Administración de redes Linux

LDAP III

Gestión de acceso en LDAP

Iria Estévez Ayres

uc3m | Universidad Carlos III de Madrid

Departamento de Ingeniería Telemática

Abril 2025

Índice

Apartado 1

Gestión de acceso

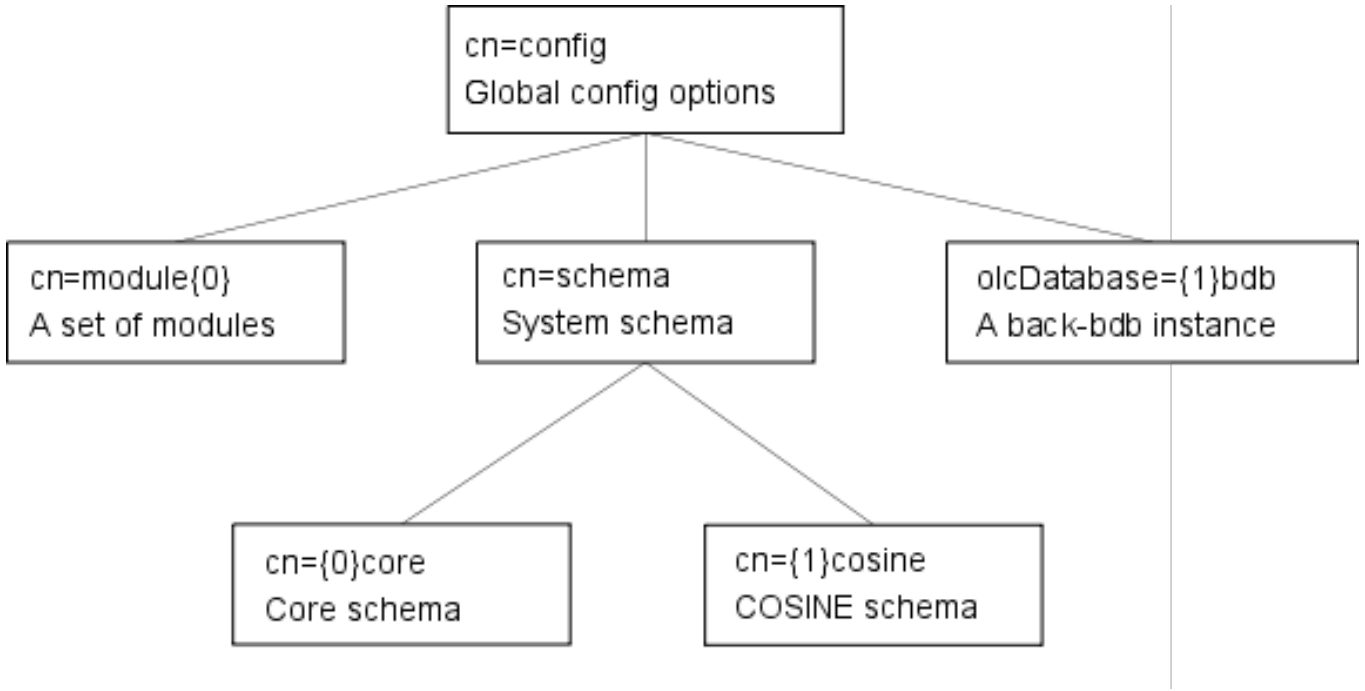
Estructura ficheros configuración

- Vamos a ir viendo la estructura de la configuración de slap.
- Organizada en el directorio `/etc/ldap/slap.d`

```
telematica@debian-mini:~$ sudo ls /etc/ldap/slapd.d/
'cn=config'  'cn=config.ldif'
telematica@debian-mini:~$ sudo ls /etc/ldap/slapd.d/'cn=config'
'cn=module{0}.ldif'  'cn=schema'  'cn=schema.ldif'  'olcBackend={0}mdb.ldif'
'olcDatabase={0}config.ldif'  'olcDatabase={-1}frontend.ldif'  'olcDatabase={1}mdb.ldif'
telematica@debian-mini:~$ sudo ls /etc/ldap/slapd.d/'cn=config'/'cn=schema'
'cn={0}core.ldif'  'cn={1}cosine.ldif'        'cn={2}nis.ldif'  'cn={3}inetorgperson.ldif'
telematica@debian-mini:~$ sudo cat /etc/ldap/slapd.d/'cn=config'/'cn=schema'/'cn={3}inetorgperson.ldif'
# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
# CRC32 cf95fbc7
dn: cn={3}inetorgperson
objectClass: olcSchemaConfig
cn: {3}inetorgperson
olcAttributeTypes: {0}( 2.16.840.1.113730.3.1.1 NAME 'carLicense' DESC 'RFC2
 798: vehicle license or registration plate' EQUALITY caseIgnoreMatch SUBSTR
  caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
olcAttributeTypes: {1}( 2.16.840.1.113730.3.1.2 NAME 'departmentNumber' DESC
  'RFC2798: identifies a department within an organization' EQUALITY caseIgn
 oreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1
 .15 )
```

Entendiendo la configuración. Estructura

```
$ sudo ldapsearch -H ldapi:/// -Y EXTERNAL -b cn=config dn
```



Entendiendo la configuración. Nodo Raíz

Raíz del árbol del directorio. Contiene configuración global.

```
$ sudo ldapsearch -H ldapi:/// -Y EXTERNAL -b cn=config cn=config
#...
# config
dn: cn=config
objectClass: olcGlobal
cn: config
olcArgsFile: /var/run/slapd/slapd.args
olcLogLevel: none
olcPidFile: /var/run/slapd/slapd.pid
olcToolThreads: 1
