

LDAP

LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL

Servicios de directorio

Base de datos que se puede consultar telemáticamente con información sobre diversas entidades

Para cada entidad se almacenan diversos atributos de interés (de acuerdo a un esquema)

Las entidades suelen organizarse jerárquicamente

La información suele ser bastante estática

Puede usarse con fines técnicos, administrativos, de negocio, informativos...

Muchos sistemas operativos y aplicaciones distribuidas tienen su servicio de “directorio”, con diferentes posibilidades

En una organización suele haber múltiples directorios, con diferentes fines, información parcial, redundante e incluso incoherente u obsoleta

LDAP es un estándar derivado de OSI X.500 que suelen implementar esos directorios. A veces se complementa con extensiones propietarias

Directorios: consideraciones de diseño

Organización del árbol y nomenclatura

Tipos de objetos y sus atributos

Métodos de acceso a la información

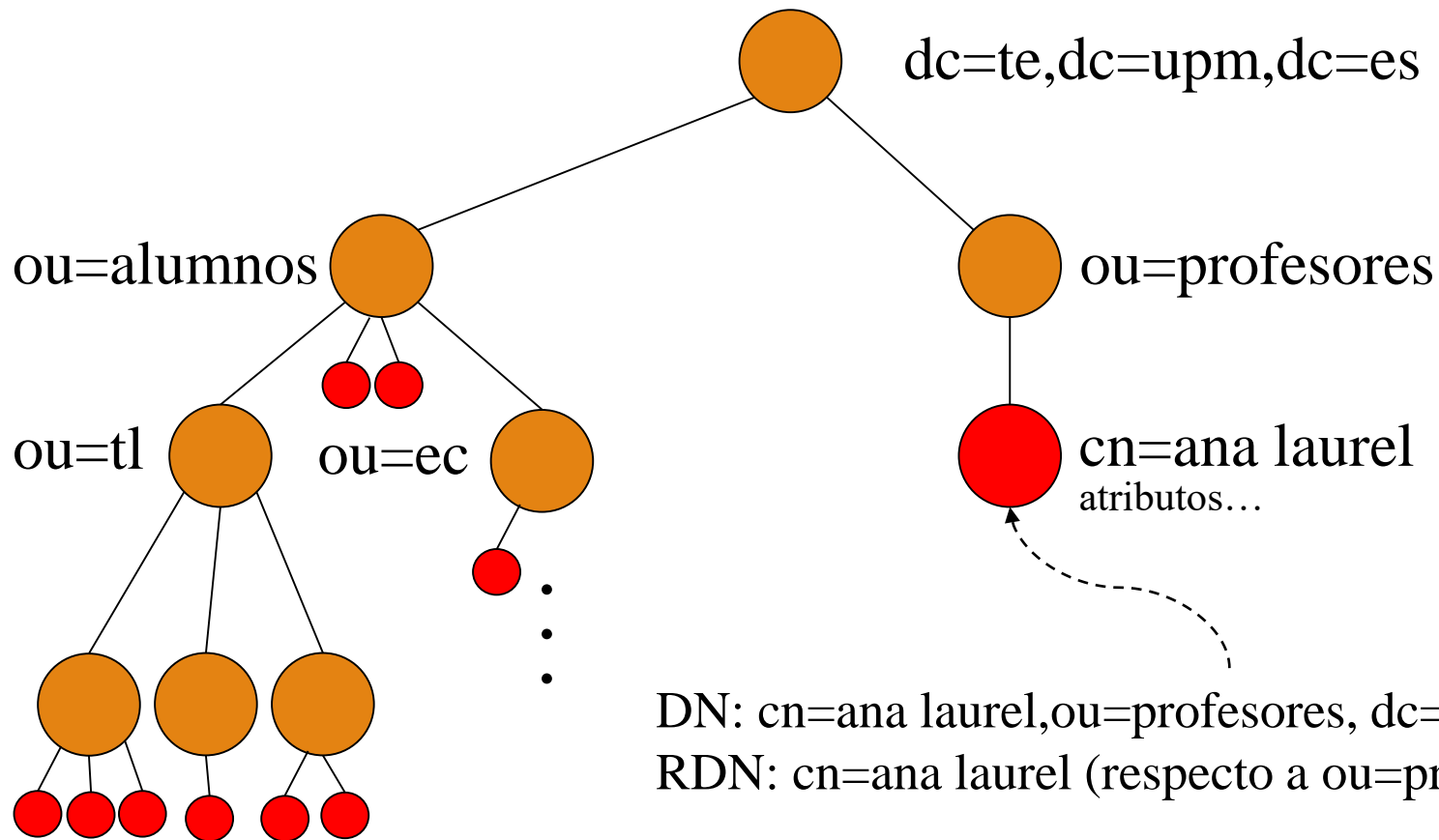
Seguridad

Distribución y replicación

Gestión de la información

LDAP: [RFC 4510](#), [ldapwiki.com](#)

Ejemplo de árbol LDAP



DN: `cn=ana laurel,ou=profesores, dc=te,dc=upm,dc=es`
RDN: `cn=ana laurel` (respecto a `ou=profesores`)

¿Qué pasa si un alumno cambia de titulación?

