Tema 4
Servicios de directorio

LDAP (Lightweight Directory Access Protocol)

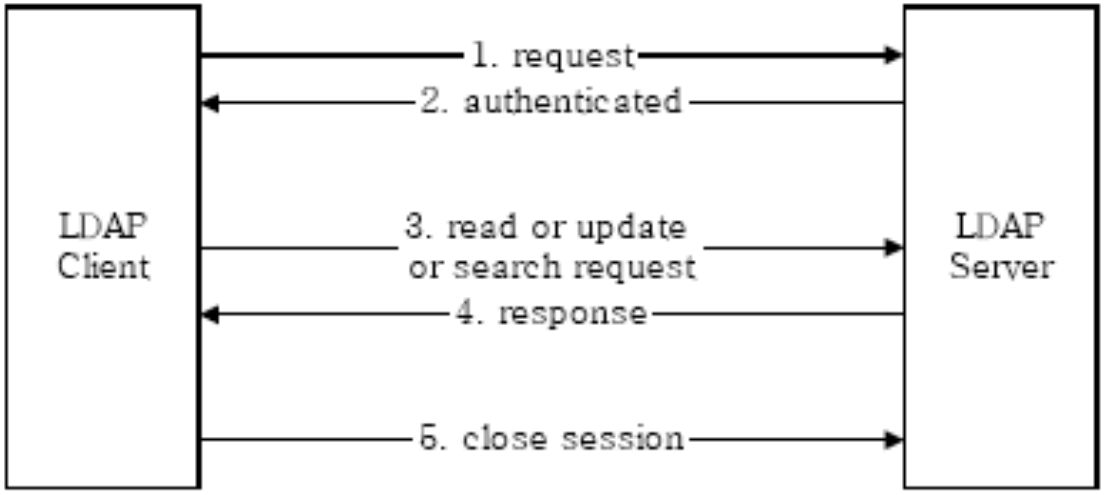
- LDAP se diseñó en la Universidad de Michigan como alternativa *ligera* a DAP, empleando la pila TCP/IP(Puerto 389) (RFC 2251).
- LDAP es un estándar abierto, incorporado en muchos productos software, como Microsoft Active Directory o clientes de correo.
- Método estándar de acceso y actualización de la información del directorio
  - Es un protocolo de comunicaciones.

Video

- https://www.youtube.com/watch?v=F2nFtlS8uEo

Interacción básica LDAP

- La interacción entre un cliente y un servidor LDAP sigue estos pasos:
  - El cliente establece una sesión con el servidor (*binding*).
  - El cliente solicita la ejecución de operaciones de lectura, actualización y búsqueda.
  - El cliente cierra la sesión con el servidor (*unbinding*).