#....
```

- **olcArgsFile**: nombre absoluto y opciones del programa
- **olcLogLevel**: especifica el nivel de mensajes de depuración a `syslogd`. Los mensajes de más prioridad son guardados sin importar el valor de este atributo.
- **olcPidFile**: pid del proceso
- **olcToolThreads**: número máximo de hilos a usar. Por defecto 1.

Entendiendo la configuración. Módulos

Si se han habilitado cuando se configuraba `slapd`, estas entradas sirven para indicar un conjunto de módulos a cargar.

```
$ sudo ldapsearch -H ldapi:/// -Y EXTERNAL -b cn=module{0},cn=config
#...

# module{0}, config
dn: cn=module{0},cn=config
objectClass: olcModuleList
cn: module{0}
olcModulePath: /usr/lib/ldap
olcModuleLoad: {0}back_mdb

#....
```

- **objectClass: olcModuleList** tipo de objeto módulo.
- **olcModulePath**: indica el directorio donde se pueden encontrar los módulos.
- **olcModuleLoad**: nombre del módulo a cargar.
  - `back_mdb` es el módulo para cargar el backend MDB, que está basado en una biblioteca software propia de LDAP, LMDB (*Lightning Memory-Mapped Database*).

Entendiendo la configuración. Schemas

Definición de los schemas usados por la BD

```
$ sudo ldapsearch -H ldapi:/// -Y EXTERNAL -b cn=schema,cn=config
# schema, config
dn: cn=schema,cn=config
objectClass: olcSchemaConfig
cn: schema
... # Schema del sistema
# {0}core, schema, config
dn: cn={0}core,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: {0}core
... # Schema core: requisito
### Schemas adicionales del usuario
```

- **olcAttributeTypes**: tipo de atributo.
- **olcObjectClasses**: clase de objetos.

Entendiendo la configuración. Configuración del backend

Las directivas aplican a todos los backend de la misma clase.

```
$ sudo ldapsearch -H ldapi:/// -Y EXTERNAL -b olcBackEnd={0}mdb,cn=config
#...
# {0}mdb, config
dn: olcBackend={0}mdb,cn=config
objectClass: olcBackendConfig
olcBackend: {0}mdb
#...
```

- **objectClass: olcBackendConfig**
- **olcBackend**: indica el tipo de backend. Fijaos que también forma parte del dn.

