Administració de dominis

Jordi Masfret Corrons

Implantació de sistemes operatius (ASX)
Sistemes informàtics (DAM)
Sistemes informàtics (DAW)

Índex

Introducció

Les xarxes d'àrea local han anat estenent el seu ús a tot tipus d'organitzacions, empreses públiques o privades. La utilització de les xarxes d'àrea local s'ha generalitzat en molts entorns, al mateix temps que ha augmentat la complexitat d'aquestes xarxes: cada vegada més, les empreses o institucions tenen més ordinadors connectats entre si mitjançant aquestes xarxes. En l'àmbit domèstic, ens pot servir una xarxa on tots els nodes siguin iguals (xarxa entre iguals), on cadascun dels ordinadors tingui els seus usuaris, amb les seves preferències. Aquest esquema de xarxa correspondria a un grup de treball.

A mesura que augmenta la complexitat de la xarxa, esdevé necessari establir algun mètode per simplificar la gestió i el manteniment d'aquesta xarxa. Si en alguns casos ja és prou complicat fer el manteniment d'un sol ordinador, per a un administrador de sistemes es faria gairebé impossible mantenir una xarxa on tots els ordinadors tenen els seus propis usuaris, aplicacions i preferències. Per això, sorgeix la necessitat de centralitzar tota aquesta informació en un sol ordinador, amb la qual cosa es facilita d'una manera molt important tota la gestió d'usuaris i equips que formen part de la xarxa.

La manera de centralitzar aquesta informació d'usuaris i equips és mitjançant la creació d'un domini. En un domini, com a mínim hi ha un servidor (PDC, *primary domain controller*), que emmagatzema tota aquesta informació. Això, a banda de simplificar l'administració del domini, permet que un usuari pugui accedir a les mateixes preferències, aplicacions i fitxers de treball independentment de l'ordinador des del qual es connecta.

Hi ha moltes maneres d'implementar un domini, però si utilitzem programari lliure, com és el nostre cas, fent servir la distribució de GNU/Linux Ubuntu Server 10.04 LTS, escollirem la implementació mitjançant OpenLDAP. OpenLDAP és una implementació lliure de l'estàndard LDAP (*lightweight directory access protocol*, 'protocol d'accés a directori lleuger'), que permet una manera centralitzada i eficient d'implementar dominis des del punt de vista de la gestió, especialment dels usuaris i dels grups.

En l'apartat "Implementació de dominis LDAP" d'aquesta unitat, veurem tots els factors que s'han de tenir en compte a l'hora de planificar un domini, els requeriments de maquinari i programari necessaris per fer una instal·lació bàsica d'un servidor de domini LDAP, una descripció genèrica del protocol i també com s'ha de documentar tot el procés. És un apartat molt important, ja que sense una planificació prèvia, i una documentació del procés, la realització de la feina no tindria sentit.

En l'apartat "Administració de comptes i grups LDAP", un cop s'haurà dut a terme la implementació del servidor de LDAP, veurem que, mitjançant una eina amb interfície web (phpLDAPadmin), podem fer la gestió dels usuaris, i els grups

d'aquest domini. També integrarem el servidor de LDAP amb el protocol SAMBA per tal que al servidor es puguin connectar clients que funcionen amb altres sistemes operatius com els de la família Windows.

Per tal de poder assolir convenientment els resultats d'aprenentatge d'aquesta unitat, és necessari que, utilitzant una màquina virtual basada en Ubuntu Server 10.04 LTS, seguiu les instruccions de l'apartat "Implementació de Dominis LDAP", i que posteriorment, resolgueu les qüestions d'autoavaluació, i la pràctica proposada en la secció "Annex" del material web sobre administració d'usuaris i grups amb phpLDAPadmin, que està relacionada amb l' apartat "Administració de comptes i grups LDAP".

Resultats d'aprenentatge

En finalitzar aquesta unitat, l'alumne/a:

1. Centralitza la informació en servidors administrant estructures de dominis i analitzant-ne els avantatges.

- Implementa dominis.
- Administra comptes d'usuari i comptes d'equip.
- Centralitza la informació personal dels usuaris del domini mitjançant l'ús de perfils mòbils i carpetes personals.
- Crea i administra grups de seguretat.
- Crea plantilles que facilitin l'administració d'usuaris amb característiques similars.
- Organitza els objectes del domini per facilitar-ne l'administració.
- Utilitza màquines virtuals per administrar dominis i verificar-ne el funcionament.
- Documenta l'estructura del domini i les tasques realitzades.

1. Implementació de dominis LDAP

Inicialment, quan muntem una xarxa informàtica amb pocs nodes, podem establir un esquema, en què cadascun dels nodes té les mateixes funcionalitats, sense cap tipus de jerarquia. Això s'anomena *xarxa d'igual a igual*, i conforma el que podem designar com a *grup de treball*.

En aquest esquema de funcionament de la xarxa, la informació no està centralitzada, i cadascun dels nodes té uns usuaris amb les preferències corresponents. D'aquesta manera, hi ha la possibilitat que un usuari determinat pugui accedir a un dels nodes de la xarxa, però que no ho pugui fer des d'altres.

A més a més, pot ser que aquesta xarxa es vagi ampliant amb nous usuaris i nous equipaments, els quals s'hauran de connectar a un ordinador determinat, amb uns usuaris concrets, cosa que en complica molt la gestió.

És evident que, davant d'això, cal una gestió centralitzada dels usuaris i dels recursos dels ordinadors que formen part de la xarxa d'àrea local. Ha de realitzar aquesta tasca un ordinador en concret que farà la funció de **servidor** de domini.

