



Biblioteca Virtual FP

Plan FP 2015

Unidad 10

Servicios de directorio. LDAP

IFC08CM15. Despliegue de aplicaciones web
Curso 2015

Índice

- ▶ Servicios de directorio.
 - Introducción.
 - X.500.
 - Características.
- ▶ LDAP
 - Introducción.
 - Versiones.
 - Características.
 - Backend.
 - Aplicaciones prácticas.

Índice

- Modelo de datos.
 - DIT
 - ▶ Entidades (*entry*)
 - ▶ *objectClasses*.
 - ▶ Atributos.
 - ▶ Esquemas (*schemas*).
- ▶ Modelo de nombrado.
- ▶ Modelo de funcionamiento (operaciones).
- ▶ LDIF.
- ▶ Usos.

Índice

- ▶ Software.
- ▶ Autenticación/Autorización LDAP
 - *Apache.*
 - *Tomcat.*
- ▶ Bibliografía.

Servicios de directorio

Introducción

► Una definición

- Sistema software que ofrece servicios de gestión y acceso a un conjunto de información (directorío).
- Búsqueda de información basada en nombres.

Servicios de directorio

Introducción

- ▶ Termino “ambiguo”, según la definición
 - La sistemas de ficheros “son servicios de directorio”.
 - La bases de datos “son servicios de directorio”.
 - DNS en un servicio de directorio.
 - ...

- ▶ Se suele utilizar el termino “servicio de directorio” para referirse a los servicios basados en los estándares X.500.

Servicios de directorio

X.500

- ▶ Conjunto de estándares sobre servicios de directorio definidos por la ITU (<http://www.itu.int/es/>).
- ▶ Creado en 1988.
- ▶ Adoptado por la ISO en 1990
- ▶ Describe cómo organizar las entradas de forma jerárquica, de forma que el directorio sea fácilmente escalable y se simplifique la tarea de búsqueda.

Servicios de directorio

X.500

► Define

◦ Protocolos

- DAP (*Directory Access Protocol*)
- DSP (*Directory System Protocol*)
- DISP (*Directory Information Shadowing Protocol*)
- DOP (*Directory Operational Bindings Management Protocol*)

◦ Modelos de datos.

Servicios de directorio

Características

- ▶ Arquitectura cliente/servidor.
- ▶ Organización jerárquica e los datos.
- ▶ Estructura flexible.
- ▶ Muchas lecturas y pocas escrituras -> Optimizados para consultas.
- ▶ No transaccional (no hay *roolback*).
- ▶ Alto rendimiento (miles de accesos por segundo).
- ▶ Distribuidos.

Servicios de directorio

Características

► Webs

- http://es.wikipedia.org/wiki/Servicio_de_directorio
- http://en.wikipedia.org/wiki/Directory_service
- <http://es.wikipedia.org/wiki/X.500>
- <http://en.wikipedia.org/wiki/X.500>

LDAP

Introducción

► X.500

- Protocolo DAP para acceder a los servicio de directorio a través de una red.
- DAP se basaba en la pila de protocolos OSI.
- Apenas había implementaciones de esa pila de protocolos, por lo que DAP no tuvo mucha aceptación.

LDAP

Introducción

- ▶ **LDAP (Lightweight Directory Access Protocol)**
 - Estándar abierto para acceder y manipular un servicio de directorio distribuido.
 - Creado en 1993 en la Universidad de Michigan.
 - Definido por la ITU con el objetivo de ofrecer la misma funcionalidad que DAP pero sobre la pila de protocolos TCP/IP.
 - Ventajas:
 - Funciona sobre la pila TCP/IP.
 - Simplifica DAP, eliminando opciones raramente utilizadas.

LDAP

Introducción

- ▶ LDAP era compatible con servicios de directorio basados en el estándar X.500, pero dado su éxito, pronto surgieron servicios de directorio LDAP independientes.
- ▶ La terminología X500 y LDAP es similar.

LDAP

Versiones

- ▶ **LDAPv2.**

- Obsoleto

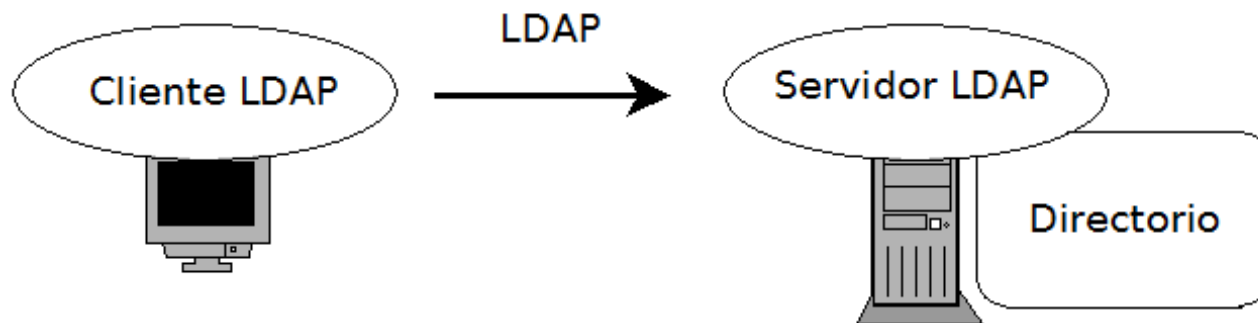
- ▶ **LDAPv3.**

- Remplaza a LDAP v2.
- Más rápido.
- Más opciones de autenticación.
- Esquemas.
- SSL/TLS y Certificados digitales X.509.

LDAP

Características

- ▶ Técnicamente LDAP, como su nombre indica, es solo un protocolo que define como **acceder** a un directorio de datos.
 - El servidor tiene por tanto libertad para implementar el directorio



LDAP

Características

- ▶ Necesariamente, también define y describe
 - Como los datos son **representados** en el directorio.
 - Como los datos son **cargados (importados) y exportados** en/del directorio (LDIF).
- ▶ LDAP **NO define** como los datos son **almacenados y manipulados**.
 - ¿Quién se encarga entonces de esas labores?
 - Las implementaciones del servicio de directorio LDAP (servidores LDAP)
 - Algunos ejemplos:
 - Directorio Activo de Microsoft.
 - OpenLDAP.

LDAP

Características

► Define 4 modelos

- **Modelo de información (modelo de datos)**
 - Define la estructura de la información almacenada en el directorio.
- **Modelo de nombrado**
 - Como se nombra y se identifica a la información almacenada en el directorio.
- **Modelo funcional**
 - Operaciones sobre la información: búsquedas, lecturas, escrituras y modificaciones.
 - Describe las operaciones pero no la forma de imprimir las.
- **Modelo de seguridad**
 - Control de acceso.
 - Quién y qué puede hacer en el directorio.

LDAP

Backend

- ▶ Las implementaciones del servicio de directorio (servidores LDAP) utilizan un motor de bases de datos como *backend* para almacenar los datos.
- ▶ Existen algunas diferencias respecto a otras BD:
 - El concepto de directorio se aproxima más al de índice que al de depósito de información.
 - Un directorio puede tener que soportar miles de consultas de lectura por segundo, al ser un recurso utilizado por muchas aplicaciones.
 - En cambio, recibe muy pocas peticiones de escritura.
 - No necesita soporte de transacciones:
 - Se aceptan inconsistencias temporales.
 - La replicación es más sencilla.

LDAP

Aplicaciones prácticas

- ▶ Es una herramienta cada vez más valorada por los administradores.
- ▶ Un uso habitual es la autenticación centralizada, que permite a un usuario utilizar una misma cuenta (y por tanto una misma contraseña) para autenticarse en diferentes máquinas o *servicios*.

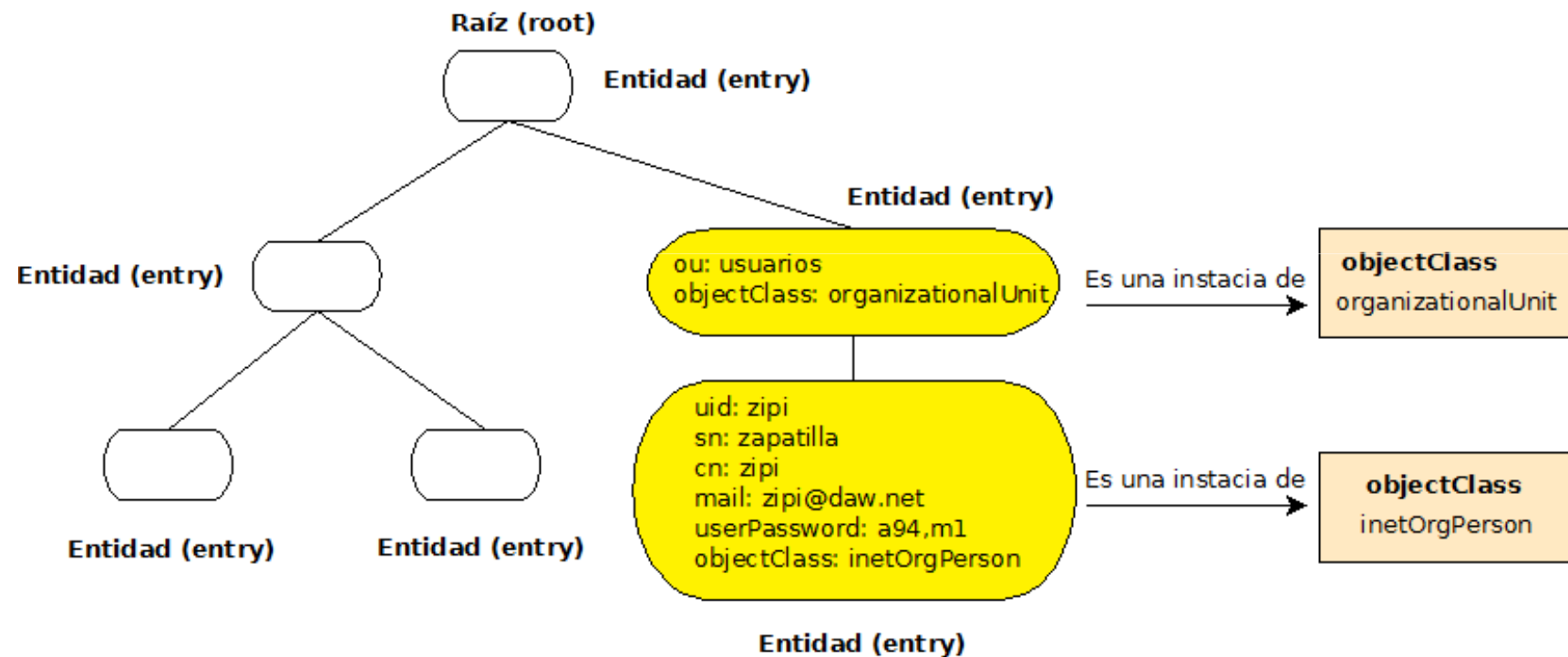
LDAP

Modelo de datos. DIT

- ▶ La información de un directorio LDAP esta formada por un conjunto de objetos – entradas (*entry*) – organizadas jerárquicamente.
- ▶ La estructura resultante se denomina DIT (*Data Information Tree*).
- ▶ La entrada más alta del árbol se denomina normalmente raíz (*root*).