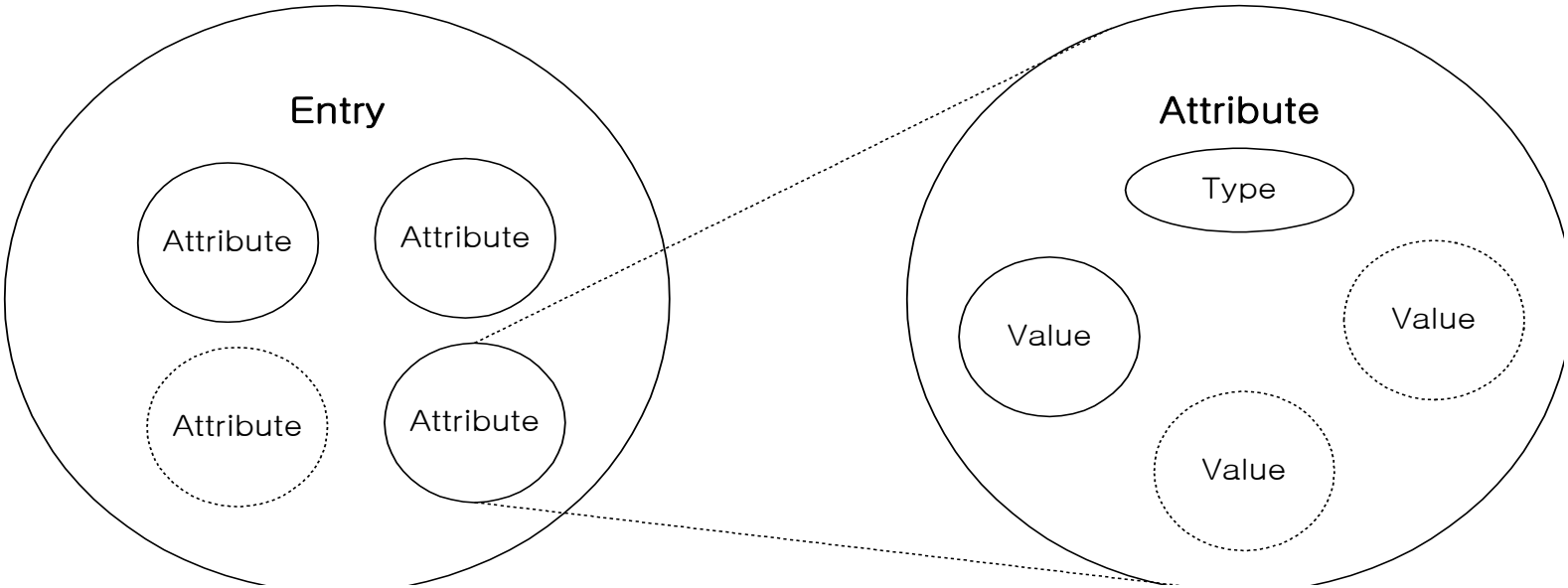


Modelos de LDAP

- Modelo de información. Describe la estructura de la información almacenada en un directorio LDAP.
- Modelo de nombres. Describe el espacio de nombres de LDAP, es decir, cómo se organiza e identifica la información.
- Modelo funcional. Describe qué operaciones se pueden ejecutar sobre la información de un directorio LDAP.
- Modelo de seguridad. Describe cómo se protege la información de accesos no autorizados.

Modelo de información (1)

- Entradas
  - Almacena y organiza estructuras de datos
  - Un objeto, como una persona o un servidor



Modelo de información (2)

- Cada atributo de una entrada tiene un tipo que establece la sintaxis de sus valores. Algunas de las sintaxis definidas en LDAP son las siguientes:

Sintaxis	Descripción
bin	Información binaria
ces	Secuencia de caracteres con mayúsculas y minúsculas significativas en las comparaciones
cis	Secuencia de caracteres sin distinguir mayúsculas y minúsculas en las comparaciones
tel	Número de teléfono
dn	Distinguished name
Generalized Time	Año, mes, día y tiempo representado en una cadena de caracteres
Postal Address	Dirección postal con líneas separadas por "$"

Modelo de información (3)

- Atributos comunes en las entradas

Atributo, alias	Sintaxis	Ejemplo
CountryName,c	cis	Spain
LocalityName,l	cis	Murcia
OrganizationName,o	cis	Universidad de Murcia
OrganizationalUnitName,ou	cis	Facultad de Informática
CommonName,cn	cis	Eduardo Martínez
SureName,sn	cis	Martínez
TelephoneNumber	tel	968-36-4666
JpegPhoto	bin	mi foto

  - CommonName se emplea para identificar una entrada dentro de cierto contexto del directorio.
- El conjunto de entradas del directorio se denomina Directory Information Base (DIB).

Modelo de información (4)

- Al igual que las tablas de una base de datos relacional, mediante esquemas se define el tipo de entradas que pueden ser almacenadas en un directorio.
- Por cada tipo de entrada se especifican los atributos que contiene, y cuáles son opcionales. Al crear o modificar entradas se puede comprobar si verifica el esquema.
- También se puede definir la herencia de entradas, y dónde pueden aparecer en el árbol jerárquico de nombres.
  - El atributo objectClass indica el tipo de entrada

Modelo de información (5)

- Tipos de entrada definidos en RFC 2252 y RFC 2256

Tipo	Superior	Atributos Requeridos	Atributos Opcionales
top		objectClass	
alias	top	aliasedObjectName	
person	top	cn, sn	description, seeAlso, telephoneNumber, userPassword
organizational-Person	person		l, ou, postalAddress, postalCode, st, street, title,...
inetOrgPerson	organizational-Person		jpegPhoto, mail, uid, o, userCertificate,...

  - objectClass toma el valor top o alias. Es multievaluado y también toma el valor del tipo de entrada.