> Un **domini** és un conjunt d'ordinadors que estan connectats en xarxa entre ells, i que formen part d'una estructura jerarquitzada que permet gestionar d'una manera centralitzada en un servidor l'accés a un conjunt de recursos per part dels usuaris i equips que en formen part.

Mitjançant aquesta filosofia, s'augmenta d'una manera significativa la fiabilitat i disponibilitat dels recursos del domini, i l'accés als recursos d'un determinat usuari del domini és independent de l'ordinador des del qual vol accedir a aquests recursos.

1.1 Dominis LDAP

Sistemes operatius diferents de LDAP tenen una implementació diferent dels dominis, com, per exemple, l'Active Directory de Windows Server.

LDAP és una especificació oberta que permet una implementació d'un domini mitjançant sistemes operatius lliures, i també propietaris. Podem obtenir implementacions lliures de LDAP; per exemple, *OpenLDAP*, que pot funcionar en sistemes operatius lliures com ara GNU/Linux.

OpenLDAP

El programari OpenLDAP és una implementació basada en codi obert, del Protocol d'Accés Lleuger a Directori.

1.1.1 Estructura client-servidor

Per poder crear un domini, cal implementar una estructura en forma de client-servidor. Això vol dir que hi ha d'haver un o més nodes de la xarxa (generalment, ordinadors amb un sistema operatiu orientat a la xarxa), que funcionin d'una manera ininterrompuda i que, mitjançant una base de dades, permeten els recursos de la xarxa. Aquests ordinadors s'anomenen **servidors**.

Els servidors gestionen i permeten l'accés a aquests recursos dels clients que s'hi connecten. Per tal de permetre l'accés a algun recurs de la xarxa, el client ha d'estar donat d'alta en una base de dades desada en el servidor de domini.

Quan els clients volen accedir a un determinat recurs del domini, s'han d'identificar mitjançant un compte d'usuari i una contrasenya, o des d'un compte d'equip específic, que estarà emmagatzemat en el servidor, i que, per tant, no dependrà del client concret des del qual es vulgui identificar l'usuari.

L'accés als recursos del domini és independent de l'ordinador físic des del qual es duu a terme la connexió: només depèn de l'usuari del domini amb el qual es vol fer aquest accés.

1.1.2 El protocol LDAP

LDAP és un acrònim anglès de *lightweight directory access protocol*; és a dir, 'protocol d'accés a directori lleuger'. És un protocol del tipus client-servidor que permet llegir i editar directoris a través d'una xarxa que funciona sobre el protocol TCP/IP. Un directori és un conjunt de registres. Per exemple: una llista telefònica ordenada alfabèticament en què cada persona i organització té un telèfon i una adreça associats.

Protocol X.500

És el protocol d'accés a directori (DAP), que segueix la norma ISO/IEC 9594. És el precursor de LDAP i permet una manera de desenvolupar un directori de persones en una organització, perquè pugui formar part d'un directori global disponible per qualsevol persona d'arreu del món per mitjà d'Internet.

En el cas dels dominis, LDAP serveix per accedir a un servei de directori (com ara un servidor de domini amb usuaris, equips i recursos); la darrera versió és la 3.

Inicialment, el 1993, va ser desenvolupat per la Universitat de Michigan per tal de reemplaçar el protocol DAP (que es feia servir per accedir als serveis de directori X.500 d'OSI), integrant-lo d'una manera adequada a les xarxes TCP/IP. Des del 1995, DAP es va convertir en un LDAP autosuficient, de manera que es pot utilitzar per altres coses a banda d'accedir als directoris del tipus X.500.

De fet, LDAP defineix el mètode d'accés a les dades en el servidor a nivell del client, i no la manera com s'emmagatzema aquesta informació. LDAP dóna a l'usuari un conjunt de mètodes que permeten:

- Connectar-se.
- Desconnectar-se.
- Cercar informació.
- Comparar informació.
- Inserir entrades.
- Canviar entrades.
- Esborrar entrades.

A més a més, en la seva versió actual (la 3), LDAP ofereix encriptació via protocol SSL, i mecanismes d'autenticació per tal d'accedir a la informació emmagatzemada a la base de dades d'una manera segura.

LDAP presenta la informació en forma d'una estructura d'arbre jeràrquica, anomenada *DIT* (*directory information tree*, 'arbre d'informació de directori'). En aquest arbre, la informació anomenada *entrades* o *DSE* (*directory service entry*, 'entrada de servei de directori'), és representada en forma de branques. La branca localitzada a l'arrel és l'entrada arrel. Cada entrada en el directori LDAP està relacionada amb un objecte real o abstracte; per exemple, una persona, un ordinador, paràmetres, etc.

Cada entrada està formada per una col·lecció de parells de valors (o claus), anomenada *atributs*. D'aquesta manera es permet distingir cada objecte que consta en l'arbre. Hi ha dos tipus d'atributs:

- **Atributs normals**: són els habituals, com ara el nom, el cognom...), que serveixen per distingir l'objecte.
- **Atributs operacionals**: atributs als quals només pot accedir el servidor per tal de manipular les dades del directori (per exemple, modificar dades).

Cadascuna de les entrades està indexada per un DN (*distinguished name*, 'nom distingit'), de manera que es pot identificar aquest element d'una manera unívoca. Per crear un DN, prenem el nom de l'element anomenat *RDN* (*relative distinguished name*, 'nom distingit relatiu'), i hi afegim el nom sencer de l'entrada pare. La identificació unívoca d'una entrada depèn de la utilització correcta de parells de valors o claus. El conjunt de claus que es fa servir normalment són les següents:

- **uid** (*userid*): és un identificador únic per a cada usuari.
- **cn** (*common name*): és el nom d'usuari.
- **givenname**: és el nom de la persona.
- **sn** (*surname*): és el cognom de la persona.
- **o** (*organitzation*: és l'organització o companyia a la qual pertany aquesta persona.