LDAP

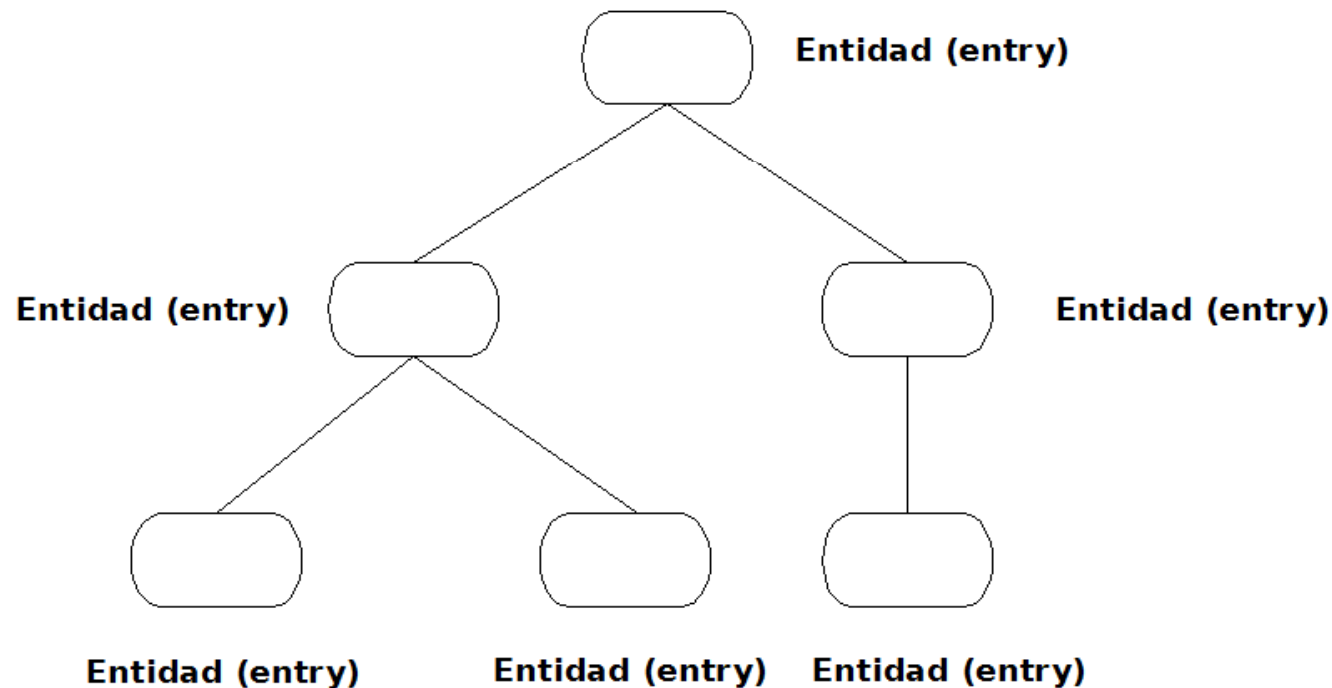
Modelo de datos. DIT



LDAP

Modelo de datos. Entidades (*entry*)

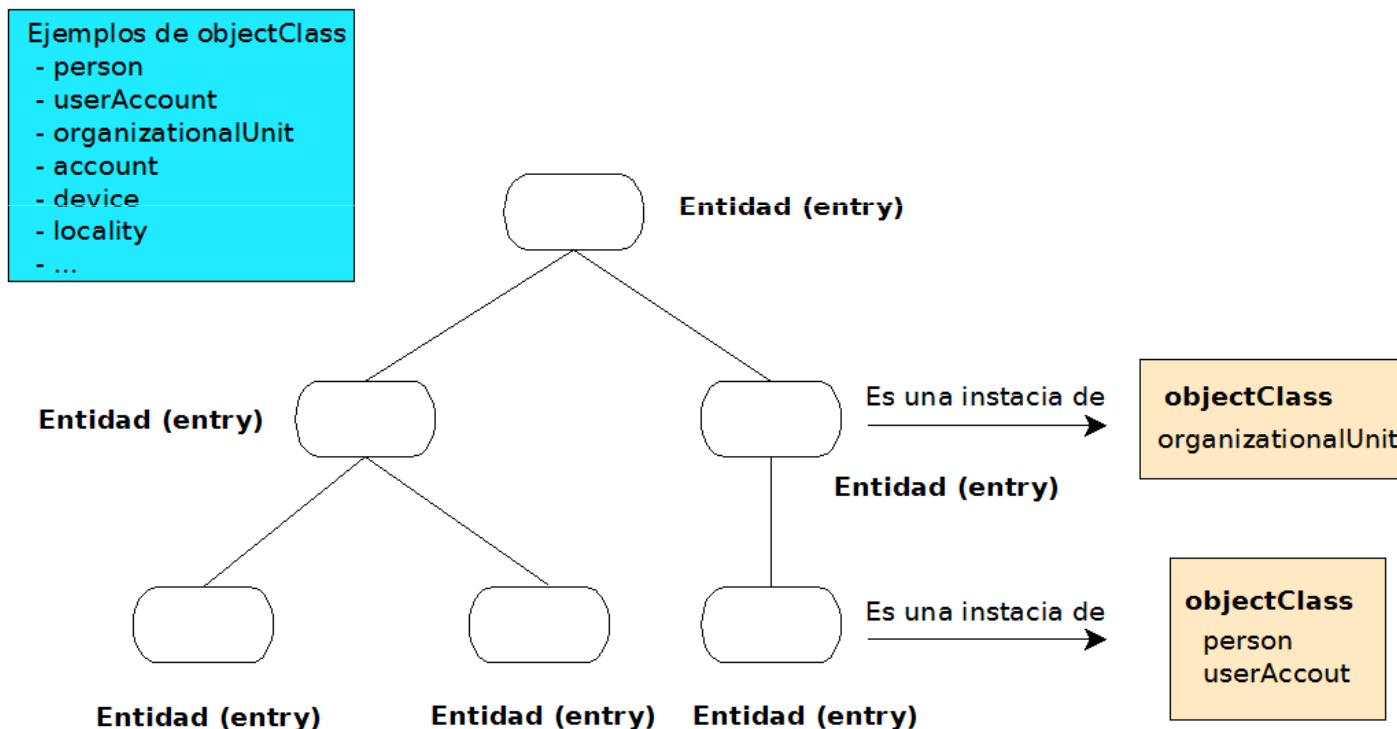
- Conjunto de objetos que forma el directorio LDAP organizados jerárquicamente (DIT).



LDAP

Modelo de datos. *objectClass*

- ▶ Cada entidad (*entry*) es una instancia de una o varias clases (*objectClass*).



LDAP

Modelo de datos. *objectClass*

- ▶ Cada *objectClass* tiene un nombre y define uno varios atributos y sus tipos de datos.
 - Ejemplos de objectClass

Nombre: account
Atributos:
userid (obligatorio) (*)
description
localityName
organizationName
...

Nombre: person
Atributos:
cn (common name) (*)
sn (surname) (*)
telephoneNumber
organizationName
...

- * –> Atributos obligatorios (MUST)
- El resto opcionales (MAY)

LDAP

Modelo de datos. *objectClass*

DESC	● RFC2256: a person
MAY	● userPassword ● telephoneNumber ● seeAlso ● description
MUST	● sn ● cn
NAME	● person
objectClass	● top ● synthetic_JXplorer_schema_object
OID	● 2.5.6.6
SUP	● top

MAY	● description ● seeAlso ● localityName ● organizationName ● organizationalUnitName ● host
MUST	● userid
NAME	● account
objectClass	● top ● synthetic_JXplorer_schema_object
OID	● 0.9.2342.19200300.100.4.5
SUP	● top

LDAP

Modelo de datos. *objectClass*

- ▶ Los *objectClass* son por lo tanto colecciones de atributos.
 - Obligatorio (*MUST*)
 - Opcional (*MAY*)
- ▶ Los *objectClass* puede formar parte de una jerarquía y heredar los atributos de sus padres.
- ▶ Se definen en esquemas (se explican posteriormente).

LDAP

Modelo de datos. *objectClass*

- ▶ Los *objectClass* pueden ser de tipo
 - STRUCTURAL
 - Usados para crear entidades.
 - AUXILIARY
 - Añadidas en entidades existentes (que tienen al menos un *objectClass* STRUCTURAL)
 - ABSTRACT
 - Para definir jerarquías de *objectClass*.