Modelo de nombres (1)

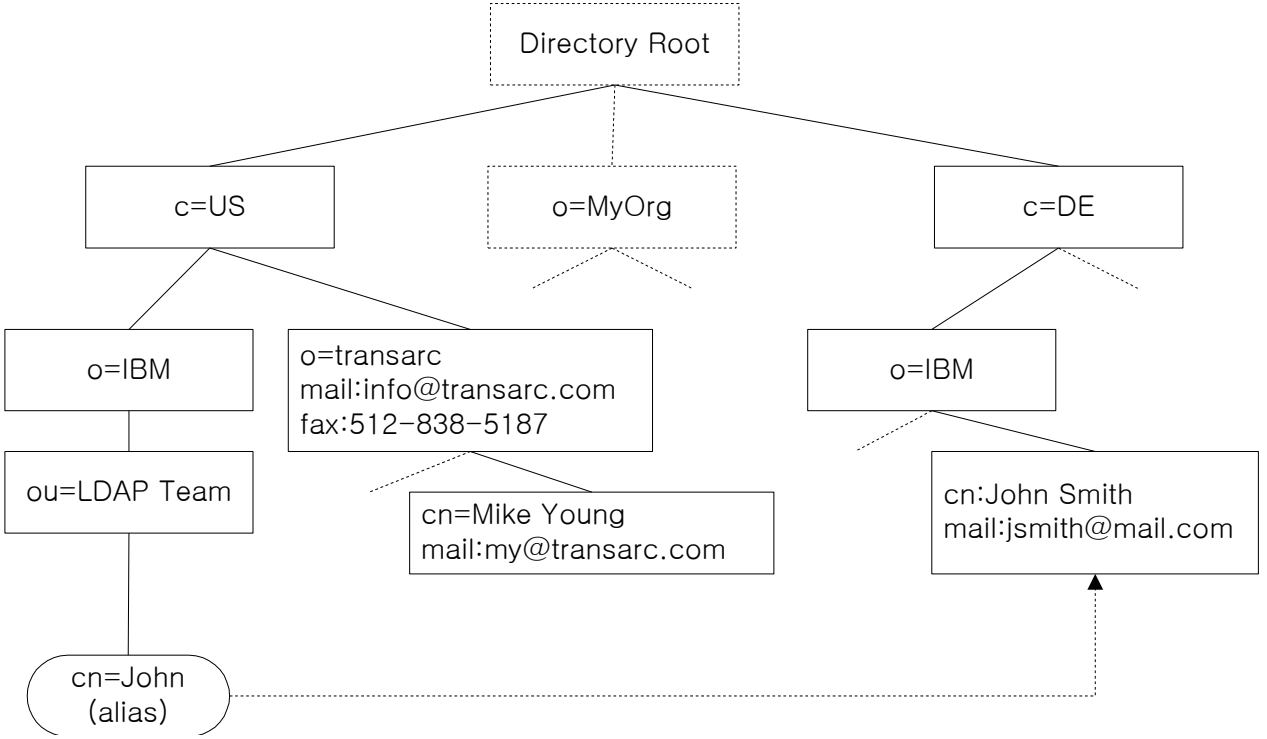
- Directory Information Tree (DIT). Estructura tipo árbol que organiza las entradas del directorio.
- Distingished name (DN). Nombre de una entrada, que corresponde con el nombre del camino inverso desde la entrada al nodo raíz del DIT. Está formado por una secuencia de RDN separados por comas.
- Relative distingished name (RDN). Nombre de una arista del DIT. Se deriva de los atributos de la entrada de la que parte, en el camino inverso hacia la raíz. Habitualmente tiene la forma *atributo=valor*.

Modelo de nombres (2)

- El nodo raíz del directorio es conceptual, es decir, realmente no existe.
- Lo normal es que la organización de las entradas siga un esquema geográfico u organizacional:
  - Los nodos hijo del raíz son entradas que representan países.
  - Bajo estas se encuentran organizaciones nacionales, estados, provincias.
  - En el siguiente nivel hay entradas que representan más subdivisiones en la organización (departamentos) o personas.
  - El último nivel representa personas, servidores, impresoras, etc.
- El DN de una entrada se especifica al construirse.
- El DIT no es estrictamente un árbol, ya que puede haber alias.

Modelo de nombres (3)

- Ejemplo de DIT



cn=John,ou=LDAP Team,o=IBM,c=US
cn=John Smith,o=IBM,c=DE

Modelo funcional (1)