Type	Description
config	Slapd configuration backend
dnssrv	DNS SRV backend
ldap	Lightweight Directory Access Protocol (Proxy) backend
ldif	Lightweight Data Interchange Format backend
mdb	Memory-Mapped DB backend
meta	Meta Directory backend
monitor	Monitor backend
passwd	Provides read-only access to passwd(5)
perl	Perl Programmable backend
shell	Shell (extern program) backend
sql	SQL Programmable backend

Entendiendo la configuración. Bases de datos

```
$ sudo ldapsearch -H ldapi:/// -Y EXTERNAL
-b olcDatabase={1}mdb,cn=config
#...
# {1}mdb, config
dn: olcDatabase={1}mdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcMdbConfig
olcDatabase: {1}mdb
olcDbDirectory: /var/lib/ldap
olcSuffix: dc=arlinux,dc=com
olcAccess: {0}to attrs=userPassword by self write by
 anonymous auth by * none
olcAccess: {1}to attrs=shadowLastChange by self write
 by * read
olcAccess: {2}to * by * read
olcLastMod: TRUE
olcRootDN: cn=admin,dc=arlinux,dc=com
olcRootPW: {SSHA}xP4WHY541f6pwHHR1yp9xQR57PfXNw/t
olcDbCheckpoint: 512 30
olcDbIndex: objectClass eq
olcDbIndex: cn,uid eq
olcDbIndex: uidNumber,gidNumber eq
olcDbIndex: member,memberUid eq
olcDbMaxSize: 1073741824

#...
```

- **olcDatabase: [[indice]]tipo**
- **olcDbDirectory**: directorio donde está la BD.
- **olcSuffix**: el sufijo de DN que será pasado a esta BD.
- **olcAccess**: a qué se da permisos y a quién.
- **olcRootDN**: qué DN no está sujeto al control administrativo que se indica en esta base de datos.
- **olcRootPW**: password de ese DN (si está en la BD).
- **olcDbMaxSize**: tamaño máximo en bytes.

Listas de control de acceso (ACLs)

```
# The userPassword by default can be changed
        # by the entry owning it if they are authenticated.
        # Others should not be able to see it, except the
        # admin entry below
        access to attrs=userPassword
                by dn.regex="cn=admin,dc=lab,dc=it,dc=uc3m,dc=es" write
                        by anonymous auth
                        by self write
                        by * none
        # The admin dn has full write access
        access to *
                by dn="cn=admin,dc=lab,dc=it,dc=uc3m,dc=es" write
                        by * read
        # For Netscape Roaming support, each user gets a roaming
        # profile for which they have write access to
        access to dn.regex=".*,ou=Roaming,o=morsnet"
                by dn="cn=admin,dc=lab,dc=it,dc=uc3m,dc=es" write
                        by dnattr=owner write
```

Como se puede observar el patrón que se sigue es:

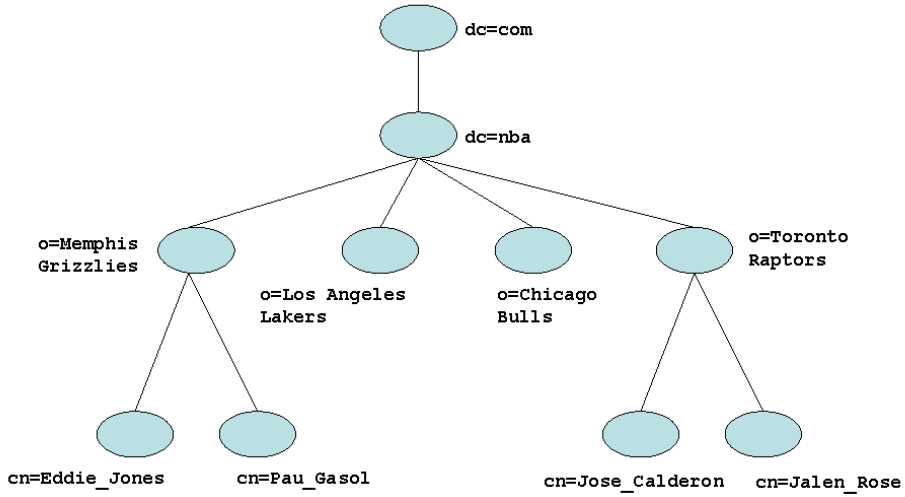
1. Indicar a qué recurso se da acceso (**access to** ...)
2. Indicar quién(es) tiene(n) acceso a ese recurso (**by dn=...** write)
3. Indicar qué clase de acceso (lectura, escritura) se tiene (by dn=... **write**)