- ▶ Web (ejemplos de *objectClass*).
 - <http://www.zytrax.com/books/ldap/ape/>

LDAP

Modelo de datos. *objectClass*

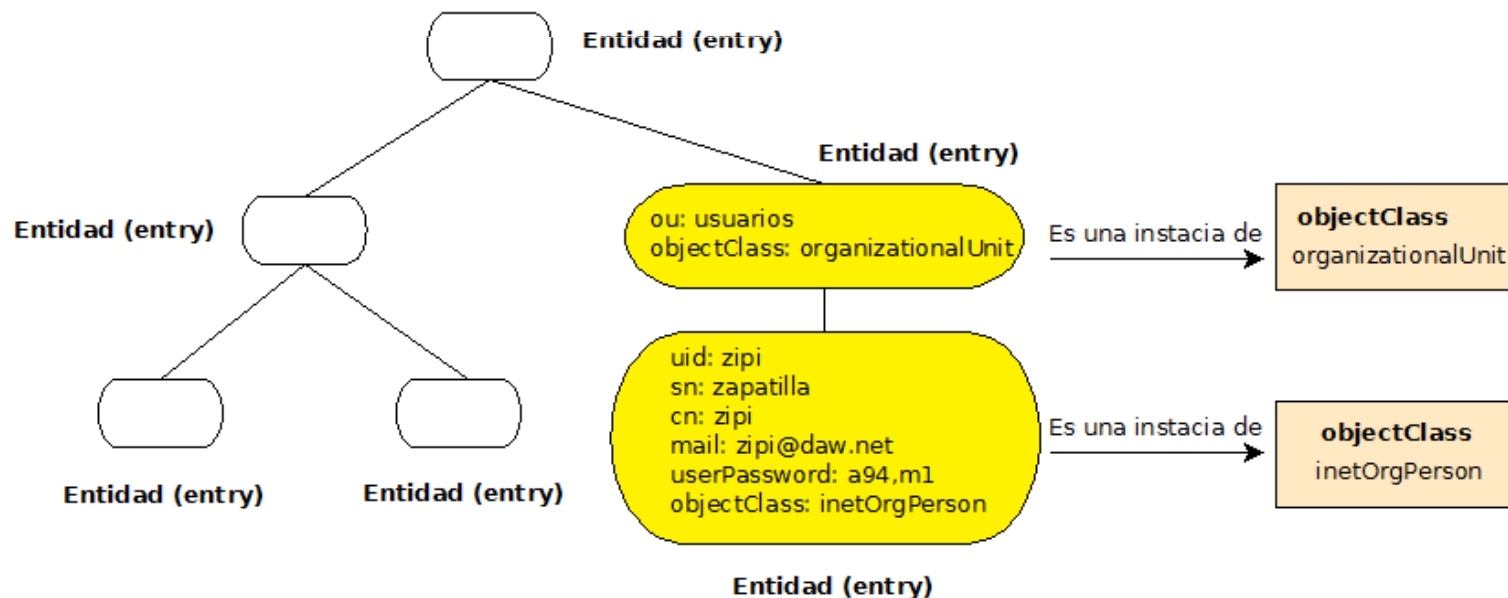
► Las entidades

- Deben pertenecer a un (uno y solo uno) *STRUCTURAL objectClass*.
- Pueden pertenecer a uno o varios *AUXILIARY objectClasses*.
- Pueden pertenecer solo a un *ABSTRACT objectClass*.

LDAP

Modelo de datos. Atributos

- En función de los *objectClass* a los que pertenezcan (sean instancias de) las entidades tendrán valores para los atributos.



LDAP

Modelo de datos. Atributos

- ▶ En las entidades se definen el atributo especial *objectClass* que contiene como valor el/los *objectClass(es)* a los que pertenece la entidad.



LDAP

Modelo de datos. Atributos

- ▶ Todos los atributos son miembros de una o mas *objectClass(es)*.
- ▶ Cada atributo define un tipo de datos que puede contener.
- ▶ Los atributos pueden ser opcionales (MAY) o obligatorios (MUST) dependiendo de la *objectClass*.
 - Un atributo puede ser obligatorio en una *objectClass* y opcional en otra.

LDAP

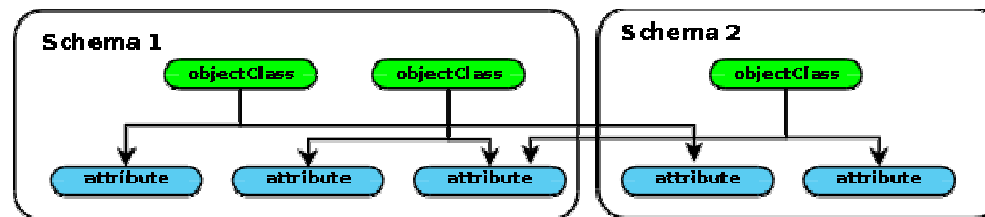
Modelo de datos. Atributos

- ▶ Los atributos puede tener uno o varios valores.
- ▶ Los atributos tienen nombres y a veces abreviaturas.
 - Ejemplo: cn es una abreviatura de commonName.
- ▶ En cada nivel de la jerarquía los datos contenidos en los atributos pueden ser usados para identificar a la entrada (*entry*).

LDAP

Modelo de datos. Esquemas (*Schemas*)

- ▶ Los esquemas (*schemas*) son paquetes que definen:
 - *objectClass* y atributos.
 - Un atributo definido en un esquema puede ser usado por *objectClass* de otros esquemas.



- Podemos crear nuestros esquemas propios con los *objectClass* que nos interesen.

LDAP

Modelo de datos. Esquemas (*Schemas*)

- ▶ Organización de los datos en LDAP:
 - Los datos están contenidos en atributos
 - Los atributos se agrupan en *objectClass*
 - Los *objectClass* se agrupan en esquemas

- ▶ Los esquemas (*schemas*) son paquetes que definen tanto *objectClass* (*es*) como atributos.
 - Podemos crear nuestros esquemas propios con los *objectClass* que nos interesen.

LDAP

Modelo de datos. Esquemas (*Schemas*)

- ▶ Web (ejemplos de esquemas)
 - <http://www.zytrax.com/books/ldap/ape/>

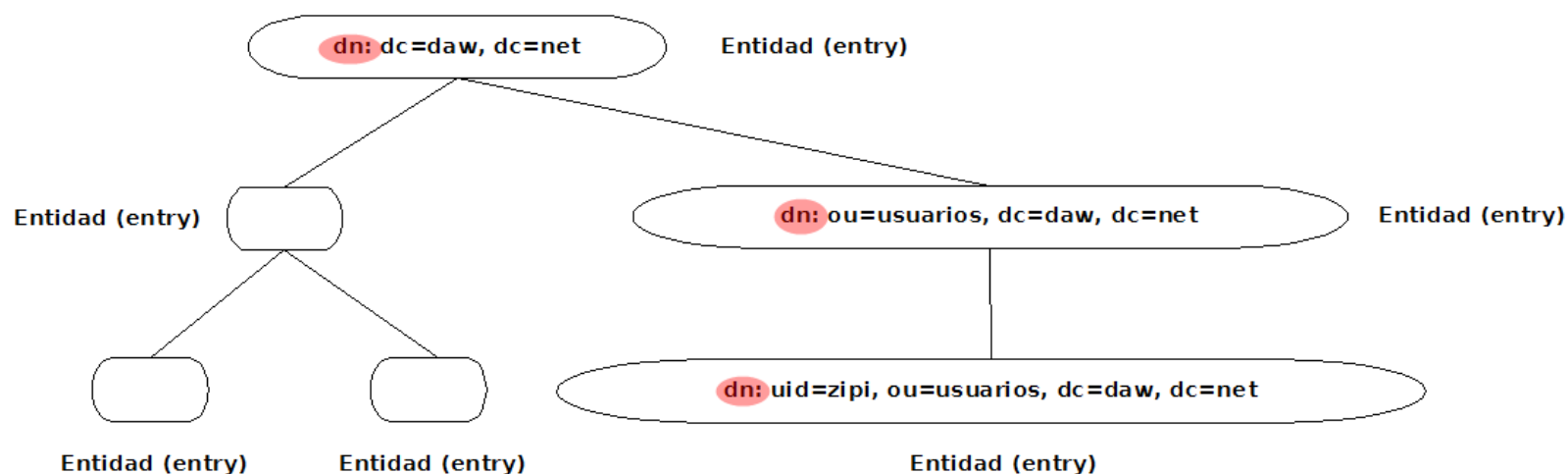
```
objectclass ( 2.5.6.6 NAME 'person' SUP top STRUCTURAL
  MUST ( sn $ cn )
  MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )

objectclass ( 2.5.6.7 NAME 'organizationalPerson' SUP person STRUCTURAL
  MAY ( title $ x121Address $ registeredAddress $ destinationIndicator $
    preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
    telephoneNumber $ internationaliSDNNNumber $
    facsimileTelephoneNumber $ street $ postOfficeBox $ postalCode $
    postalAddress $ physicalDeliveryOfficeName $ ou $ st $ l ) )
```