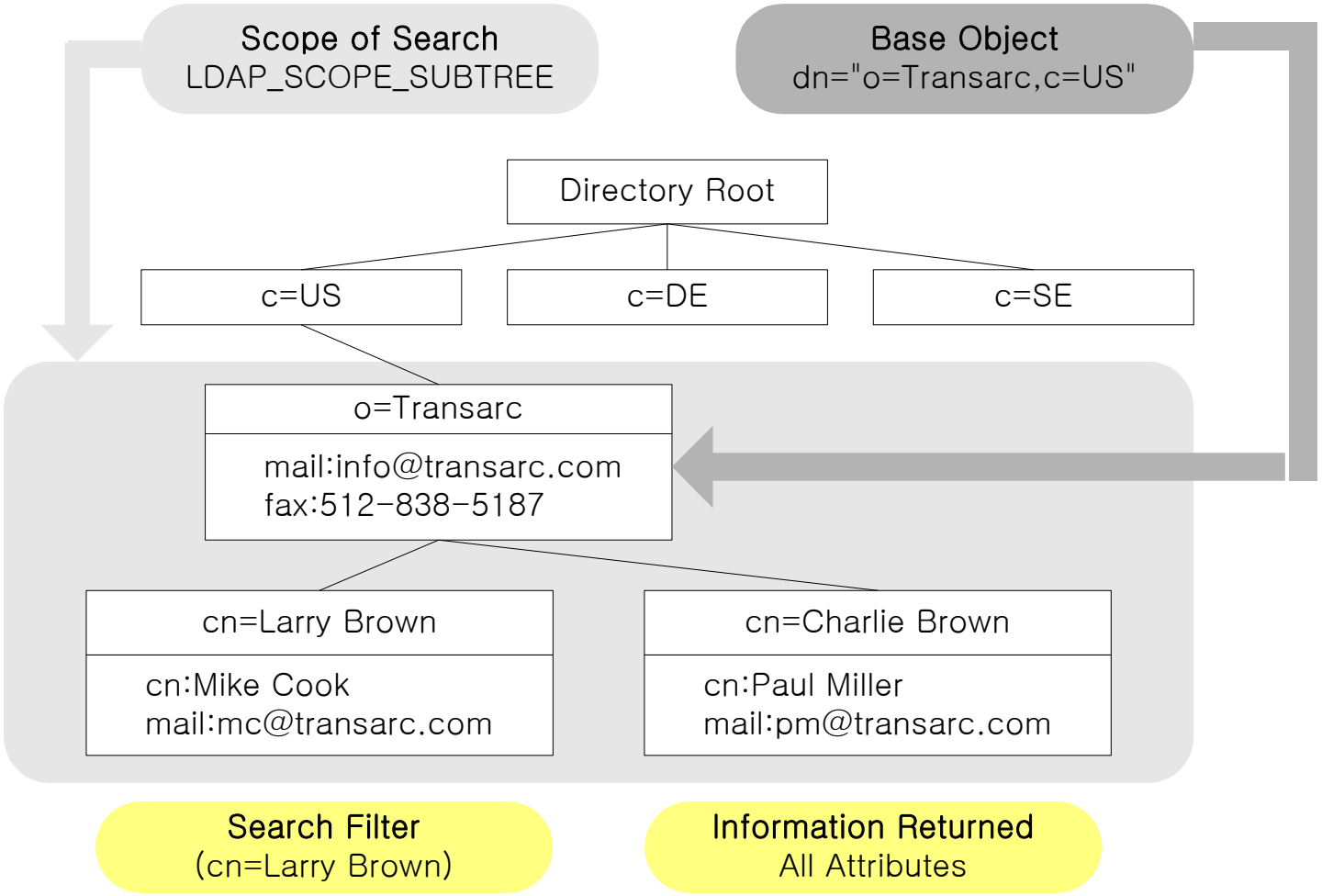
- Las operaciones que se pueden realizar sobre un servidor LDAP se pueden dividir en tres categorías:
  - Consultas: incluyen las operaciones *search* y *compare* para recuperar información del directorio.
  - Actualización: incluyen operaciones para modificar la información almacenada en el directorio, como *add*, *delete* y *modify*.
  - Autenticación: son las operaciones *bind*, *unbind* y *abandon*, para conectarse y desconectarse a un servidor LDAP.

Modelo funcional (2)

- La operación de lectura/búsqueda tiene los siguientes parámetros:
  - *Base*: DN de la entrada en la que se inicia la búsqueda.
  - *Alcance*: hasta qué nivel de profundidad se realizará la búsqueda:
    - *Entrada base*: sólo la entrada Base.
    - *Un nivel*: sólo los hijos inmediatos de la entrada Base.
    - *Subárbol*: la entrada Base y todos sus descendientes.
  - *Filtro de búsqueda*: criterio que debe cumplir una entrada para que se devuelva en el resultado.
  - *Atributos devueltos*: lista de atributos devueltos de las entradas que cumplen el filtro de búsqueda.
  - *Des-referencia de alias*: especifica si los alias se des-referencian en la búsqueda.
  - *Límites*: límite temporal y de tamaño del resultado.

