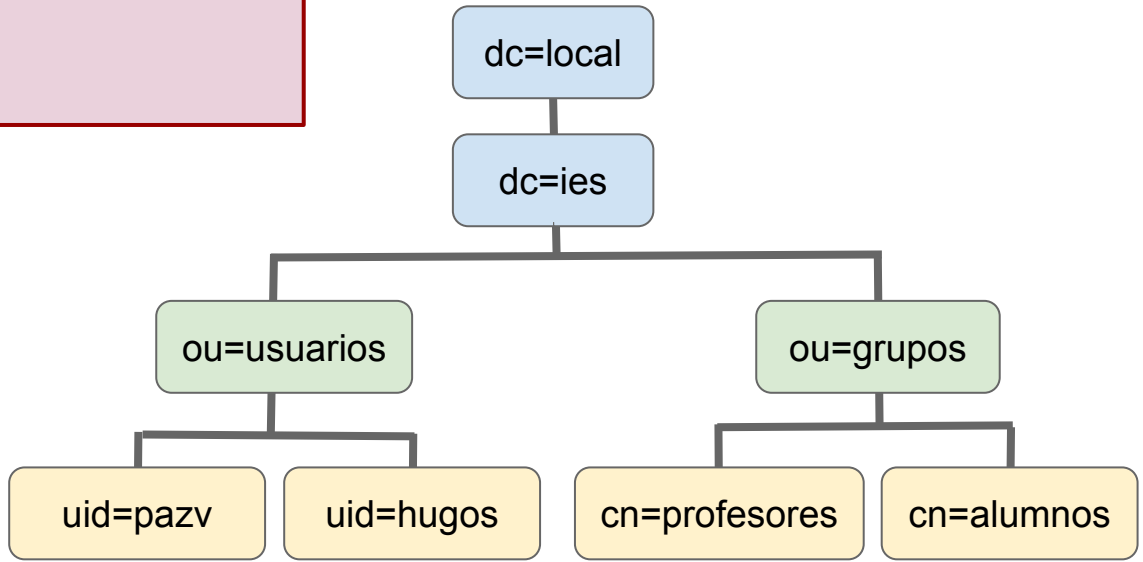
Directorio

- Un **directorio** es un árbol de entradas de datos que es de naturaleza **jerárquica** y se denomina **DIT** (Directory Information Tree).
- Puede considerarse una base de datos de objetos de distintas **clases**.
- A diferencia de una base de datos tradicional, es especialmente apta para operaciones de **lectura**, **búsqueda** y **navegación**. En lugar de serlo para operaciones de escritura.
- A la parte superior de esta estructura se le conoce como el elemento **raíz**.
- Una entrada consta de un conjunto de **atributos**.
- Un atributo tiene una clave y uno o más valores .
- Cada atributo debe estar definido en al menos una clase de objeto .
- Los atributos y las clases de objetos se definen en **esquemas**.

Ejemplo de directorio

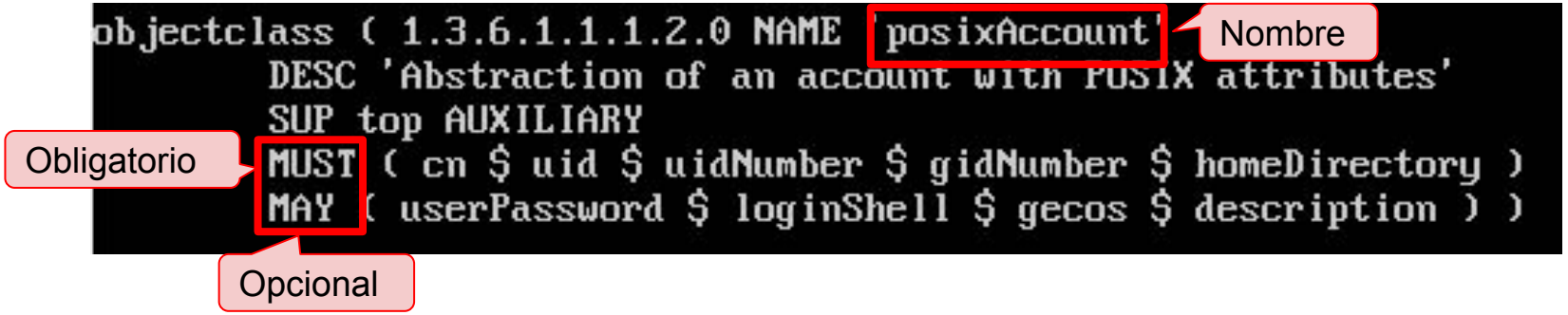
dn: uid=pazv,ou=usuarios,dc=ies,dc=local
objectClass: inetOrgPerson
uid: pazv
cn: Paz Vega
sn: Vega

dn (**nombre distinguido**):
Identificador único de cada entrada.