- **u** (*organizational unit*): és el departament de l'organització o companyia on treballa aquesta persona.
- **mail**: és l'adreça de correu electrònic personal.

A més a més d'aquestes claus, n'hi pot haver d'altres sempre que siguin necessàries. Amb tot això, un exemple de DN ('nom distingit'), prendria la forma:

```
uid=jeapil,cn=pillou,givenname=jean—francois
```

El RDN ('nom distingit relatiu') seria:

```
uid=jeapil
```

En general, els usuaris en un domini LDAP tindran un nom distingit que consistirà en el seu **uid**, més el nom del domini més l'extensió d'aquest.

La col·lecció d'objectes i definicions d'atributs que un servidor LDAP pot gestionar s'anomena *esquema*. Això fa possible definir si un atribut pot tenir un valor o més, o fer que aquest sigui obligatori o opcional.

LDAP ens dóna tot un conjunt de funcions (o procediments) per tal de dur a terme consultes en les dades desades en el servidor, com per exemple cercar, modificar i eliminar entrades en el directori.

En la taula 1.1, es mostren les operacions principals que es poden dur a terme amb LDAP:

TAULA 1.1. Operacions que podem dur a terme amb LDAP

Operació	Descripció
Abandon	Abandonar l'operació prèvia enviada al servidor.
Add	Afegir una entrada al directori.
Bind	Iniciar una nova sessió en el servidor LDAP.
Compare	Comparar les entrades en un directori en funció dels criteris.
Delete	Esborrar una entrada d'un directori.
Extended	Dur a terme operacions esteses.
Rename	Canviar el nom d'una entrada.
Search	Cercar entrades en un directori.
Start TLS	Fer servir l'extensió de seguretat TLS (*transport layer security*, 'seguretat de capa de transport') de la versió 3 per obtenir una connexió segura.
Unbind	Aturar la sessió en el servidor LDAP.

LDAP també ens dóna un format d'intercanvi de dades (LDIF: *lightweight data interchange format*), que permet exportar i importar dades des d'un directori o cap a aquest fent servir un fitxer de text simple. La majoria de servidors LDAP suporten aquest format, fet que permet un grau d'interoperabilitat molt gran entre ells.

La sintaxi d'aquest format és la següent:

```
[<id>]
   dn: <nom distingit>
   <attribut>: <valor>
   <attribut>: <valor>
   ...
```

Exemple de LDAP

```
   dn: cn=John Doe,dc=example,dc=com
   cn: John Doe
   givenName: John
   sn: Doe
   telephoneNumber: +1 888 555 6789
   telephoneNumber: +1 888 555 1232
   mail: john@example.com
   manager: cn=Barbara Doe,dc=example,dc=com
   objectClass: inetOrgPerson
   objectClass: organizationalPerson
   objectClass: person
   objectClass: top
```

on

- **dn**: és el nom distingit de l'entrada (nom complet, com si fos un directori absolut si parléssim de fitxers). No és cap atribut ni forma part de l'entrada.
- **cn=John Doe**: és l'entrada RDN ('nom relatiu distingit').
- **dc=example, dc=com**: són els noms distingits de l'entrada pare, on **dc** significa 'component de domini' (*domain component*).
- La resta de línies són atributs en aquesta entrada, que habitualment fan servir cadenes mnemotècniques per tal de recordar més fàcilment el significat: "cn" per 'nom comú', "dc" per 'component de domini', "mail" per 'correu electrònic' i "sn" per 'cognom'.

En aquest fitxer l'identificador (id) és opcional; és un nombre enter positiu que permet identificar cada entrada a la base de dades.

En relació amb aquest tipus de fitxers LDIF, cal tenir en compte que:

- Cada nova entrada ha d'estar separada de l'anterior mitjançant una línia buida.
- Es pot definir un atribut que ocupi diverses línies sempre que a partir de la segona línia es comenci amb un espai en blanc o una tabulació.
- Es poden definir diversos valors per un atribut repetint la cadena de caràcters nom: valor en línies separades.
- Quan el valor conté un caràcter especial (no imprimible, espai en blanc o dos punts), l'atribut ha d'anar seguit per **::** si el valor és codificat en base 64.

Un servidor emmagatzema un subarbre que comença a partir d'una entrada específica (per exemple, "dc=example, dc=com"), i tots els seus fills. els servidors també poden tenir referències a altres servidors, de manera que un intent d'accés a "ou=department, dc=example, dc=com" pot resultar en un redireccionament a

un altre servidor que conté aquesta part de l'arbre de directori. Si és així, el client pot contactar amb l'altre servidor.

Alguns servidors suporten encadenament; és a dir, un servidor pot contactar amb un altre i retornar el resultat al client.

Normalment, LDAP no defineix cap ordre en concret. Així, un servidor pot tornar valors d'un atribut, els atributs d'una entrada i les entrades trobades a partir d'una operació de cerca en qualsevol ordre.

1.1.3 Dominis, subdominis

Per entendre el funcionament de l'autenticació d'usuaris en xarxes GNU/Linux cal conèixer el significat del concepte *domini/subdomini* i la traducció d'aquest concepte en sistemes GNU/Linux.

També és imprescindible saber com funciona el sistema de gestió d'usuaris i grups en els sistemes GNU/Linux i el procés de configuració de l'autenticació d'usuaris en una xarxa formada per xarxes GNU/Linux.