Esquema ([RFC 4512](#))

Clases de objetos

- [OID, Private Enterprise Numbers](#)
- Tipo: estructural, auxiliar, abstracta
- Herencia
- Atributos obligatorios
- Atributos opcionales

Atributos

- OID
- Nombres
- Sintaxis
- Reglas de comparación
- Multiplicidad de valores

Ejemplo de esquema

```
objectclass ( 2.5.6.6 NAME 'person'
  DESC 'RFC2256: a person'
  SUP top STRUCTURAL
  MUST ( sn $ cn )
  MAY ( telephoneNumber $ seeAlso $ description ) )

objectclass ( 2.5.6.7 NAME 'organizationalPerson'
  DESC 'RFC2256: an organizational person'
  SUP person STRUCTURAL
  MAY ( title $ x121Address $ registeredAddress $ destinationIndicator $
    preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
    telephoneNumber $ internationaliSDNNumber $
    facsimileTelephoneNumber $ street $ postOfficeBox $ postalCode $
    postalAddress $ physicalDeliveryOfficeName $ ou $ st $ l ) )

objectclass ( 1.3.6.1.1.1.2.0 NAME 'posixAccount'
  DESC 'Abstraction of an account with POSIX attributes'
  SUP top AUXILIARY
  MUST ( cn $ uid $ uidNumber $ gidNumber $ homeDirectory )
  MAY ( userPassword $ loginShell $ gecos $ description ) )
```

Ejemplo de esquema

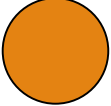
```
attributetype ( 2.5.4.3 NAME ( 'cn' 'commonName' )  
  DESC 'RFC2256: common name(s) for which the entity is known by'  
  SUP name )
```

```
olcAttributeTypes: ( 2.5.4.41 NAME 'name'  
  EQUALITY caseIgnoreMatch  
  SUBSTR caseIgnoreSubstringsMatch  
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )
```

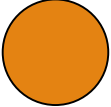
```
attributetype ( 2.5.4.20 NAME 'telephoneNumber'  
  DESC 'RFC2256: Telephone Number'  
  EQUALITY telephoneNumberMatch  
  SUBSTR telephoneNumberSubstringsMatch  
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.50{32} )
```

```
attributetype ( 2.5.4.28 NAME 'preferredDeliveryMethod'  
  DESC 'RFC2256: preferred delivery method'  
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.14  
  SINGLE-VALUE )
```

Objetos contenedores

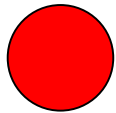


DN: dc=te,dc=upm,dc=es
(objectClass: dcObject)
dc: te



DN: ou=profesores,dc=te,dc=upm,dc=es
(objectClass: organizationalUnit)
ou: profesores
description: Profesores del DTE
...

Objetos de usuario



DN: cn=ana laurel,ou=profesores,dc=te,dc=upm,dc=es
(objectClass: inetOrgPerson, posixAccount)

cn: ana laurel

givenName: Ana

sn:: TGF1cmVslEdhcmPDrWE=

uid: alaurel

uidNumber: 1008

gidNumber: 3000

homeDirectory: /home/alaurel

userPassword: kshs73hdh

loginShell: /bin/csh

...

Otras clases de objetos: posixGroup, shadowAccount, nisMap,
nisObject, nisNetgroup...

Consultar [RFC 2307](#)

Seguridad ([RFC 4513](#))

Modos de acceso cifrado

- En claro (TCP/389)
- Cifrado StartTLS (TCP/389), con certificados X.509
- Cifrado SSL (TCP/636), con certificados X.509

Estados de autenticación

- Anónimo
- Autenticado, tras operación Bind/SASL

Autorización de operaciones (modelo de ACL)

- Qué: ramas, objetos, atributos...
- Quién: anónimo, usuarios, conjuntos...
- Acceso: ninguno, búsqueda, lectura, modificación, control...