Consultad documentación OpenLDAP (apartado 8)
`https://www.openldap.org/doc/admin24/access-control.html`

¿Cómo indicar a qué recurso se da acceso? (I)

1. Si se da acceso a todo `access to *`
2. Un recurso o conjunto de recursos (usando expresiones regulares)
   `dn[.<basic-style>] = regex`
   - `basic-style` puede ser `regex` para indicar que se especifica una expresión regular que puede englobar a un conjunto de recursos, o
   - `basic-style` puede ser `exact`, un recurso concreto.
   - Si no se especifica `basic-style`, por defecto es `regex`
3. Indicar un subárbol a partir de un DN de un elemento. Según el valor de `scope-style`:
   - `dn.base = ...`: se refiere sólo al nodo con el DN dado.
   - `dn.one = ...`: todas las entradas cuyo padre sea el DN proporcionado.
   - `dn.subtree = ...`: todas las entradas en el subárbol cuya raíz es el DN proporcionado.
   - `dn.children = ...`: todas las entradas debajo del DN (exceptuando la entrada nombrada por el DN).

¿Cómo indicar a qué recurso se da acceso? (II)



- `dn.base="dc=nba,dc=com"` hace referencia únicamente al nodo con DN `dc=nba,dc=com`
- `dn.one="dc=nba,dc=com"` hace referencia a todos los nodos que están justo un nivel por debajo del nodo indicado, es decir, `o=Memphis Grizzlies,dc=nba,dc=com`; `o=Los Angeles Lakers,dc=nba,dc=com`; o=`Chicago Bulls,dc=nba,dc=com` y `o=Toronto Raptors,dc=nba,dc=com`.
- `dn.subtree="dc=nba,dc=com"` hace referencia al propio nodo y a todos los que hay por debajo de él, independientemente del nivel en que se encuentren. En el caso de la figura, estará haciendo referencia a todos los nodos excepto a `dc=com`.
- `dn.children="dc=nba,dc=com"` es semejante al caso anterior, sólo que esta vez no incluye el propio nodo. Esta expresión estará haciendo referencia a todos los nodos del árbol excepto `dc=com` y `dc=nba,dc=com`

¿Cómo indicar a qué recurso se da acceso? (III)

Ejemplo. Nodos en LDAP

```
0: o=suffix
1: cn=Manager,o=suffix
2: ou=people,o=suffix
3: uid=kdz,ou=people,o=suffix
4: cn=addresses,uid=kdz,ou=people,o=suffix
5: uid=hyc,ou=people,o=suffix
```

Ejemplo. Expresiones

Expresión	A qué da acceso
`dn.base="ou=people,o=suffix"`	2
`dn.one="ou=people,o=suffix"`	3, 5
`dn.subtree="ou=people,o=suffix"`	2, 3, 4 y 5
`dn.children="ou=people,o=suffix"`	3, 4 y 5

Adicionalmente:

1. Se pueden seleccionar entradas usar un filtro `to filter=<ldap filter>`.
   - `to filter=(objectClass=person)` seleccionaría todas las entradas que pertenezcan a la clase `person`.
2. Se pueden seleccionar entradas seleccionando por DN y, además, filtrando.
   - `to dn.one="ou=people,o=suffix" filter=(objectClass=person)` del subconjunto 3 y 5, seleccionaría las que pertenezcan a la clase `person`.

¿Cómo indicar a qué recurso se da acceso? (y IV)

- Para un **mismo nodo**, se pueden definir **distintas políticas de acceso** a sus distintos atributos → Uso de `attrs`
- A continuación de `attrs` aparece una lista de atributos separados por comas o bien una expresión regular.

Ejemplo. No permitimos acceso a su password

```
access to attrs=userPassword
by dn.regex="cn=admin,dc=lab,dc=it,dc=uc3m,dc=es" write
by anonymous auth
by self write
by * none
```

¿Cómo indicar a quién se concede el acceso?