El terme *domini* pot fer referència a dos conceptes:

- Domini d'Internet.
- Domini local, d'administració de sistemes.

Un domini d'Internet és una estructura jeràrquica de noms separats per punts que, per mitjà dels servidors de noms de domini, permet determinar la ubicació (adreça IP) d'un equip connectat a Internet.

Cada nom de l'estructura determina un servidor DNS que coneix l'adreça IP de l'equip amb el nom anterior en l'estructura (excepte el primer nom que determina el node en qüestió). L'objectiu, juntament amb el servei de noms de domini, és traduir les adreces IP dels nodes actius de la xarxa en paraules més fàcils de recordar per a les persones.

Des del punt de vista de l'administració de sistemes, un domini local constitueix un conjunt d'equips interconnectats en una xarxa local que comparteixen informació administrativa centralitzada (usuaris, grups, contrasenyes...). Aquesta informació es fa servir per poder autenticar-se i crear un entorn inicial de treball per als usuaris que, segons els permisos que tinguin, podran accedir als recursos que proporciona el sistema.

L'autenticació per mitjà de la xarxa en sistemes GNU/Linux requereix fonamentalment la disponibilitat d'almenys un o diversos ordinadors que emmagatzemin

físicament aquesta informació i que la comuniquin a la resta de màquines connectades en xarxa, quan calgui, mitjançant un esquema client-servidor.

Per exemple, quan un usuari vol iniciar una sessió en qualsevol ordinador client del grup d'autenticació (domini), aquest ordinador haurà de validar les dades de l'usuari en el servidor i obtenir del mateix servidor tota la informació necessària per poder crear el context inicial de treball per a l'usuari.

> Un subdomini és un nivell de classificació jeràrquica dels noms de domini, definits amb finalitats administratives o organitzatives. Es podria considerar com un domini de segon nivell. Normalment, es tracta d'una sèrie de caràcters o d'una paraula, que s'escriu a l'esquerra del domini i separat per un punt.

A nivell d'Internet es pot dir que el subdomini s'utilitza per referir-se a una adreça web que treballa com un annex (o lloc relacionat) d'un domini principal. Per exemple, un subdomini es pot representar de la manera següent:

```
1 http://subdomini.domini_principal.com/
2 http://www.domini_principal.org/subdomini/
```

Dintre de l'estructura del servidor es reflecteix com un directori, el qual conté la informació per mostrar.

Els subdominis són definits per les mateixes empreses que realitzen l'allotjament del servei web. Es pot tractar tant de la mateixa empresa interessada com d'una empresa especialitzada a oferir serveis d'hostatge (*hosting*) per a tercers. En aquest últim cas, hi pot haver unes certes limitacions, tant pel nombre de subdominis permesos com pel tipus de servei que ofereixen. Per exemple, hi ha empreses que regalen un subdomini en el moment de registrar un bloc amb ells, o d'altres ofereixen serveis d'hostatge gratuït.

A nivell local, un subdomini seria una subdivisió d'un domini amb finalitats organitzatives, per tal de facilitar la gestió i administració del domini principal. Podem pensar que un subdomini és equivalent a un departament dins d'una empresa gran.

1.2 Disseny del domini

Dissenyar un domini implica fer una planificació anticipada de la forma que tindrà. Habitualment, els dominis es representen en forma d'arbre (si més no, la implementació d'aquests mitjançant el protocol LDAP). Per tant, abans de començar, hem de pensar quina forma tindrà aquest arbre, és a dir, si hi haurà subdominis, quines branques tindrà, quins usuaris i quins grups d'usuaris contindrà.

En qualsevol cas, a l'inici del disseny, l'administrador haurà de pensar en quins

departaments ha de dividir el domini, i quins usuaris corresponen a cadascun d'aquests departaments.

Per tal d'entendre i seguir les explicacions d'aquests materials, haurem de fixar un disseny concret, que serà el que haurem de tenir en ment per tal d'implementar-lo, i seguir totes les passes necessàries per implementar-lo. És impossible de seguir amb la implantació d'un domini, si no tenim enllestit aquest domini, o si més si no tenim un esboç dels elements principals de què ha de constar.

En un domini creat emb LDAP, tenim una sèrie d'elements que són prefixats:

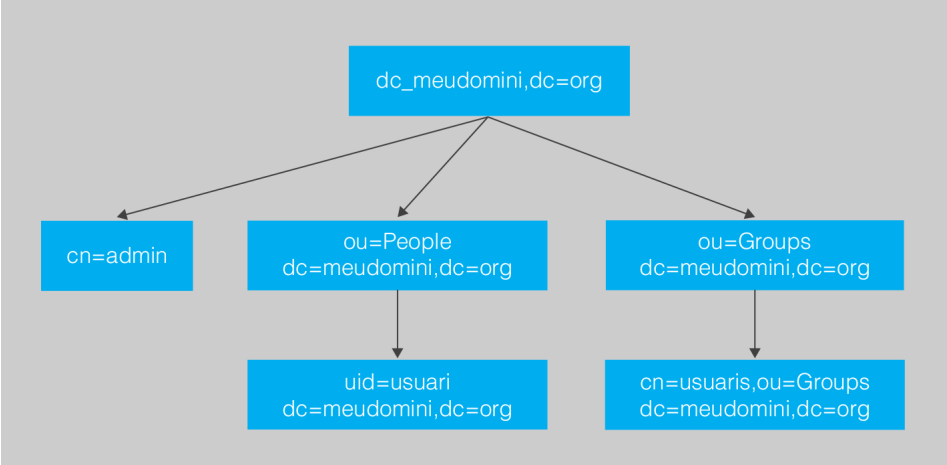
- **Usuari administrador (cn=admin)**: és l'usuari amb drets d'administració que pot crear, eliminar i modificar els usuaris i els grups del domini.
- **Unitat organitzativa People (ou=People)**: aquesta unitat organitzativa inclou tots els usuaris individuals del domini, que es distingeixen els uns dels altres mitjançant el seu identificador (uid).
- **Unitat organitzativa Groups (ou=Groups)**: aquesta unitat organitzativa inclou tots els grups d'usuaris. És molt important agrupar els usuaris en funció de característiques semblants, per tal de simplificar-ne la gestió. Així, podem agrupar els usuaris en funció dels drets i dels permisos d'accés a objectes del domini. Cal dir que els grups del domini s'han de crear abans que els usuaris individuals, perquè d'aquesta manera simplifiquem el procés de creació d'usuaris. Un cop s'han creat els grups del domini, quan creem l'usuari, el podem assignar directament a un determinat grup sense haver de fer cap altre pas posterior. Si quan creem els usuaris no s'han creat els grups d'usuaris prèviament, hauríem de crear aquests grups posteriorment, i després hauríem d'editar les propietats dels usuaris un per un, per tal d'assignar-los a un grup concret.

Dins dels elements que no són prefixats, haurem d'escollir:

- **Nom del domini**: és un nom distingit, format pel nom pròpiament dit, i la seva extensió. Crearem un domini amb el nom **meudomini** i extensió **org**, per tant, el nom distingit del domini serà **dc=meudomini, dc=org**.
- **Nom del grup d'usuaris**: escollirem com a nom del grup **usuaris**, i el nom distingit corresponent serà **cn=usuaris, ou=Groups, dc=meudomini, dc=org**.
- **Nom d'usuari** : per tal que el domini tingui un mínim de funcionalitat, i puguem realitzar alguna prova, haurem de crear com a mínim un usuari del domini. Aquest usuari tindrà com a nom **usuari**, i penjarà de la unitat organitzativa **People**. El seu nom distingit complet serà **uid=usuari, dc=meudomini, dc=org**.

Seguint aquestes orientacions, podeu veure l'esquema dels objectes mínims del domini en forma d'arbre en la figura 1.1.

FIGURA 1.1. Esquema del domini



Representació en forma d'arbre dels objectes del domini descrits

1.2.1 Anàlisi dels requeriments

A l'hora de dissenyar un domini, com a mínim, hem d'especificar:

- Extensió del domini: que correspon en el model ldap a un component de domini. Aquesta extensió pot tenir el valor .com, .org, etc. i l'indiquem mitjançant **dc=com**, **dc=org**, etc.
- Nom del domini: també correspon a un component del domini. Pot tenir el valor que vulguem; en qualsevol cas, ha de començar amb un caràcter, i ha de tenir un cert significat. Per exemple, pot ser: meudomini, dominiexemple, etc. i l'indiquem mitjançant **dc=meudomini**, **dc=dominiexemple**, etc.
- La unitat organitzativa **People**: contindrà tots els usuaris individuals del sistema, i s'indica mitjançant **ou=People**.
- Els usuaris del sistema, que en la representació gràfica, són fills de la unitat organitzativa People. Cadascun dels usuaris s'ha d'identificar unívocament mitjançant un identificador d'usuari. Per exemple, en el protocol LDAP, un usuari anomenat *pepet* s'indicaria de la manera següent: **uid=pepet**.
- La unitat organitzativa **Group**: conté unitats organitzatives que serveixen per agrupar els usuaris del sistema mitjançant grups. En la implementació LDAP s'anomena **ou=Group**.
- Els grups d'usuari del sistema: en la representació gràfica, són fills de la unitat organitzativa Group. Cadascun dels grups d'usuaris s'identifica unívocament amb un nom de grup. Per exemple, el grup d'usuaris desenvolupadors s'identificaria mitjançant un nom comú (cn) de la forma **cn=desenvolupadors**.

Requeriments de maquinari

Qualsevol ordinador pot fer de servidor, però és convenient que si emmagatzema informació important tingui maquinari tolerant a errors, com ara fonts d'alimentació redundant o sistemes de discos en RAID

A més de tots aquests requeriments de planificació, també tenim una sèrie de requeriments de maquinari i programari:

- **Sistema operatiu**: un sistema operatiu que suporti la implementació de LDAP. Si ens fixem en la implementació OpenLDAP, aleshores ens pot servir qualsevol distribució de GNU/Linux. En el nostre cas utilitzarem **Ubuntu Server 10.04 LTS**.
- **Ordinador servidor**: és necessari un ordinador que suporti el sistema operatiu de xarxa. En el cas d'Ubuntu Server 10.04 LTS, si no utilitzem un entorn gràfic, els requeriments mínims del sistema són els que podem veure en la taula 1.2.
- **Ordinadors clients**: han d'estar connectats mitjançant una xarxa al servidor. Per tal de facilitar-ne la configuració, és convenient que el seu sistema operatiu sigui el mateix que el del servidor (Ubuntu 10.04 LTS), si bé es poden utilitzar altres distribucions de GNU/Linux i, fins i tot, és possible fer servir ordinadors que funcionin amb sistemes operatius de la família Windows.