LDAP

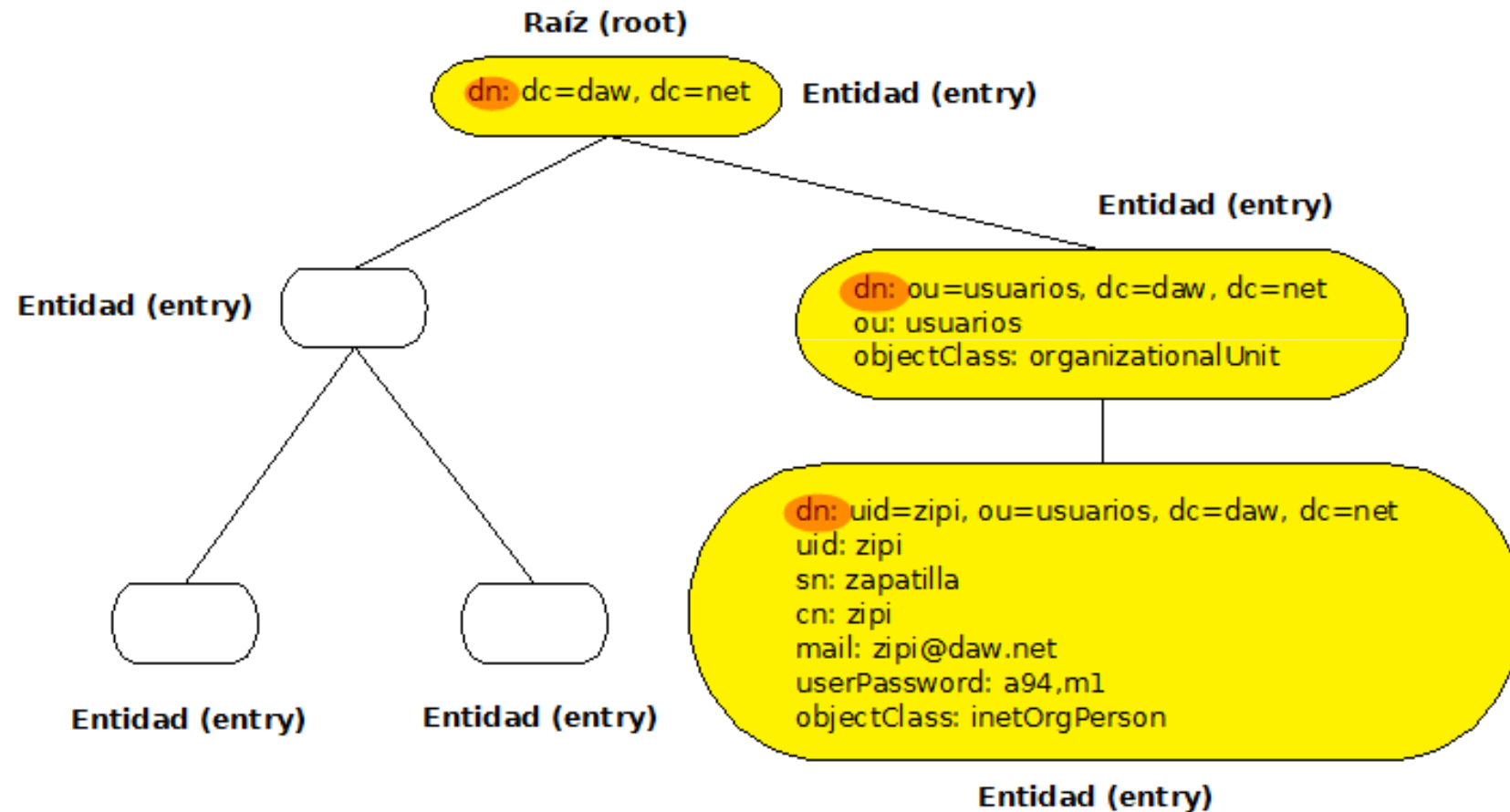
Modelo de nombrado

- ▶ Define como se nombra y se identifica a la información almacenada en el directorio.
- ▶ Las entradas se organizan en el DIT en base a su DN (*Distinguished Name*).



LDAP

Modelo de nombrado



LDAP

Modelo de nombrado

- ▶ DN (*Distinguished Name*): nombre único que identifica de forma unívoca a una entrada.
- ▶ Secuencias de RDNs (*Relative Distinguished Names*) y cada RDN se corresponde con una rama del DIT partiendo de la raíz hacia la entrada dentro del directorio.

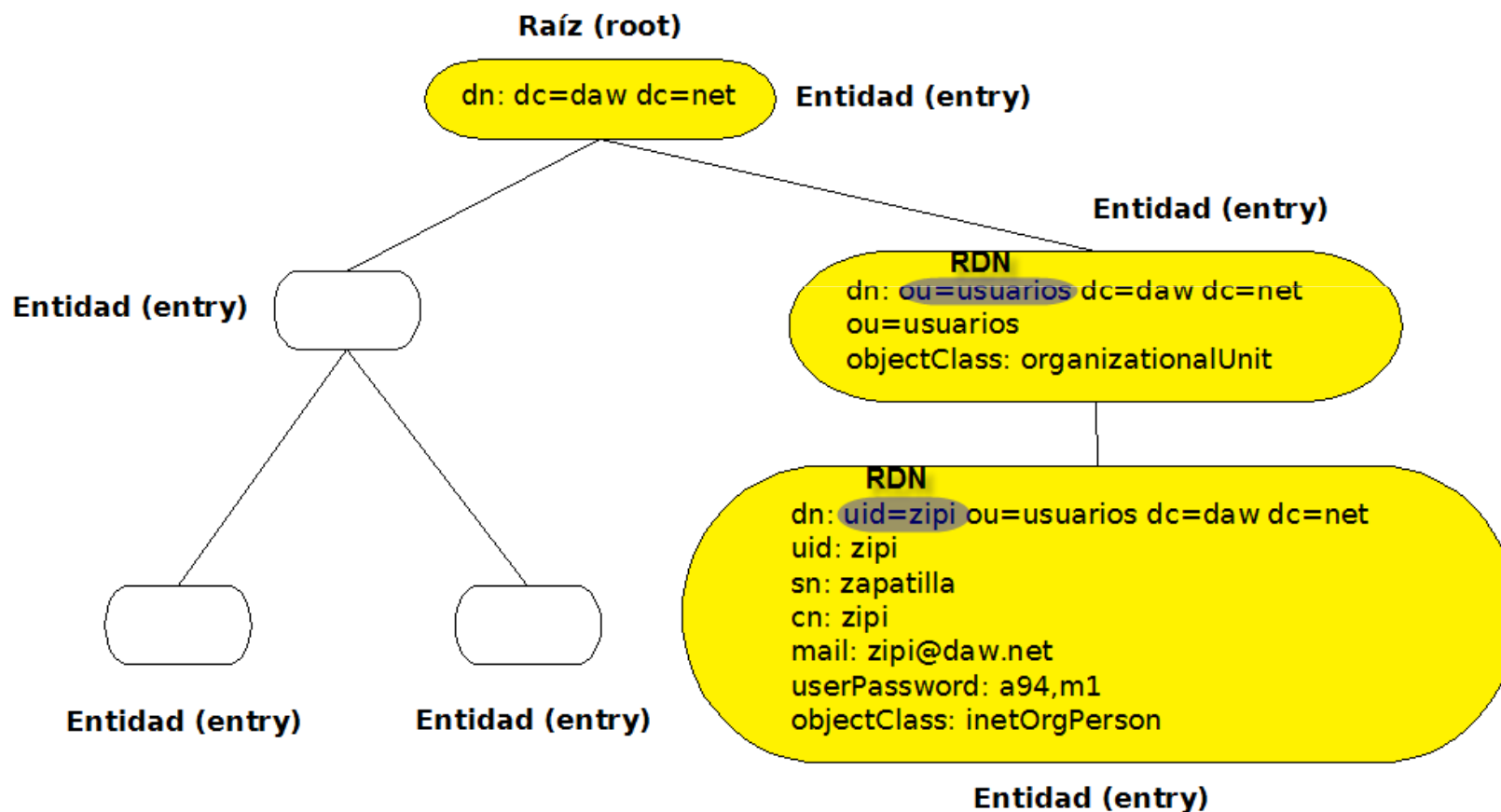
RDN

```
dn: uid=zipi, ou=usuarios, dc=daw, dc=net
uid: zipi
sn: zapatilla
cn: zipi
mail: zipi@daw.net
userPassword: a94,m1
objectClass: inetOrgPerson
```

LDAP

Modelo de nombrado

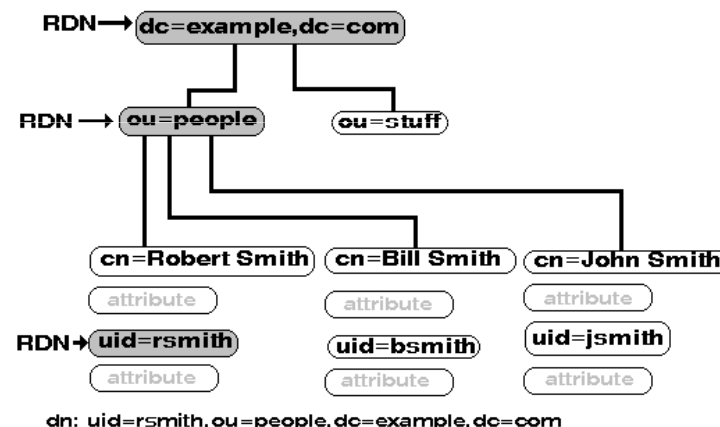
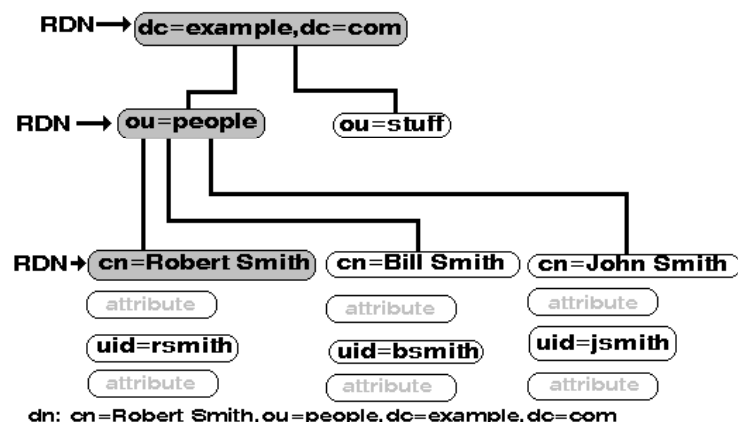
- ▶ DN = camino hasta la raíz + RDN (*relative* DN)



LDAP

Modelo de nombrado

- ▶ Se puede elegir que atributo de la entidad formara el RDN teniendo en cuenta que el DN debe ser único.