Distribución y replicación

Los servidores pueden contener referencias a otros servidores (superiores o subordinados) para partes distribuidas del árbol de directorio

Navegación de referencias

- Por parte del cliente
- Por parte del servidor (encadenamiento)

Replicación

- Maestro-esclavo
- Multimaestro

Compartición de usuarios mediante LDAP

Base de datos de usuarios y grupos

- Accesible mediante LDAP
- Esquema adecuado para gestionar usuarios y grupos
- Almacenamiento puede ser independiente de LDAP

Integración transparente con sistemas POSIX

- PAM (autenticación)
- NSS (consulta)

Integración con otros sistemas y aplicaciones

OpenLDAP: principales componentes

Servidor: slapd, slurp

Configuración: /usr/local/etc/openldap

Esquema: /usr/local/etc/openldap/schema

Base de datos: /var/db/openldap-data

Utilidades de servidor: slapadd, slapcat, slapindex...

Herramientas de cliente: ldapadd, ldapsearch, ldapmodify, ldapdelete...

OpenLDAP: configuración básica

```
include core.schema
include cosine.schema
include nis.schema
include inetorgperson.schema
moduleload back_mdb
database mdb
suffix "dc=ejemplo,dc=es"
rootdn "cn=Manager,dc=ejemplo,dc=es"
rootpw "{SSHA}kdajadkdaljdasl"
directory /var/db/openldap-data
index objectClass eq
index uid eq
index uidNumber eq
```

OpenLDAP: control de acceso

```
access to dn.base="" by * read
access to dn.base="cn=Subschema" by * read
```

```
access to attrs=userPassword
  by self =xw
  by anonymous auth
  by * none
```

```
access to attrs=homeDirectory,uidNumber,gidNumber
  by users read
```

```
access to dn.subtree="dc=ejemplo,dc=es"
  by self write
  by users read
  by anonymous auth
```

Añadir objetos

ldapadd

-x

Usar autenticación simple

-f datos.ldif

Fichero de datos

-D 'cn=Manager,dc=ejemplo,dc=es'

-W

Usuario para autenticación

Pedir contraseña

Añadir objetos

```
ldapadd -x -f datos.ldif  
-D 'cn=Manager,dc=ejemplo,dc=es' -W
```

```
dn: uid=asanchez,ou=usuarios,dc=ejemplo,dc=es  
objectClass: posixAccount  
objectClass: inetOrgPerson  
cn: Ana  
sn: Sánchez  
uid: asanchez  
uidNumber: 1234  
gidNumber: 5678  
homeDirectory: /home/asanchez  
mail: asanchez@ejemplo.es  
...
```

Modificar objetos

```
ldapmodify -x -f datos.ldif  
-D 'cn=Manager,dc=ejemplo,dc=es' -W
```

```
dn: uid=pepe,ou=usuarios,dc=ejemplo,dc=es  
changetype: modify  
replace: mail  
mail: pepe@upm.es  
-  
delete: description
```

Borrar objetos

```
ldapdelete -x  
-D 'cn=Manager,dc=ejemplo,dc=es' -W  
'DN' ...
```



Objetos que hay que borrar

Buscar objetos

`ldapsearch -x`

`-D 'cn=Manager,dc=ejemplo,dc=es' -W`

`-L`  Formato de la respuesta

`-b 'dc=ejemplo,dc=es'`

`'FILTRO'`  Punto de partida

`atributos`

 Filtro

 Atributos deseados

Filtros de búsqueda

Ejemplos de filtros ([RFC 4515](#)):

- (uid=pepe)
- (cn:caseExactMatch:=Juan)
- (description=*sistemas*)
- (!(uidNumber=100))
- (&(mail=*@ejemplo.es)(objectClass=posixAccount))