  En cas que utilitzem com a sistema operatiu dels clients Ubuntu 10.04 (edició d'escriptori), hi ha els requeriments que es mostren en la taula 1.3. Podem observar que els requeriments de l'edició d'escriptori són força més elevats que la versió de servidor, suposant que el servidor només s'hi instal·li l'intèrpret de ordres en mode text.
- **Altres elements necessaris per crear la xarxa**: commutadors (*switches*), encaminadors (*routers*), armaris, cablejat, etc.

TAULA 1.2. 04 LTS

Element	Requeriment
Processador (x86) amb el joc d'instruccions i686	300 MHz
Memòria RAM	128 MB (megabytes)
Disc dur (o espai lliure)	1 GB (gigabyte)
Resolució monitor	VGA (640 x 480 píxels)

TAULA 1.3. 04 LTS edició d'escriptori

Element	Requeriment
Processador (x86) amb el joc d'instruccions i686	1 GHz
Memòria RAM	512 MB (megabytes)
Disc dur (o espai lliure)	5 GB (gigabytes)
Resolució monitor	VGA (1024x768)

1.2.2 Implementació

Per tal d'implementar el domini de LDAP, suposarem que ja tenim instal·lat un sistema **Ubuntu Server 10.04 LTS** i que en coneixem la contrasenya d'administració. Cal recordar que, per fer tots aquests passos, ens cal ser usuari administrador del sistema, cosa que podem aconseguir obrint una consola del sistema, i executar l'ordre:

```
usuari@ubuntu-server~$sudo bash
[sudo] password for usuari :
root@ubuntu-server~#
```

Un cop hem iniciat l'intèrpret d'ordres com a usuari administrador (**root**), podrem fer tots els passos necessaris per implementar el domini mitjançant LDAP. Suposarem que volem crear un domini anomenat **meudomini.org**, i que la contrasenya de l'administrador és 123456. Vegem tot seguit els passos que hem de dur a terme:

1. Instal·lem el servidor:

```
apt-get install slapd ldap-utils
```

2. Instal·lem uns quants fitxers d'esquema:

```
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/cosine.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/nis.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/inetorgperson.ldif
```

3. Establim la contrasenya de l'LDAP (en l'exemple posem 123456):

```
slappasswd -h {CRYPT}:
New password: 123456
Re-enter new password: 123456
{CRYPT}aLJLqqUipInfk
```

4. Creem el fitxer `config.ldif` amb el contingut següent:

```
dn: cn=config
changetype: modify

dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootDN
olcRootDN: cn=admin,cn=config

dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {CRYPT}aLJLqqUipInfk

dn: olcDatabase={0}config,cn=config
changetype: modify
delete: olcAccess
```

En la línia que conté **olcRootPW** hem d'escriure el que retorna la instrucció **slappasswd -h {CRYPT}**

Algorismes d'encriptació

Un algorisme d'encriptació s'utilitza per codificar informació a fi que únicament hi puguin accedir les persones que en coneixen la clau per descodificar-la. Per encriptar les contrasenyes es fan servir diferents algorismes, com ara DES, MD5, SHA, . . .

5. Carreguem aquest fitxer de configuració en el servidor LDAP:

```
ldapadd -Y EXTERNAL -H ldapi:/// -f config.ldif
```

6. Creem el fitxer `backend.meudomini.org.ldif` amb el contingut següent:

```
# Load dynamic backend modules

dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulepath: /usr/lib/ldap
olcModuleload: back_hdb
# Database settings

dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcSuffix: dc=meudomini,dc=org
olcDbDirectory: /var/lib/ldap
olcRootDN: cn=admin,dc=meudomini,dc=org
olcRootPW: {CRYPT}aLJLqqUipInfk
olcDbConfig: set_cachesize 0 2097152 0
olcDbConfig: set_lk_max_objects 1500
olcDbConfig: set_lk_max_locks 1500
olcDbConfig: set_lk_max_lockers 1500
olcDbIndex: objectClass eq
olcLastMod: TRUE
olcDbCheckpoint: 512 30
olcAccess: to attrs=userPassword by dn="cn=admin,dc=meudomini,dc=org" write by
    anonymous auth by self write by * none
olcAccess: to attrs=shadowLastChange by self write by * read
olcAccess: to dn.base="" by * read
olcAccess: to * by dn="cn=admin,dc=meudomini,dc=org" write by * read
```

Hem de tornar a escriure la contrasenya encriptada mitjançant el mètode {CRYPT} en la línia que conté **olcRootPW**, i hem d'escriure el nom distingit de l'usuari administrador a la línia que conté **olcAccess**.

389 Directory Server

Les distribucions de GNU/Linux com ara Red Hat, CentOS, i Fedora disposen d'una interfície gràfica per dur a terme les tasques d'instal·lació i administració d'un domini, que s'anomena *Red Hat Directory Server* (en el cas de Red Hat), i 389 Directory Server en el cas de CentOS i Fedora.

7. Carreguem el fitxer ldif al directori:

```
ldapadd -Y EXTERNAL -H ldapi:/// -f backend.meudomini.org.ldif
```

8. Omplim el directori del *front-end*. Creem el fitxer `frontend.meudomini.org.ldif` amb el contingut següent:

```
# Create top-level object in domain

dn: dc=meudomini,dc=org
objectClass: top
objectClass: dcObject
objectclass: organization
o: Example Organization
dc: meudomini
description: Domini exemple LDAP meudomini
# Admin user.

dn: cn=admin,dc=meudomini,dc=org
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: administrador LDAP
userPassword: {CRYPT}aLJLqqUipInfk
```

```

dn: ou=people,dc=meudomini,dc=org
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=meudomini,dc=org
objectClass: organizationalUnit
ou: groups

dn: uid=usuari,ou=people,dc=meudomini,dc=org
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: usuari
sn: usuari
givenName: usuari
cn: usuari
displayName: usuari
uidNumber: 1000
gidNumber: 10000
userPassword: usuari
gecos: usuari
loginShell: /bin/bash
homeDirectory: /home/usuari
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: usuari@meudomini.org
postalCode: 31000
l: Manresa
o: Example
mobile: +34 (0)6 xx xx xx xx
homePhone: +34 (0)9 xx xx xx xx
title: System Administrator
postalAddress:
initials: usuari

dn: cn=meudomini,ou=groups,dc=meudomini,dc=org
objectClass: posixGroup
cn: example
gidNumber: 10000
```