- ▶ Web (ejemplos)
 - <http://www.zytrax.com/books/ldap/apa/dn-rdn.html>

LDAP

LDIF

- ▶ *LDAP Data Interchange Files (LDIF).*
- ▶ Estándar para representar las entradas LDAP en formato texto.
- ▶ Usando
 - Importar/exportar datos entre servidores LDAP.
 - Almacenamiento en disco -> Copias de seguridad
 - Añadir, borrar, modificar, ... entradas.
 - ...
- ▶ Web
 - <http://www.zytrax.com/books/ldap/ch8/#overview>

LDAP

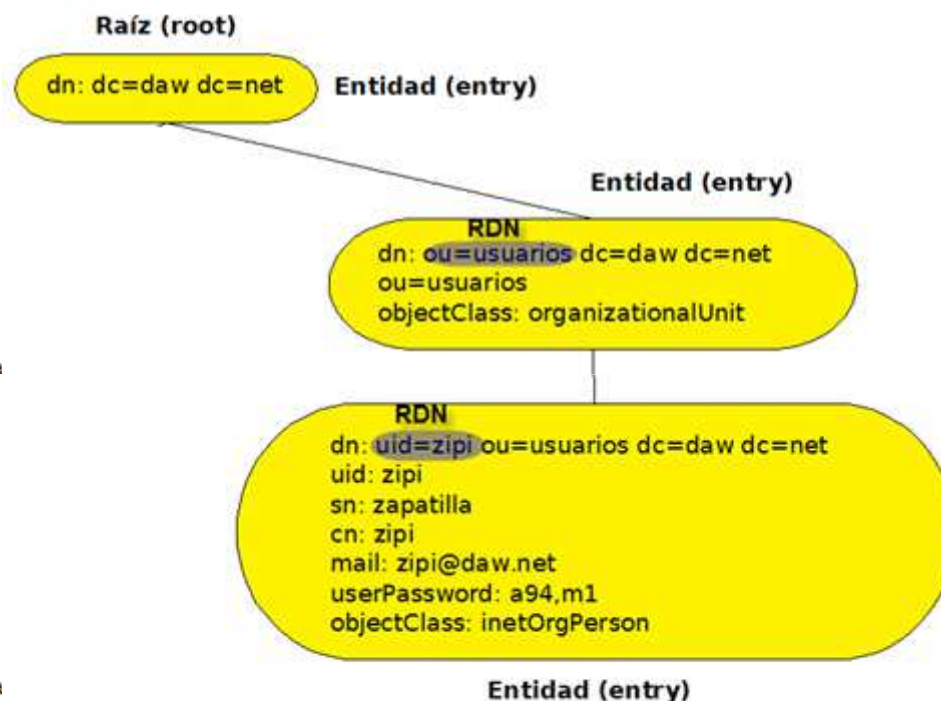
LDIF

```
# Unidad organizativa usuarios
dn: ou=usuarios,dc=daw01,dc=net
objectClass: organizationalUnit
ou: usuarios
```

```
# Unidad organizativa grupos
dn: ou=grupos,dc=daw01,dc=net
objectClass: organizationalUnit
ou: grupos
```

```
# Usuario zipi en al unidad organizativa usua
dn: uid=zipi,ou=grupos,dc=daw01,dc=net
objectClass: inetOrgPerson
uid: zipi
sn: zapatilla
cn: zipi
mail: asterix@daw01.net
userPassword: zipi
```

```
# Usuario zape en al unidad organizativa usua
dn: uid=zape,ou=grupos,dc=daw01,dc=net
objectClass: inetOrgPerson
uid: zape
sn: zapatilla
cn: zape
mail: zape@daw01.net
userPassword: zape
```



LDAP

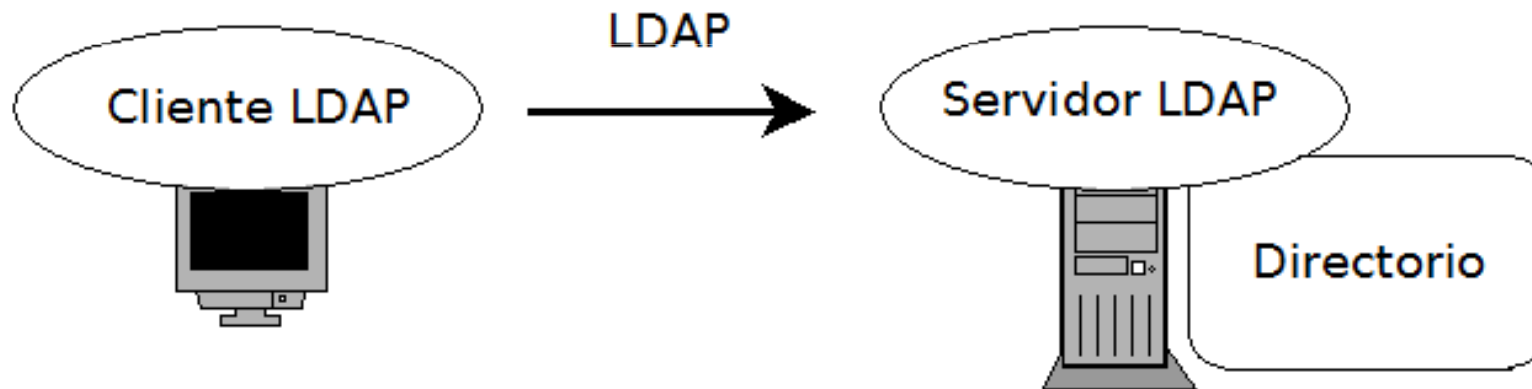
LDIF

- ▶ ¿Qué permite representar LDIF?
 - Entradas (modelos de nombrado y datos)
 - Operaciones sobre las entradas (modelo de funcionamiento)
 - Restricciones de acceso (modelo de seguridad)

LDAP

Modelo de funcionamiento

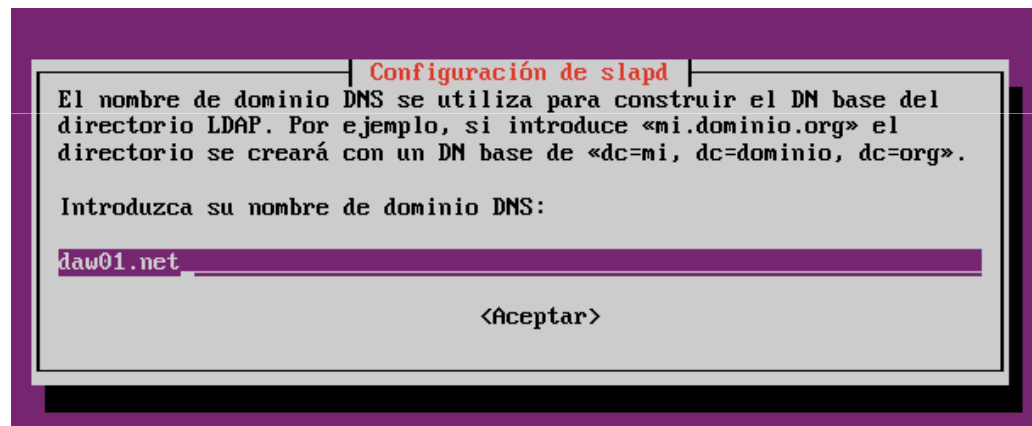
- ▶ Arquitectura cliente/servidor.
 - Servidor -> Puerto 389/TCP



Práctica

► Práctica 10.1

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



```
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
```

LDAP

Modelo de funcionamiento

- ▶ Operaciones sobre el servidor LDAP.
 - Consulta
 - Búsqueda y lectura (*search*)
 - Actualización
 - Añadir (*add*)
 - Borrar (*delete*)
 - Modificar (*modify*)
 - Renombrar un dn (*rename*).
 - Autenticación y control (*bind, unbind, ...*)