Modelo funcional (3)

- Operación de consulta



Esquemas LDAP

- Los esquemas del directorio contienen la definición de los tipos de entradas y atributos que se pueden crear.
  - Se emplea el lenguaje ASN.1 (ITU-T Abstract Syntax Notation-1 (X.691)).
- Por ejemplo, la implementación OpenLDAP proporciona varios esquemas de uso frecuente:
  - *core.schema*: definiciones más frecuentes, encontradas en varios RFC (2252,2256)
  - *inetorgperson.schema*: definición de inetOrgPerson (RFC 2798)
  - *java.schema*: definiciones de entradas para almacenar referencias a objetos Java (RFC 2713)
- Se pueden añadir nuevos esquemas para almacenar información de carácter específico.

Entradas LDAP (1)

- Tipos de entradas LDAP
  - Un *objectclass:*
    - define un tipo de entrada LDAP.
    - puede ser parte de una jerarquía de herencia.
    - tiene un identificador de objeto (OID).
    - define sus atributos miembro, que se pueden agrupar en dos conjuntos:
      - MUST: atributos obligatorios del objectclass
      - MAY: atributos opcionales del objectclass
  - Todos los *objectclass* soportados por un servidor LDAP forman una colección conocida como *subschema*.

Entradas LDAP (2)

- Definición formal de *objectclass* (RFC 2252)

```
ObjectClassDescription = "(" whsp numericoid whsp
[ "NAME" qdescrs ]
[ "DESC" qdstring ]
[ "OBSOLETE" whsp ]
[ "SUP" oids ]
[ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ]
[ "MUST" oids ]
[ "MAY" oids ]
whsp ")"
```

  - *whsp* significa espacio en blanco.
  - *numericoid* es un OID en formato numérico.
  - *qdescrs* es uno o más nombres.
  - *oids* es uno o más nombres u OIDs.

Entradas LDAP (3)

- Ejemplo de objectclass: *country*

```
objectclass ( 2.5.6.2 NAME 'country' SUP top STRUCTURAL
    DESC '2 character iso assigned country code'
    MUST c
    MAY ( searchGuide $ description ) )
```

  - 2.5.6.2 NAME 'country' identifica este objectclass:
    - 2.5.6.2 es el identificador único de este objectclass.
    - country es un nombre human-friendly del objectclass.
  - SUP top indica que la clase superior a esta es top. Un objectclass puede tener una o más clases superiores.

Entradas LDAP (4)

- *STRUCTURAL*: indica que el objectclass es de tipo estructural. Teniendo en cuenta que una entrada del DIT puede tener varios objectclass, el tipo de un objectclass puede ser:
  - STRUCTURAL: se puede crear una entrada en el DIT con este objectclass únicamente.
  - AUXILIARY: no se puede crear una entrada en el DIT con este objectclass sólo.
  - ABSTRACT: no se puede crear una entrada en el DIT con este objectclass. Se emplea como clase abstracta en la jerarquía de objectclass (ejemplo: top).
- *DESC 'descripción'*: descripción textual del objectclass, pensada para lectores, no para tratamiento en programas.
- *MUST c*: el atributo c es obligatorio en este tipo de objeto.
- *MAY searchGuide & description*: atributos opcionales.

Atributos LDAP (1)

- Un attribute define un tipo de atributo que se puede emplear en uno o más objectclass.
- Un attribute puede ser parte de una jerarquía de herencia:
  - *commonName* (cn) o *surename* (sn) heredan de name.
- Cada attribute tiene un OID.
- Una definición de un atributo incluye:
  - Su sintaxis (string, number, etc).
  - Cómo realizar distintos tipos de comparaciones.

Atributos LDAP (2)

- Definición formal de *attribute* (RFC 2252)

```
AttributeTypeDescription = "(" whsp numericoid whsp
[ "NAME" qdescrs ]
[ "DESC" qdstring ]
[ "OBSOLETE" whsp ]
[ "SUP" woid ]
[ "EQUALITY" woid
[ "ORDERING" woid
[ "SUBSTR" woid ]
[ "SYNTAX" whsp noidlen whsp ]
[ "SINGLE-VALUE" whsp ]
whsp ")"
```

  - *noidlen* es un OID que, al final, puede indicar opcionalmente una longitud máxima entre {}.