9. Afegim les entrades al directori LDAP:

```
ldapadd -x -D cn=admin,dc=meudomini,dc=org -W -f frontend.meudomini.org.ldif
```

10. Comprovem que el contingut s'ha afegit satisfactòriament fent una cerca:

```
ldapsearch -xLLL -b "dc=meudomini,dc=org" uid=usuari sn givenName cn

dn: uid=usuari,ou=people,dc=meudomini,dc=org
sn: usuari
givenName: usuari
cn: usuari
```

11. Amb aquest pas ja hem fet la configuració bàsica del domini i n'hem creat els elements mínims. Si ho volem, per facilitar la tasca d'administració podem instal·lar phpladapadmin, mitjançant l'ordre:

phpLDAPadmin es pot fer servir des de qualsevol màquina amb qualsevol sistema operatiu que tingui un navegador web, i que estigui connectada en xarxa al servidor.

```
apt-get install phpldapadmin
```

12. Editem el fitxer de configuració, per exemple, amb l'editor nano:

```
nano /etc/phpldapadmin/config.php
```

13. Cerquem les línies següents:

```
$servers->setValue('server','base',array('dc=example,dc=com'));
$servers->setValue('login','bind_id','cn=admin,dc=example,dc=com');
```

14. Les substituïm per aquestes:

```
$servers->setValue('server','base',array('dc=meudomini,dc=org'));
$servers->setValue('login','bind_id','cn=admin,dc=meudomini,dc=org');
```

15. Reiniciem el servidor web apache:

```
/etc/init.d/apache2 restart
```

16. Accedim a phpldapadmin iniciant un navegador i escrivint la URL següent a la barra de navegació:

http://127.0.0.1/phpldapadmin

Autenticació amb LDAP

Un cop tenim el servidor LDAP funcionant, podem configurar el client, per tal que els usuaris que hem creat amb LDAP puguin iniciar la sessió en el servidor. El client pot ser el mateix servidor o un altre ordinador connectat a ell mitjançant la xarxa. Per fer això cal seguim els passos següents:

1. Instal·lem els paquets **auth-client-config** i **libnss-ldap** que faciliten l'autenticació d'un client Ubuntu en un servidor LDAP. Per fer-ho, hem d'escriure en una consola:

```
apt-get install libnss-ldap auth-client-config
```

2. Ens demanarà l'adreça del servidor LDAP. Contestem:

```
ldapi:///127.0.0.1
```

Connexió d'altres clients per xarxa

En cas que ens connectem al servidor LDAP mitjançant un client connectat en xarxa, hem de modificar **127.0.0.1**, o **localhost**, per l'adreça IP del servidor; la resta de la configuració és la mateixa que si ho fem localment.

3. Tot seguit escrivim el nom distingit del domini i l'extensió corresponent:

```
dc=meudomini,dc=org
```

4. Ens demana quina versió de l'LDAP farem servir; escollim la versió 3.

5. Ens demana si el *root* local ha de ser administrador de l'LDAP; contestem que sí.

6. Pregunta si necessitem autenticar per accedir a les entrades de la base de dades; contestem l'opció per defecte (no).

7. Ens demana el compte que s'ha de fer servir quan el *root* canviï una contrasenya. Contestem:

```
dc=admin,dc=meudomini,dc=org
```

8. Escrivim la contrasenya de *root*, i s'acaba la configuració del paquet.

9. Un cop hem configurat **libnss-ldap**, habilitem el perfil LDAP del paquet **auth-client-config** LDAP escrivint:

```
auth-client-config -t nss -p lac_ldap
```

Podem veure el significat dels paràmetres d'aquesta instrucció en la taula 1.4.

TAULA 1.4. Paràmetres de auth-client-config

Paràmetre	Significat
-t	Només modifica el fitxer /etc/nsswitch.conf.
-p	Nom del perfil que s'ha d'habilitar o deshabilitar.
lac_ldap	El perfil de auth-client-config que és part del paquet ldap-auth-config

10. Fent servir la utilitat **pam-auth-update** configurem el sistema perquè faci servir autenticació via LDAP:

```
pam-auth-update
```

11. En el menú de configuració de la utilitat, habilitem com a mínim l'autenticació LDAP.

12. Ens assegurem que tenim habilitat el connector (*plug-in*) **pam_mkhomedir**, perquè, quan un usuari s'autentiqui via LDAP, es creï automàticament el seu directori personal (si no, no podrà iniciar la sessió). Per fer-ho, comprovem que el fitxer pam_mkhomedir.so està en el directori `/lib/security`.

13. Cerquem dins dels fitxers `/etc/pam.d/gdm` i `/etc/pam.d/login` les línies que comencen per:

```
session . . .
```

I hi afegim la línia:

```
session required /lib/security/pam_mkhomedir.so skel=/etc/skel umask=0022
```

Assegurament de l'autenticació mitjançant TLS i SSL

TLS i SSL

secure sockets layer, 'protocol de capa de connexió segura (SSL) i *transport layer security*, 'seguretat de la capa de transport' (TLS), que n'és el successor, són protocols criptogràfics que proporcionen comunicacions segures en una xarxa, que habitualment és Internet.