Esquema

- /etc/ldap/schema
- http://www.zytrax.com/books/ldap/ape/



Clase de objetos (Ejemplos)

Nombre	*MUST (Obligatorios)*	*MAY (Opcionales)*
organizationalUnit	ou	telephoneNumber, postalCode, postalAddress, description
posixGroup	gidNumber	memberUid, description
person	sn, cn	userPassword, telephoneNumber, description
inetOrgPerson [->organizationalPerson] [->person]		departmentNumber, displayName, employeeNumber, employeeType, givenName, homePhone, homePostalAddress, initials, mail, mobile, uid
posixAccount	cn, uid, uidNumber, gidNumber, homeDirectory	userPassword, loginShell, gecos, description

Utilidades OpenLDAP: Línea de comandos

- **ldapadd**: Agrega objetos en LDAP.
- **ldapmodify**: Modifica objetos en LDAP.
- **ldapdelete**: Elimina objetos en LDAP.
- **ldapsearch**: Busca objetos en LDAP.
- **ldappasswd**: Establece contraseña de un usuario en LDAP.
- **slapadd**: Acepta entradas desde un archivo LDIF.
- **slapcat**: Vuelca el contenido del directorio LDAP en un fichero LDIF.
- **slapindex**: Vuelve a indexar la base de datos de datos LDAP.
- **slappasswd**: Generar contraseñas con encriptación.

Instalación

Requisitos previos:

- El servidor tiene asignado una **IP estática**.
- El archivo **/etc/hostname** contiene el nombre correcto del servidor.
- El archivo **/etc/hosts** contienen los nombres adecuados para el servidor.
  - 192.168.1.100 u-server.ies.local u-server

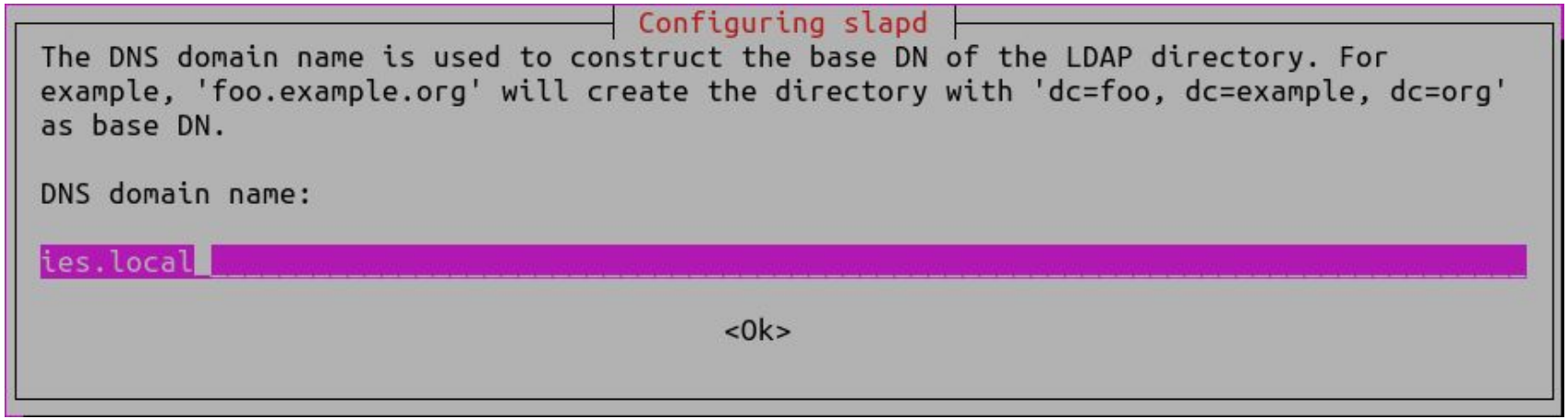
Orden de instalación:

```
$ sudo apt install slapd ldap-utils -y
```