LDAP

Modelo de funcionamiento

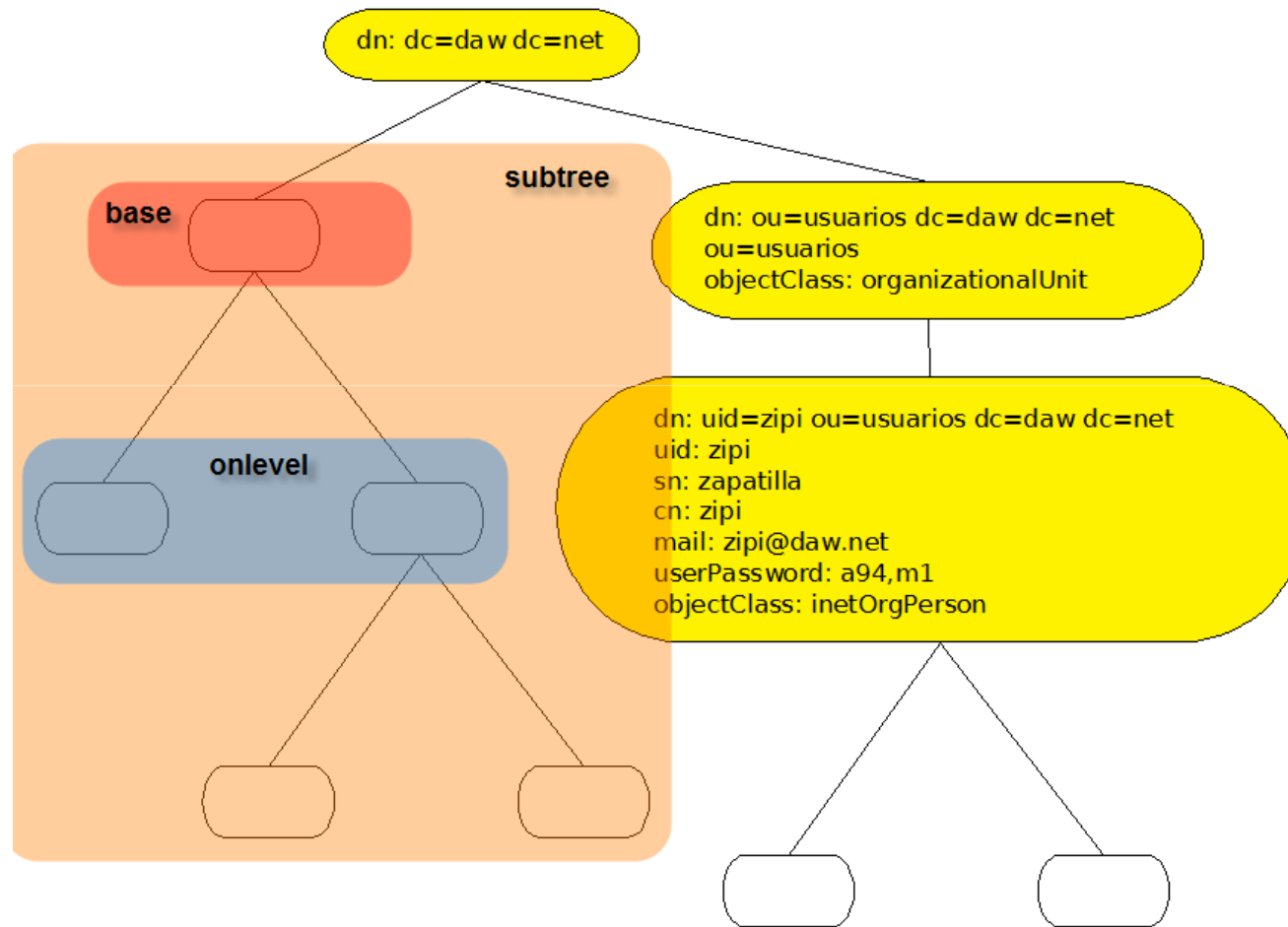
► Consultas (1)

◦ Parámetros principales (1)

- Base: DN a partir del donde buscar.
- Ámbito: Profundidad de búsqueda a partir de la entrada base. Tres opciones:
 - *base*: Solo se busca en la base.
 - *onlevel*: búsqueda sobre el siguiente nivel a la base.
 - *subtree*: búsqueda sobre todo el subárbol bajo la base.

LDAP

Modelo de funcionamiento



LDAP

Modelo de funcionamiento

► Consultas (2)

◦ Parámetros principales (2)

- Lista de atributos a recibir.
- Filtro de búsqueda.

• Ejemplos

- `(objectClass=*)`
- `(objectClass=person)`
- `(cn=*)`
- `(cn=zipi)`
- `(&(objectClass=person)(cn=zipi))`
- `(|(cn=zipi)(sn=zapatilla))`
- `(&(objectClass=person)(|((cn=zipi)/cn=zape)))`

Práctica

- ▶ **Práctica 10.2**
 - Operaciones LDAP.

```
# Unidad organizativa usuarios
dn: ou=usuarios,dc=daw01,dc=net
objectClass: organizationalUnit
ou: usuarios

# Unidad organizativa grupos
dn: ou=grupos,dc=daw01,dc=net
objectClass: organizationalUnit
ou: grupos

# Usuario zipi en al unidad organizativa usuarios
dn: uid=zipi,ou=grupos,dc=daw01,dc=net
objectClass: inetOrgPerson
uid: zipi
sn: zapatilla
cn: zipi
mail: asterix@daw01.net
userPassword: zapi

# Usuario zape en al unidad organizativa usuarios
dn: uid=zape,ou=grupos,dc=daw01,dc=net
objectClass: inetOrgPerson
uid: zape
sn: zapatilla
cn: zape
mail: zape@daw01.net
userPassword: zape
```

```
uid=zape,ou=grupos,dc=daw01,dc=net
uid=zipi,ou=grupos,dc=daw01,dc=net
ou=usuarios,dc=daw01,dc=net
ou=grupos,dc=daw01,dc=net
```

LDAP

Usos

- ▶ Representar y almacenar información sobre organizaciones (departamentos, usuarios, equipamiento, ...)
- ▶ Servicios centralizados
 - Usuarios/grupos.
 - Autenticación (Sistema, FTP, Correo, Web, WiFi, ...)
 - Perfiles de usuarios
 - ...

LDAP

Software

- ▶ Servidores LDAP
 - *OpenLDAP*
 - *Active Directory (AD) (Microsoft)*
 - *Apache Directory.*
 - *Oracle Internet Directory*
 - *RedHat Directory Server*
 - *IBM Directory Server*
 - *Open DS*
 - *389 Directory Server*
 - ...

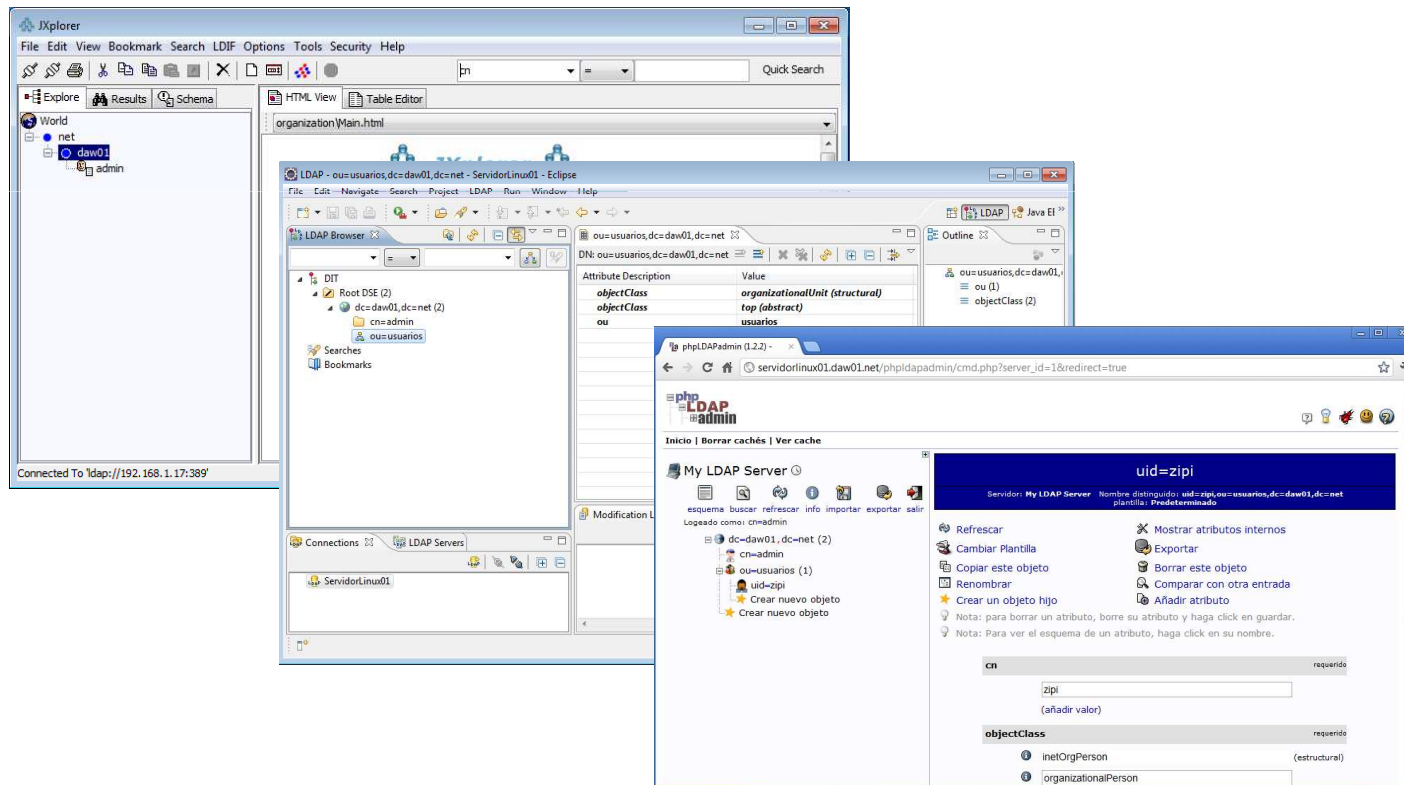
LDAP

Software

- ▶ Clientes LDAP
 - *Apache Directory Studio*
 - *JXplorer*
 - *phpLDADadmin*
 - *LDAPExplorerTool*
 - *Fusiondirectory*
 - *OpenLDAP Tools*
 - ...

Práctica

- ▶ Práctica 10.3
 - Clientes LDAP.