Se especifica el usuario o usuarios después de **by**

Especificador	Entidades
*	Todos los usuarios
anonymous	Usuarios anónimos (sin autenticar)
users	Usuarios autenticados
self	Usuario asociado a la entrada sobre la que se aplica la directiva
dn[.<basic-style>]=<regex>	Usuarios que encajan con la expresión regular que se indique
dn.<scope-style>=<DN>	Usuarios bajo el ámbito de un DN concreto

Ejemplo

```
by dn.regex="cn=admin,dc=lab,dc=it,dc=uc3m,dc=es" write
by anonymous auth
by self write
by * none
```

¿Cómo indicar qué operaciones pueden efectuar sobre los recursos?

Nivel	Privilegios	Descripción
none	=0	sin acceso
auth	=x	necesario para acceder al sistema
compare	=cx	necesario para comparar
search	=scx	necesario para efectuar búsquedas
read	=rscx	necesario para leer
write	=wrscx	necesario para escribir o modificar

- El orden de declaración de permisos es relevante.
  - Cuando se va a hacer una operación que necesite consultar los permisos, el servidor busca en el conjunto de directivas de acceso la primera que encaje con el recurso solicitado y con el usuario que requiere el permiso, y ésa es la que aplica, independientemente de que haya más adelante en el fichero de configuración otra directiva que también encaje y que sea más restrictiva o más flexible.

Ejercicio en clase (I)

Fichero charles.ldif

```
dn: uid=charles,ou=gente,dc=arlinux,dc=com
changetype: add
objectClass: inetOrgPerson
uid: charles
mail: charles@arlinux.com
mobile: 222222
givenName: Charles
sn: Babbage
cn: Charles
```

Vuelve a añadir a Charles Babbage (añadiéndole el número de móvil y cambiando el tipo de clase de objeto).

```
$ sudo ldapmodify -x -D "cn=admin,dc=arlinux,dc=com" -W -H ldapi:/// -f charles.ldif
```

Ejercicio en clase (II)

Comprueba el valor de `olcAccess`

```
$ sudo ldapsearch -H ldapi:/// -Y EXTERNAL -b olcDatabase={1}mdb,cn=config
#...
olcAccess: {0}to attrs=userPassword by self write by anonymous auth by * none
olcAccess: {1}to attrs=shadowLastChange by self write by * read
olcAccess: {2}to * by * read
#...
```

Comprueba que siendo Ada puedes consultar el registro entero de Charles

```
$ ldapsearch -x -D "uid=ada,ou=gente,dc=arlinux,dc=com" -W
-b uid=charles,ou=gente,dc=arlinux,dc=com
#...
# charles, gente, arlinux.com
dn: uid=charles,ou=gente,dc=arlinux,dc=com
objectClass: inetOrgPerson
uid: charles
mail: charles@arlinux.com
mobile: 222222
givenName: Charles
sn: Babbage
cn: Charles
#...
```

Ejercicio en clase (III)

Queremos hacer que el móvil sea privado.

Fichero cambiopermisos.ldif

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcAccess
olcAccess: to attrs=mobile by self write by anonymous auth by * none
```

```
$ sudo ldapmodify -Y EXTERNAL -W -H ldapi:/// -f cambiopermisos.ldif
```

```
$ ldapsearch -x -h localhost -D "uid=ada,ou=gente,dc=arlinux,dc=com" -W
-b uid=charles,ou=gente,dc=arlinux,dc=com
#...
# charles, gente, arlinux.com
dn: uid=charles,ou=gente,dc=arlinux,dc=com
objectClass: inetOrgPerson
uid: charles
mail: charles@arlinux.com
mobile: 222222
givenName: Charles
sn: Babbage
cn: Charles
#...
```

¡¡ Aún puedo ver su móvil !!

Ejercicio en clase (IV)

Comprobamos la configuración