Atributos LDAP (3)

- Ejemplo de attribute: *name* y *commonName*

```
attributeType ( 2.5.4.4.1 NAME 'name'
    DESC 'name(s) associated with the object'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 {32768} )

attributeType ( 2.5.4.3 NAME ( 'cn' 'commonName' )
    DESC 'common name(s) associated with the object'
    SUP name )
```

  - Por defecto, un atributo es multi-valuado. Si sólo puede aparecer una vez, debe indicarse explícitamente con SINGLE-VALUE.

LDAP: ejemplo de despliegue

- LDAP para "autenticación"
  - No posee información pública, solo accesible por servicios con derecho
  - Clientes solicitan acceso a un servicio y proporcionan sus credenciales
  - Servicio solicita autenticación del usuario al propio LDAP
    - Solicitud Bind para autenticar al propio servicio frente al LDAP
      - Se recuperan los atributos del usuario que indican si puede o no acceder al servicio
    - Solicitud Bind para autenticar al usuario
      - Se pasan credenciales (login/pwd) al LDAP
        - Si el LDAP almacena las contraseñas protegidas, el servicio debe enviarlas en claro: se comparan los resúmenes digitales de la contraseña
  - DN: uid=alicia, ou=usuarios, dc=um, dc=es

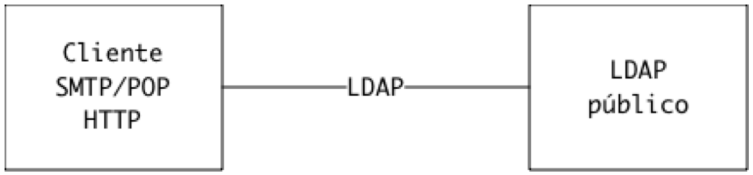
LDAP: ejemplo de despliegue

- LDAP para "autenticación" (cont.)
  - Ejemplo de entrada:

```
dn: uid=alicia,ou=Usuarios,dc=um,dc=es
objectClass: irisPerson
objectClass: irisInetEntityStr
objectClass: posixAccount
objectClass: shadowAccount
objectClass: CourierMailAccount
objectClass: labeledURIObject
objectClass: sambaSamAccount
uid: alicia
uidNumber: 14332
gidNumber: 403
mail: alicia@um.es
cn: ALICIA
irisPersonalUniqueID 14658960 (DNI)
homeDirectory: /home/pdi/72/916272
mailbox: /home/pdi/92/110372/Maildir/
userPassword:: e[redacted]9
shadowLastChange: 15071
sambaLMPassword: 9[redacted]EF
sambaNTPassword: 5[redacted]CB
sambaPwdLastSet: 1302173612
irisUserEntitlement: urn:mace:rediris.es:um.es:entitlement:correo
irisUserEntitlement: urn:mace:rediris.es:um.es:entitlement:socrates
irisUserEntitlement: urn:mace:rediris.es:um.es:entitlement:cuenta
irisUserEntitlement: urn:mace:rediris.es:um.es:entitlement:eduroam
irisUserEntitlement: urn:mace:rediris.es:um.es:entitlement:vpn
```

LDAP: ejemplo de despliegue

- LDAP para "páginas blancas"
  - Contienen información pública. Accesible mediante navegadores, pasarelas webs o clientes de correo electrónico
  - Clientes solicitan datos directamente al LDAP
    - No proporcionan credenciales
  - DN: uid=alicia, ou=usuarios, dc=um, dc=es




```
dn: uid=alicia,dc=usuarios,dc=um,dc=es
objectClass: top
objectClass: irisInetEntity
objectClass: irisPerson
objectClass: organizationalUnit
objectClass: uidObject
objectClass: pilotObject
objectClass: pkiUser
objectClass: umPerson
mail: alicia@um.es
irisUserPrivateAttribute: jpegphoto
uid: alicia
cn: ALICIA
givenName: ALICIA
sn1: MARTÍNEZ MARTÍNEZ
irisPersonalUniqueID: 23322449
gender: V
telephoneNumber: +34 8684438504
irisMailAlternateAddress: alicica@um.es
postalAddress: _Facultad de Informatica $ Campus de Espinardo
description: _INGENIERIA TELEMATICA
street: _FACULTAD DE INFORMATICA $ Campus Universitario de Espinardo $ 30100
businessCategory: PROFESOR TITULAR DE UNIVERSIDAD
```

Bibliografía

- A.S. Tanenbaum (1998) *Computer Networks*. Prentice-Hall
- J. Kurose, K. Ross (2001) *Computer Networking. A top down approach featuring the Internet*. Addison Wesley