Autenticación/Autorización LDAP

Apache

► Modulo

- `mod_authnz_ldap`
- http://httpd.apache.org/docs/2.4/mod/mod_authnz_ldap.html

► Directicas

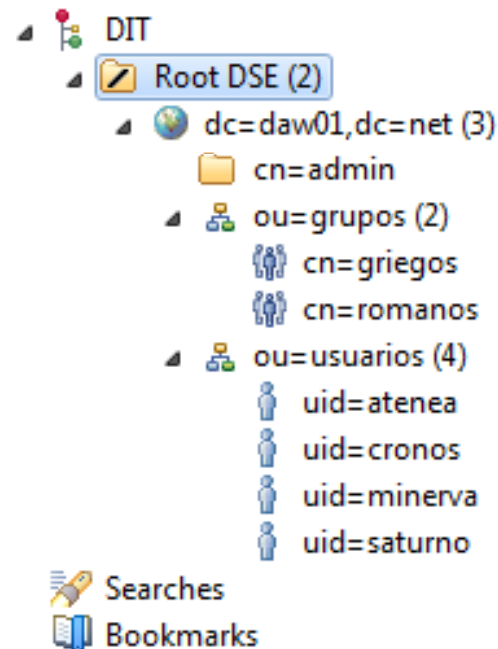
- `AuthType`
- `AuthBasicProvider`
`AuthzLDAPAuthoritative`
`AuthName`
- `AuthLDAPURL`
- `AuthLDAPBindDN`
- `AuthLDAPBindPassword`
- `Require`

Autenticación/Autorización LDAP

Apache

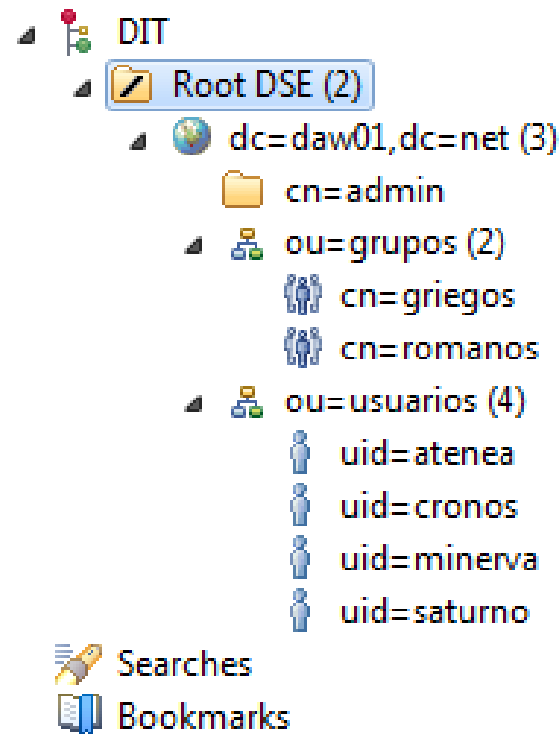
► Configuración (1)

- 1) Configurar el servidor LDAP con los usuarios y contraseñas adecuados.



Práctica

- ▶ **Práctica 10.4**
 - Configuración del el servidor LDAP



Autenticación/Autorización LDAP

Apache

- Configuración (2)
 - 2) Configurar la autenticación en *Apache*.

```
<Directory /var/www/html/profesor>
    Options Indexes FollowSymLinks
    AllowOverride None
    AuthType Basic
    AuthBasicProvider ldap
    AuthName "Introduce tu usuario y password"
    AuthLDAPURL "ldap://localhost/dc=daw01,dc=net?uid?sub?(objectClass=*)"
    AuthLDAPBindDN "cn=admin,dc=daw01,dc=net"
    AuthLDAPBindPassword despliegue
    <RequireALL>
        Require ldap-group cn=griegos,ou=grupos,dc=daw01,dc=net
    <RequireAny>
        Require ip 127.0.0.1
        Require ip 192.168.1.16
    </RequireAny>
</RequireALL>
</Directory>
```

Autenticación/Autorización LDAP

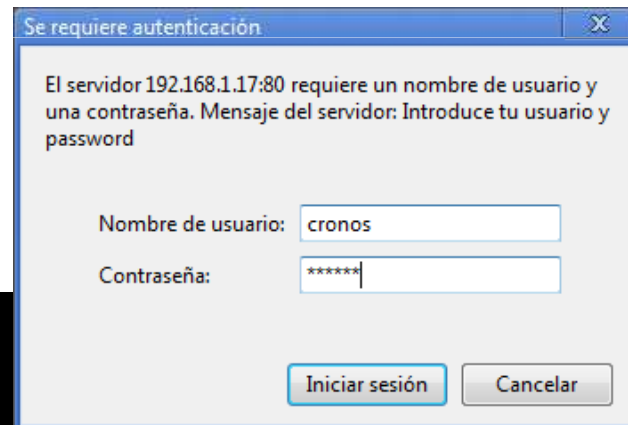
Apache

► Proceso (1)

◦ 1) Fase de autenticación (1)

- 1) Se genera un filtro de búsqueda combinando el atributo y el filtro proporcionados en la directiva AuthLDAPURL con el nombre de usuario introducido por el usuario.

```
AuthType Basic
AuthBasicProvider ldap
AuthzLDAPAuthoritative on
AuthName "Introduce tu usuario y password"
AuthLDAPURL "ldap://localhost/dc=daw01,dc=net?uid?sub?(objectClass=*)"
AuthLDAPBindDN "cn=admin,dc=daw01,dc=net"
AuthLDAPBindPassword despliegue
```



Autenticación/Autorización LDAP

Apache

► Proceso (2)

- 1) Fase de autenticación (2)
 - 2) Se establece una conexión al servidor LDAP con el usuario y password definidos en AuthLDAPBindDN y AuthLDAPBindPassword y se realiza una búsqueda con el filtro generado anteriormente. Si la búsqueda no retorna una entrada exactamente se deniega el acceso

```
AuthType Basic
AuthBasicProvider ldap
AuthzLDAPAuthoritative on
AuthName "Introduce tu usuario y password"
AuthLDAPURL "ldap://localhost/dc=daw01,dc=net?uid?sub?(objectClass=*)"
AuthLDAPBindDN "cn=admin,dc=daw01,dc=net"
AuthLDAPBindPassword despliegue
```

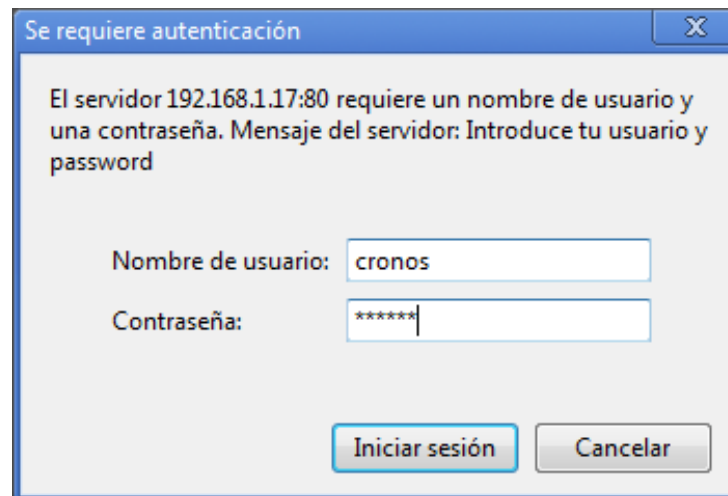
Autenticación/Autorización LDAP

Apache

► Proceso (3)

◦ 1) Fase de autenticación (3)

- 3) Se obtiene la entrada y se realiza una conexión al servidor usando el DN de la entrada y la password introducida por el usuario. Si la conexión es posible se permite el acceso y si no se deniega.



Autenticación/Autorización LDAP

Apache

► Proceso (4)

◦ 2) Fase de autorización (1)

- Se utilizan las directivas `Require` para determinar si el usuario es autorizado o no.
 - `Require ldap-user`
 - `Require ldap-dn`
 - `Require ldap-group`
 - `Require ldap-attribute`
 - `Require ldap-filter`
- Cada una de ellas tiene otro conjunto de directivas asociadas para controlar su comportamiento.

Autenticación/Autorización LDAP

Apache

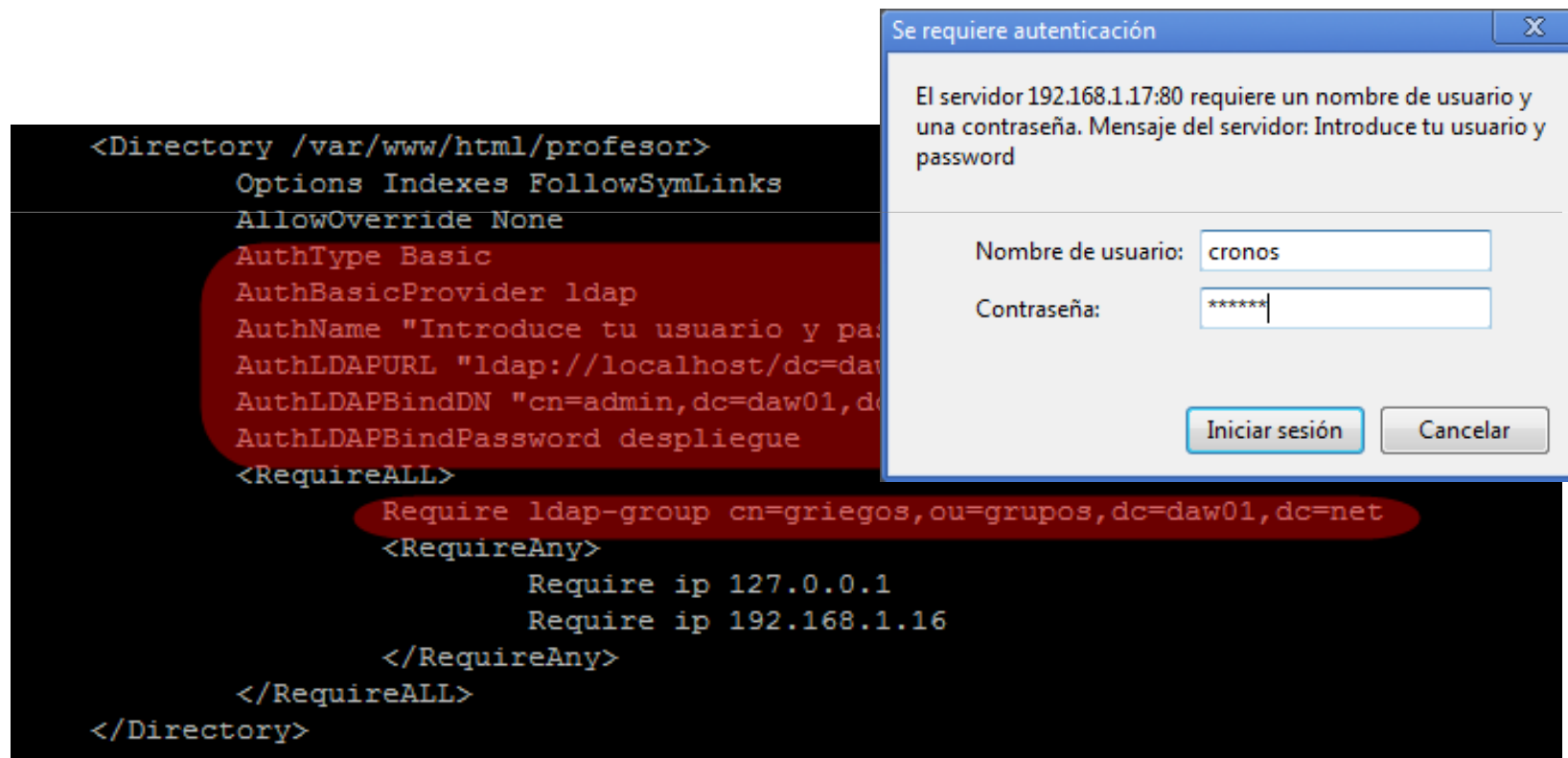
- ▶ Proceso (4)
 - 2) Fase de autorización (2)

```
<Directory /var/www/html/profesor>
    Options Indexes FollowSymLinks
    AllowOverride None
    AuthType Basic
    AuthBasicProvider ldap
    AuthName "Introduce tu usuario y password"
    AuthLDAPURL "ldap://localhost/dc=daw01,dc=net?uid?sub?(objectClass=*)"
    AuthLDAPBindDN "cn=admin,dc=daw01,dc=net"
    AuthLDAPBindPassword despliegue
    <RequireALL>
        Require ldap-group cn=griegos,ou=grupos,dc=daw01,dc=net
    <RequireAny>
        Require ip 127.0.0.1
        Require ip 192.168.1.16
    </RequireAny>
</RequireALL>
</Directory>
```