```
$ sudo ldapsearch -H ldapi:/// -Y EXTERNAL -b olcDatabase={1}mdb,cn=config
#...
olcAccess: {0}to attrs=userPassword by self write by anonymous auth by * none
olcAccess: {1}to attrs=shadowLastChange by self write by * read
olcAccess: {2}to * by * read
olcAccess: {3}to attrs=mobile by self write by anonymous auth by * none
#...
```

¡El orden importa!

Ejercicio en clase (IV)

Hay que reemplazar los permisos...

Fichero cambiopermisos2.ldif

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcAccess
olcAccess: to attrs=userPassword by self write by anonymous auth by * none
-
add: olcAccess
olcAccess: to attrs=shadowLastChange by self write by * read
-
add: olcAccess
olcAccess: to attrs=mobile by self write by anonymous auth by * none
-
add: olcAccess
olcAccess: to * by * read
```

```
$ sudo ldapmodify -Y EXTERNAL -W -H ldapi:/// -f cambiopermisos2.ldif
$ sudo ldapsearch -H ldapi:/// -Y EXTERNAL -b olcDatabase={1}mdb,cn=config
#...
olcAccess: {0}to attrs=userPassword by self write by anonymous auth by * none
olcAccess: {1}to attrs=shadowLastChange by self write by * read
olcAccess: {2}to attrs=mobile by self write by anonymous auth by * none
olcAccess: {3}to * by * read
#....
```

Ejercicio en clase (y V)

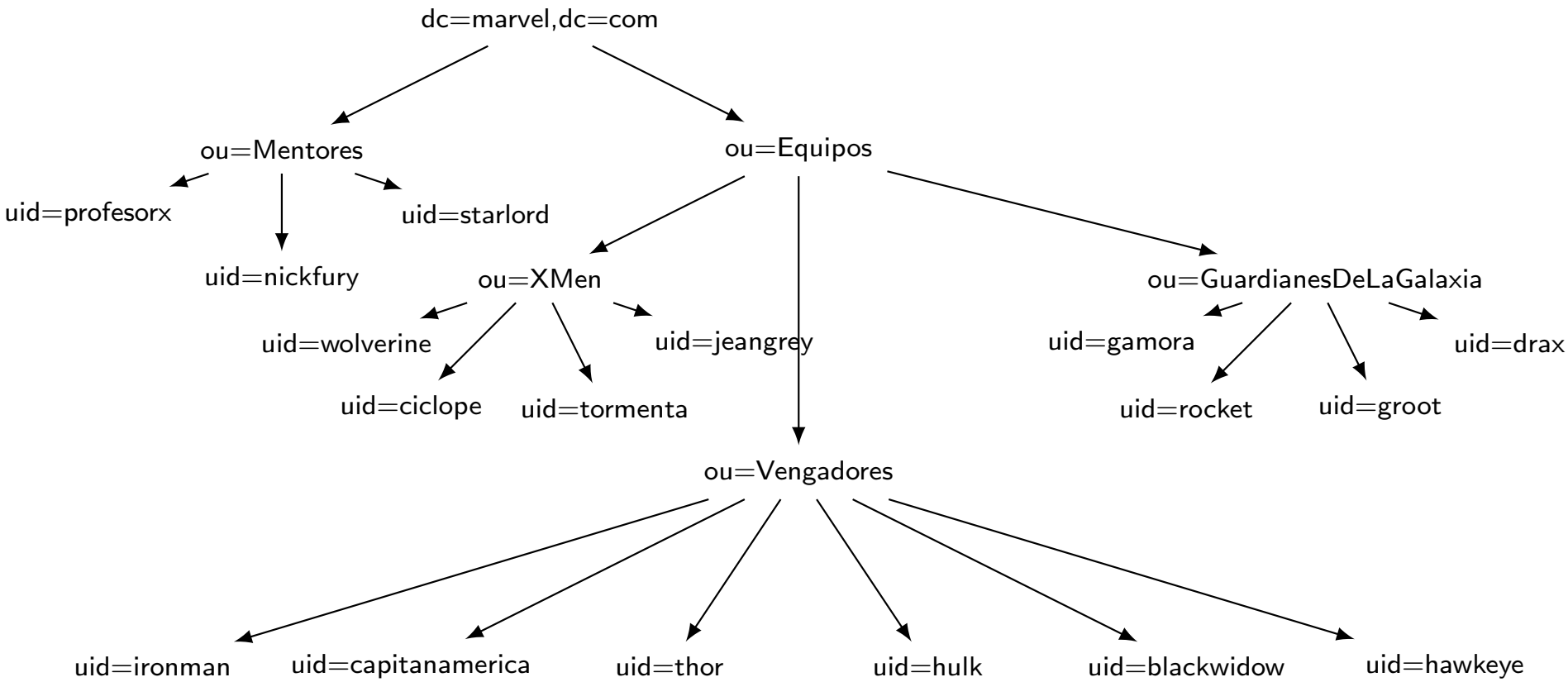
Compruebo otra vez como Ada

```
$ ldapsearch -x -h localhost -D "uid=ada,ou=gente,dc=arlinux,dc=com" -W
-b uid=charles,ou=gente,dc=arlinux,dc=com
#...
# charles, gente, arlinux.com
dn: uid=charles,ou=gente,dc=arlinux,dc=com
objectClass: inetOrgPerson
uid: charles
mail: charles@arlinux.com
givenName: Charles
sn: Babbage
cn: Charles
#...
```