Cambiar contraseña

```
ldappasswd -x
```

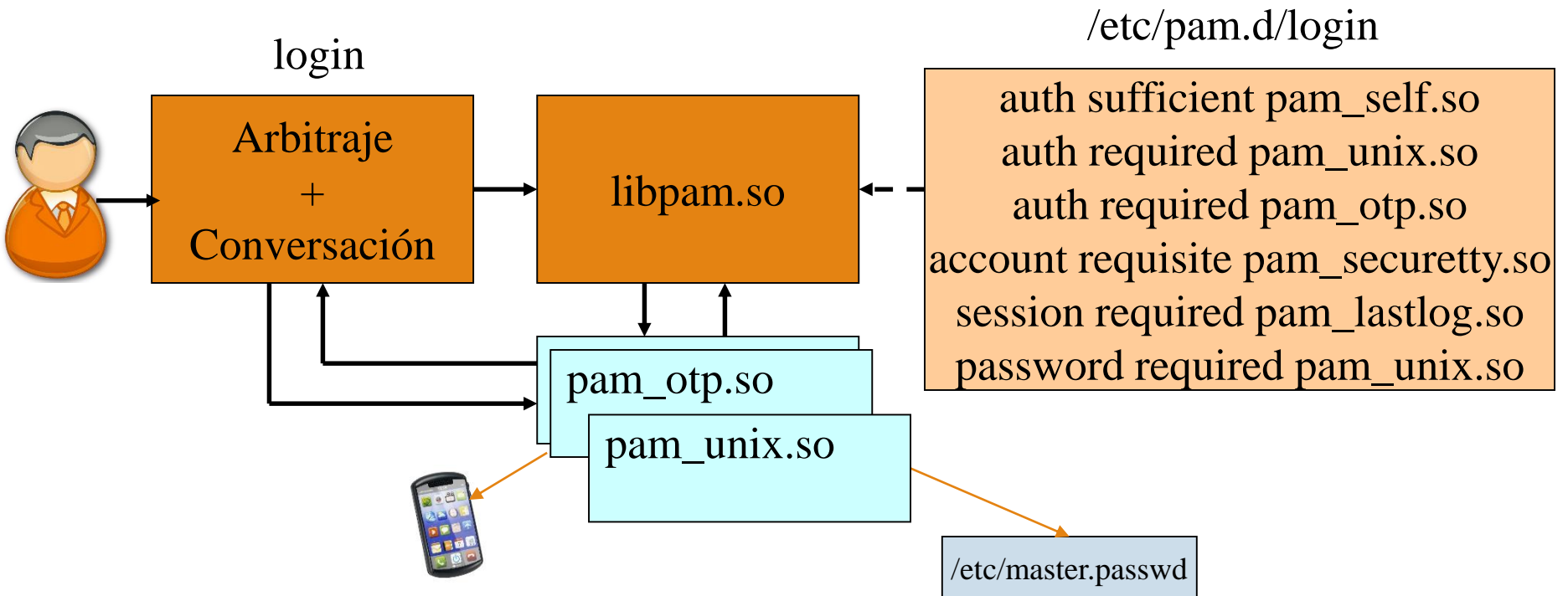
```
-D 'cn=Manager,dc=ejemplo,dc=es' -W
```

```
-S 'uid=pepe,ou=usuarios,dc=ejemplo,dc=es'
```

Pedir nueva contraseña

Objeto cuya contraseña se
quiere cambiar

PAM (Pluggable Auth. Modules)



PAM (Pluggable Auth. Modules)

Tipos de módulos

- auth
- account
- session
- password

Respuestas

- PAM_SUCCESS
- PAM_IGNORE
- Fallo (autenticación inválida...)

Acciones de control

	PAM_SUCCESS	Fallo
required		fallo = true
requisite		fallo = true ; return
sufficient	if (! fallo) return	
binding	if (! fallo) return	fallo = true
optional		

PAM (Pluggable Auth. Modules)

Más información:

- `/etc/pam.d/README`
- [Guía de FreeBSD](#)

Ejemplo de configuración PAM

/etc/pam.d/login

```
auth    sufficient    pam_self.so    no_warn
auth    sufficient    pam_opie.so    no_warn no_fake_prompts
auth    requisite     pam_opieaccess.so    no_warn allow_local
auth    required      pam_unix.so    no_warn try_first_pass
```

```
account requisite     pam_securetty.so
account required      pam_nologin.so
account required      pam_login_access.so
account required      pam_unix.so
```

```
session required      pam_lastlog.so    no_fail
```

```
password required      pam_unix.so    no_warn try_first_pass
```

Usuarios en LDAP (I)

Antes:

```
/etc/pam.d/xxx:
```

```
auth    required    pam_nologin.so  no_warn
auth    sufficient   pam_self.so    no_warn
auth    sufficient   pam_opie.so    no_warn no_fake_prompts
auth    requisite    pam_opieaccess.so  no_warn allow_local
auth    required     pam_unix.so    no_warn try_first_pass
```

```
/etc/nsswitch.conf:
```

```
passwd: compat
```

```
group: compat
```

Usuarios en LDAP (I)

Después:

/etc/pam.d/xxx:

auth	required	pam_nologin.so	no_warn
auth	sufficient	pam_self.so	no_warn
auth	sufficient	pam_opie.so	no_warn no_fake_prompts
auth	requisite	pam_opieaccess.so	no_warn allow_local
auth	sufficient	pam_unix.so	no_warn try_first_pass
auth	required	pam_ldap.so	use_first_pass

/etc/nsswitch.conf:

passwd: **files ldap**

group: **files ldap**

Usuarios en LDAP (II)

/usr/local/etc/ldap.conf:

```
host ldap.ejemplo.es  
base dc=ejemplo,dc=es  
binddn uid=servicio,dc=ejemplo,dc=es  
bindpw clave
```

```
# Opcional para casos especiales  
pam_login_attribute uid  
pam_filter FILTRO  
nss_map_attribute ATRIB1 ATRIB2  
pam_password TIPO
```