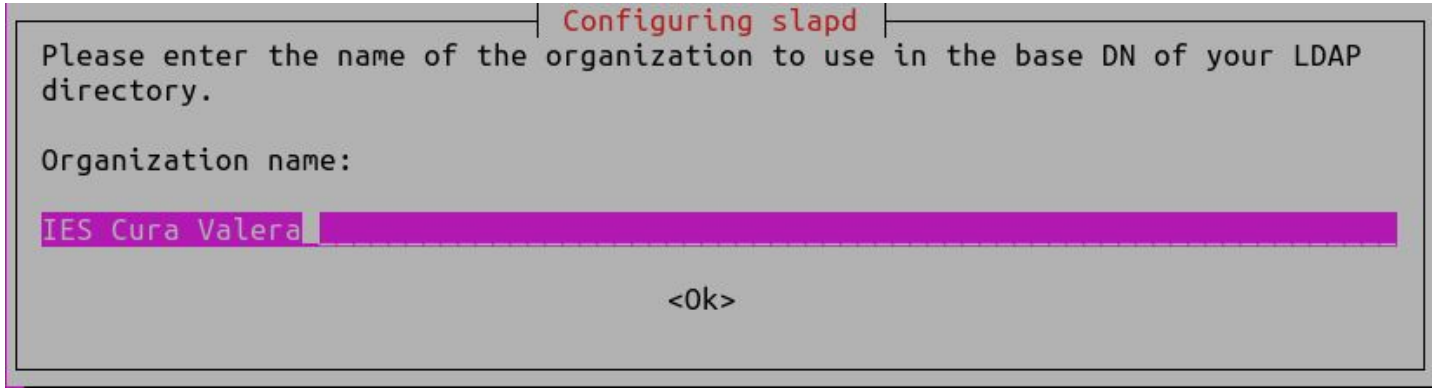
Instalación (Dominio)

Iniciamos la configuración:

$ sudo dpkg-reconfigure slapd



Configuración (nombre / admin)



Instalación (Comprobaciones)

```
$ sudo systemctl status slapd
```


```
$ sudo slapcat
```

```
$ ldapsearch -x -LLL -b dc=ies,dc=local dn
```

```
dn: dc=ies,dc=local
dn: cn=admin,dc=ies,dc=local
```

Unidades Organizativas

```
# Fichero ou.ldif

dn: ou=usuarios, dc=ies, dc=local
objectClass: organizationalUnit
ou: usuarios

# Podemos tener más de un objeto dejando una línea en blanco entre objetos.
```

-x: Autenticación simple.
-W: Introducir la contraseña.
-D: DN de usuario administrador.
-f: Fichero LDIF.

```
# ldapadd -x -W -D "cn=admin,dc=ies,dc=local" -f ou.ldif
```

Grupos

```
# Fichero grupo.ldif

dn: cn=alumnos, ou=grupos, dc=ies, dc=local
objectClass: posixGroup
cn: alumnos
gidNumber: 5002
```

```
# ldapadd -x -W -D "cn=admin,dc=ies,dc=local" -f grupo.ldif
```

Usuarios

```
# Fichero usuario.ldif
dn: uid=pazv,ou=usuarios,dc=ies,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
uid: pazv
sn: Vega
cn: Paz Vega
uidNumber: 10004
gidNumber: 5002
userPassword: miclave
loginShell: /bin/bash
homeDirectory: /home/pazv
mail: paz.vega@ies.local
```

Debe ser diferente para cada usuario

```
# ldapadd -x -W -D "cn=admin,dc=ies,dc=local" -f usuario.ldif
```

Caracteres especiales (Base64)

- El fichero LDIF debe estar codificado en formato **UTF-8**.
- Si tenemos acentos o letras como la ñ, podemos expresarlas en **Base64**
- Ejemplo: **cn: Luís -> cn:: THXDrXM=**
  - **Luís** se escribe en base64 como **THXDrXM=**
  - Para indicar que está expresado en base64 utilizamos doble punto (cn::)
- https://www.base64encode.org/

Contraseñas (SSHA)

```
marco@u-server:~/ldap$ slappasswd
New password:
Re-enter new password:
{SSHA}tH+dlwDjjmK1FByJT2KpTVGDGPwxsEuL
marco@u-server:~/ldap$
```

Ejercicio I

1) Instalar **OpenLDAP** en el servidor.
2) Crear el dominio **ies.local**
3) Crear las unidades organizativas **usuarios** y **grupos**.
4) Crear los grupos **profesores** y **alumnos** dentro de la unidad organizativa *grupos*.
5) Crear los usuarios contenidos en la tabla dentro de la unidad organizativa *usuarios*.

gidNumber	*Grupo*
5001	profesores
5002	alumnos

uidNumber	*Nombre*	*Grupo*
10001	Antonio Resines	profesores
10002	Carmen Maura	profesores
10003	Rodolfo Sancho	alumnos
10004	Paz Vega	alumnos
10005	Hugo Silva	alumnos
10006	Clara Lago	alumnos

Añadir un atributo.

```
# Fichero add_att.ldif

dn: uid=pazv,ou=usuarios,dc=ies,dc=local
changeType: modify
add: homePhone
homePhone: +34 922 541 978
```

```
# ldapmodify -x -W -D "cn=admin,dc=ies,dc=local" -f add_att.ldif
```

Modificar un atributo.

```
# Fichero mod_att.ldif

dn: uid=pazv,ou=usuarios,dc=ies,dc=local
changetype: modify
replace: mail
mail: paz@ies.local
```

```
# ldapmodify -x -W -D "cn=admin,dc=ies,dc=local" -f mod_att.ldif
```