Ejercicio entregable

1. Usando un único fichero LDIF crea el árbol que se muestra a continuación, que debe colgar del nodo dc=marvel,dc=com. Debes entregar el fichero LDIF (puede estar embebido en la memoria que entregues) y una explicación del mismo:
   - Cada entrada relativa a una persona deberá ser, al menos, de la clase inetOrgPerson
   - Todos las personas deberán tener al menos un mail y un número de teléfono.
   - Los héroes deberán tener, además, un mentor, además de un número de habitación asignada, un rol dentro del equipo (title) y su nombre real o completo.
   - Los mentores deberán tener, además, un número de identificación de empleado.

Árbol LDAP del ejercicio entregable



Ejercicio entregable

2. Crea las directivas de acceso necesarias para que se puedan aplicar las siguiente reglas (deberás entregar el LDIF resultante y una explicación del mismo):
   - El administrador tiene acceso de escritura a todo.
   - El atributo userPassword es usado para autenticarse en el sistema. Sólo puede ser modificado por el propio usuario o por el administrador. Nadie debe poder leerlo (excepto el usuario y el administrador).
   - Cada usuario puede leer sus propios datos pero sólo puede modificar el userPassword.
   - Al tener poderes mentales, a excepción de su userPassword, profesorx puede modificar el resto de los atributos de todos los héroes, incluidos el resto de mentores.
   - Nick Fury puede modificar el atributo número de habitación de todos los Vengadores.
   - Star Lord puede modificar el atributo title de todos los Guardianes de la Galaxia.
   - Todos los mentores pueden leer todos los datos del resto de mentores y de los héroes.
   - Los héroes pueden leer el mail de los mentores, pero no su número de teléfono ni su número de identificación de empleado.
   - Los héroes pueden leer pueden leer el mail y número de teléfono del resto de los héroes.
   - Los héroes pueden leer el atributo donde se guarda el nombre real del resto de héroes de su equipo y de su mentor.

Ejercicio entregable

3. Comprueba que todo ha ido bien mediante consultas con ldapsearch. En la memoria añade pantallazos de las distintas consultas para comprobar que todo es correcto. Explica el por qué de cada consulta.
4. Mejoras al árbol LDAP (30 % de la nota del entregable):
   - Después de realizar el primer apartado, modifica el árbol añadiendo más información como descripciones, lugar de trabajo o más entradas al árbol. Explica adecuadamente las modificaciones realizadas y entrega en la memoria los ficheros ldif usados (con pantallazos de los comandos usados).
   - Una vez terminado el segundo apartado, añade más reglas explicándolas adecuadamente. Muestra también en la memoria los ficheros ldif usados y, si es necesario, pantallazos.
   - Haz comprobaciones de tus mejoras adicionales.

Administración de redes Linux

LDAP III

Gestión de acceso en LDAP

Iria Estévez Ayres

uc3m | Universidad Carlos III de Madrid

Departamento de Ingeniería Telemática

Abril 2025