Práctica

► Práctica 10.5

- Autenticación y autorización LDAP en *Apache*.



The image shows a screenshot of an Apache httpd.conf configuration file and an authentication dialog box. The configuration file is displayed in a dark-themed editor with red highlighting for the authentication section. The dialog box is titled "Se requiere autenticación" and contains a message in Spanish asking for a username and password. The username field is filled with "cronos" and the password field is filled with "*****". There are "Iniciar sesión" and "Cancelar" buttons at the bottom of the dialog.

```
<Directory /var/www/html/profesor>
    Options Indexes FollowSymLinks
    AllowOverride None
    AuthType Basic
    AuthBasicProvider ldap
    AuthName "Introduce tu usuario y contraseña"
    AuthLDAPURL "ldap://localhost/dc=daw01,dc=net"
    AuthLDAPBindDN "cn=admin,dc=daw01,dc=net"
    AuthLDAPBindPassword despliegue
    <RequireALL>
        Require ldap-group cn=griegos,ou=grupos,dc=daw01,dc=net
    </RequireALL>
</Directory>
```

Se requiere autenticación

El servidor 192.168.1.17:80 requiere un nombre de usuario y una contraseña. Mensaje del servidor: Introduce tu usuario y password

Nombre de usuario: cronos

Contraseña: *****

Iniciar sesión Cancelar

Autenticación/Autorización LDAP

Tomcat

- ▶ La autenticación/autorización sobre LDAP en *Tomcat* se configura con un **JNDIRealm**.
- ▶ Web
 - <http://tomcat.apache.org/tomcat-7.0-doc/realm-howto.htm>
 - <http://tomcat.apache.org/tomcat-7.0-doc/config/realm.html>

Autenticación/Autorización LDAP

Tomcat

► Autenticación (1)

- Dos opciones.
- *Bind mode*
 - El Realm autentica al usuario en el servidor LDAP usando el nombre y password que introduce el usuario. Si puede, la autenticación es posible y el usuario se considera autenticado.

```
<Context>
  <Realm className="org.apache.catalina.realm.JNDIRealm"
    connectionURL="ldap://localhost:389"
    userPattern="uid={0},ou=usuarios,dc=daw01,dc=net"
    roleBase="ou=grupos,dc=daw01,dc=net"
    roleName="cn"
    roleSearch="(uniqueMember={0})"
  />
</Context>
```

Autenticación/Autorización LDAP

Tomcat

► Autenticación (2)

◦ *Compare mode*

- El Realm se autentica en el servidor LDAP con un usuario configurado (por ejemplo admin), y verifica si el usuario y password introducidos por el usuario existen en el servidor.

```
<Context>
  <Realm className="org.apache.catalina.realm.JNDIRealm"
    connectionName="cn=admin,dc=daw01,dc=net"
    connectionPassword="despliegue"
    connectionURL="ldap://localhost:389"
    userPassword="userPassword"
    userPattern="uid={0},ou=usuarios,dc=daw01,dc=net"
    roleBase="ou=grupos,dc=daw01,dc=net"
    roleName="cn"
    roleSearch="(uniqueMember={0})"
  />
</Context>
```

Autenticación/Autorización LDAP

Tomcat

- ▶ Autorización (representación de roles) (1)
 - Dos opciones.
 - Roles como entradas el directorio
 - Cada role se suele corresponder con una entrada de grupo y en sus atributos se definen a los usuarios.
 - Atributos del Realm para configurar la búsqueda.
 - **roleBase**
 - **roleSubtree**
 - **roleSearch**
 - **roleName**
 - **roleNested**

```
<Context>
  <Realm
    className="org.apache.catalina.realm.JNDIRealm"
    connectionURL="ldap://localhost:389"
    userPattern="uid={0},ou=usuarios,dc=daw01,dc=net"
    roleBase="ou=grupos,dc=daw01,dc=net"
    roleName="cn"
    roleSearch="(uniqueMember={0})"
  />
</Context>
```

Autenticación/Autorización LDAP

Tomcat

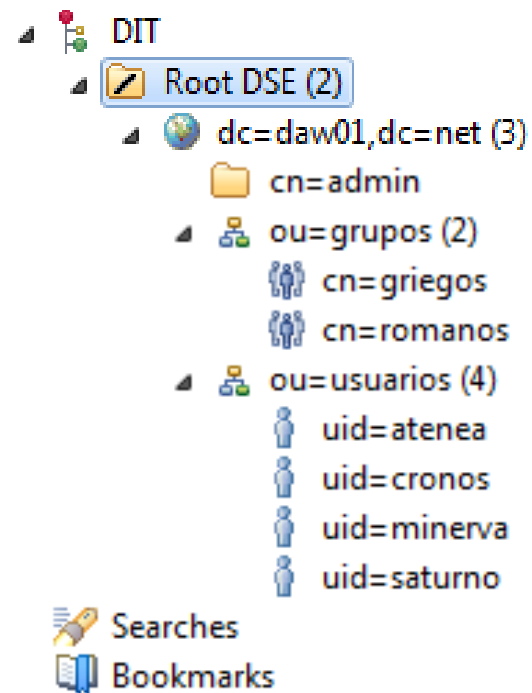
- ▶ **Autorización (representación de de roles) (2)**
 - Roles como atributos de una entrada de usuario
 - Roles almacenados como valores de los atributos.
 - Directiva para indicar que atributo se utiliza.
 - `userRoleName`

Autenticación/Autorización LDAP

Tomcat

► Configuración (1)

- 1) Configurar el servidor LDAP con los usuarios y contraseñas adecuados.



Autenticación/Autorización LDAP

Tomcat

► Configuración (2)

- 2) Configurar el Realm en el ámbito que se considere más adecuado (<Engine>, <Host>, <Context>, ...)

```
<Context>
  <Realm className="org.apache.catalina.realm.JNDIRealm"
    connectionURL="ldap://localhost:389"
    userPattern="uid={0},ou=usuarios,dc=daw01,dc=net"
    roleBase="ou=grupos,dc=daw01,dc=net"
    roleName="cn"
    roleSearch="(uniqueMember={0})"
  />
</Context>
```

Autenticación/Autorización LDAP

Tomcat

► Configuración (3)

- 3) Proteger el recurso (en el descriptor de despliegue web.xml de la aplicación).

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>JNDIRealm</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>griegos</role-name>
  </auth-constraint>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```


Autenticación/Autorización LDAP

Tomcat

- ▶ Configuración (4)
 - ▶ 4) Configurar el tipo autenticación (en el descriptor de despliegue `web.xml` de la aplicación).

```
<login-config>  
  <auth-method>BASIC</auth-method>  
  <realm-name>Acceso al curso</realm-name>  
</login-config>
```

Práctica

► Práctica 10.6

- Autenticación y autorización LDAP en *Tomcat* (*JNDIRealm*).

```
<Context>
  <Realm className="org.apache.catalina.realm.JNDIRealm"
    connectionURL="ldap://localhost:389"
    userPattern="uid={0},ou=usuarios,dc=daw01,dc=net"
    roleBase="ou=grupos,dc=daw01,dc=net"
    roleName="cn"
    roleSearch="(uniqueMember={0})"
  />
</Context>

<security-constraint>
  <web-resource-collection>
    <web-resource-name>JNDIRealm</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>griegos</role-name>
  </auth-constraint>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```

Bibliografía

- ▶ <http://www.zytrax.com/books/ldap/>
- ▶ Introducción al Servicio de Directorio. Rafael Calzada Pradas.
- ▶ <http://www.wikipedia.org>
- ▶ <http://httpd.apache.org>
- ▶ <http://tomcat.apache.org>