Eliminar un atributo.

```
# Fichero mod_att.ldif

dn: uid=pazv,ou=usuarios,dc=ies,dc=local
changetype: modify
delete: mail
```

```
# ldapmodify -x -W -D "cn=admin,dc=ies,dc=local" -f mod_att.ldif
```

Borrado de un objeto

```
# ldapdelete -x -W -D "cn=admin,dc=ies,dc=local"
    "uid=marioc,ou=usuarios,dc=ies,dc=local"
```

Ejercicio II

Realiza las siguientes modificaciones en el directorio:

1) Añade el atributo "***mobile***" a los alumnos.
2) Añade el atributo "***homePhone***" a los profesores.
3) Añade el atributo "***initials***" a los profesores.
4) Modifica la shell de *Rodolfo* por **/bin/sh**.
5) Modifica el e-mail de Rodolfo por **r.sancho@ies.es**
6) Elimina el atributo "***initials***" de Carmen.

Búsquedas (Operadores)

Tipo de búsqueda	Operador	Descripción
Igualdad	**=**	Devuelve entradas que coinciden exactamente con el valor especificado. Ejemplo: ‘uid=antonior‘
Subcadena	**=*cadena***	Devuelve entradas que contengan la subcadena especificada. Ejemplos: ‘cn=Carmen*‘ ‘cn=*Maura*‘ ‘cn=C*Maura‘
Mayor o igual	**>=**	Devuelve entradas que contengan atributos cuyo valor sea mayor o igual al indicado. Ejemplo: ‘gidNumber **>=** 5001‘
Menor o igual	**<=**	Devuelve entradas que contengan atributos cuyo valor sea menor o igual al indicado. Ejemplo: ‘uidNumber **<=** 10004‘
Presencia	**=***	Devuelve entradas que contengan uno o más valores en el atributo especificado. Ejemplo: ‘cn=*‘
Aproximado	**~=**	Devuelve entradas que contengan un valor aproximado (virgulilla = **ALT Gr + 4**). Ejemplo: ‘cn~=antonio‘

Búsquedas (Operadores booleanos)

Tipo de búsqueda	Operador	Descripción
AND	**&**	La expresión será cierta cuando todos los filtros sean ciertos. Ejemplo: (&(objectClass=person)(uid=a*))
OR	**|**	La expresión será cierta cuando al menos uno de los filtros sea cierto. Ejemplo: (|(cn=*Maura*)(uid=a*))
NOT	**!**	Realiza la negación del filtro. Ejemplo: (!(uid=c*))

Los operadores se pueden combinar. Ejemplo:

(&(objectClass=person)(|(uid=paz*)(mail=*.silva@*)))

Búsquedas (Caracteres especiales)

- ➔ **\2a** reemplaza o escapa a *.
- ➔ **\28** reemplaza o escapa a **(**.
- ➔ **\29** reemplaza o escapa a **)**.
- ➔ **\5c** reemplaza o escapa a ****.
- ➔ **\00** reemplaza o escapa a **NULL**.
- ➔ **\xx** busca un valor hexadecimal (donde xx es un valor del rango 00-FF)

Ejemplos:

- (cn=*\2a) ➡ Busca el carácter * del atributo cn.
- (file=d:\5cfile.html) ➡ Busca d:\file.html
- (bin=\5b\04) ➡ Busca los valores hexadecimales 5b04

Búsquedas (Ejemplos)

Obtener los datos sólo de los usuarios:

```
# ldapsearch -xLLL -b "dc=ies,dc=local" "(objectClass=Person)"
```

Obtener el apellido de los usuarios:

```
# ldapsearch -xLLL -b "dc=ies,dc=local" "(objectClass=Person)" sn
```

Obtener el directorio home del usuario 10004:

```
# ldapsearch -xLLL -b "dc=ies,dc=local" "(uidNumber=10004)" homeDirectory
```

Consultar el e-mail de todos los usuarios:

```
# ldapsearch -xLLL -b "ou=usuarios,dc=ies,dc=local"
"(&(objectClass=Person)(mail=*))" mail
```

Ejercicio III

Realiza las siguientes búsquedas en el directorio:

1) Mostrar sólo el dn de todos los usuarios.
2) Mostrar los usuarios cuyo nombre comience por C.
3) Mostrar el nombre y los apellidos de todos los alumnos.
4) Mostrar el uid de los profesores.
5) Mostrar el nombre de los alumnos con teléfono móvil.
6) Mostrar el nombre y los apellidos del usuario con identificador de valor 10004.
7) Mostrar los alumnos con apellido acabado en A.
8) Mostrar los alumnos con apellido no acabado en O.
9) Mostrar los profesores con identificador distinto a 10001
10) Mostrar los alumnos con identificador mayor a 10005 que tengan email o móvil.