Quan un usuari s'autentiqui en un servidor OpenLDAP, és aconsellable fer-ho amb una sessió encriptada. Això es pot aconseguir utilitzant el protocol TLS ('capa de transport segura') i el protocol SSL ('capa de sòcols segura'). Per a això, hem de seguir una sèrie de passos que detallem tot seguit:

1. Primer de tot, hem d'obtenir o crear un certificat. Com que el domini de LDAP (slapd) està compilat utilitzant la llibreria gnutls, és aconsellable fer servir la

utilitat certtool per crear aquest certificat. Instal·lem **gnutls-bin** mitjançant l'ordre següent:

```
apt-get install gnutls-bin
```

2. Tot seguit, creem la clau privada per un certificat d'autoritat (CA):

```
sh -c "certtool --generate-privkey > /etc/ssl/private/cakey.pem"
```

3. Creem el fitxer `/etc/ssl/ca.info` que, automàticament, signarà el certificat d'autoritat (CA), amb el contingut següent:

```
cn = Example Company
ca
cert_signing_key
```

4. Creem el certificat d'autoritat autosignat:

```
certtool --generate-self-signed --load-privkey \
/etc/ssl/private/cakey.pem --template \
/etc/ssl/ca.info --outfile /etc/ssl/certs/cacert.pem
```

5. Creem una clau privada per al servidor:

```
sh -c "certtool --generate-privkey > /etc/ssl/private/ldap01_slapd_key.pem"
```

Per facilitar les coses, cal reemplaçar **ldap01** en el nom del fitxer amb el nom de l'amfitrió del servidor.

6. Per tal de signar el certificat del servidor amb el certificat d'autoritat (CA), creem el fitxer `/etc/ssl/ldap01.info` amb el contingut següent:

```
organization = Example Company
cn = ldap01.meudomini.org
tls_www_server
encryption_key
signing_key
```

7. Creem el certificat del servidor:

```
certtool --generate-certificate --load-privkey \
/etc/ssl/private/ldap01_slapd_key.pem \
--load-ca-certificate /etc/ssl/certs/cacert.pem \
--load-ca-privkey /etc/ssl/private/cakey.pem \
--template /etc/ssl/ldap01.info \
--outfile /etc/ssl/certs/ldap01_slapd_cert.pem
```

8. Un cop tenim un certificat, una clau i un certificat d'autoritat instal·lats, fem servir l'eina **ldapmodify** per afegir les noves opcions de configuració:

```
ldapmodify -Y EXTERNAL -H ldapi:///

Enter LDAP Password:
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/cacert.pem
-
```

```
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/ldap01_slapd_cert.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/ldap01_slapd_key.pem

modifying entry "cn=config"
```

Cal modificar el nom dels fitxers `ldap01_slap_cert.pem`, `ldap01_slapd_key.pem` i `cacert.pem`, si els que hem utilitzat són diferents.

9. Tot seguit, editem el fitxer `/etc/default/slapd` i descomentem (traiem el símbol # del principi de la línia) de l'opció SLAPD_SERVICES:

```
SLAPD_SERVICES="ldap:/// ldapi:/// ldaps:///"
```

10. Ara, els usuaris d'openldap necessiten accedir al servidor per mitjà del certificat:

```
adduser openldap ssl-cert
chgrp ssl-cert /etc/ssl/private/ldap01_slapd_key.pem
sudo chmod g+r /etc/ssl/private/ldap01_slapd_key.pem
```

Si els fitxers `/etc/ssl/private` i `/etc/ssl/private/server.key` tenen permisos diferents, ajustem les instruccions de la manera adient.

11. Per acabar, reiniciem el domini slapd:

```
/etc/init.d/slapd restart
```

Fet això, el domini de slapd hauria d'escoltar les connexions LDAPS i ser capaç d'utilitzar STARTTLS durant l'autenticació.

1.2.3 Documentació

Per comprendre i poder mantenir fàcilment el funcionament d'un domini, cal tenir una bona documentació que reflecteixi tots els elements que en formen part.

De fet, els documents que parlen de l'arquitectura d'un domini són uns dels més estesos, però, al mateix temps, sovint no són massa ben entesos ni queda clar què han de contenir.

De vegades, aquests documents no estan ordenats, i es troben en estats d'elaboració diferents: alguns són esborranys, d'altres són complets però no estan actualitzats, d'altres contenen informació no rellevant.

En qualsevol cas, a l'hora d'elaborar aquesta documentació ens hem de fixar a qui s'adreça i també ens hem d'assegurar que es pot mantenir actualitzada. Hem de tenir en compte a qui va destinat cada document, i estructurar la documentació de manera adequada. Vegem diferents aspectes que hem de considerar a l'hora d'elaborar-la:

Eines informàtiques

Per realitzar l'esquema del domini podem utilitzar qualsevol programa de creació de dibuixos, com ara l'OpenOffice Draw. Per crear esquemes visuals de la xarxa podem fer servir eines en línia gratuïtes, com, per exemple, Pàgina web Gliffy

- Les audiències principals a les quals s'adreça la documentació del domini és el seu administrador, i el grup de suport corresponent. En aquest tipus de document es pot utilitzar terminologia tècnica.
- El contingut primari de la documentació són els principis de disseny, les categories, els grups, els usuaris, etc.
- El contingut ha de ser descriptiu, però al mateix temps no s'ha de convertir en una guia d'aprenentatge llarga; no es tracta de documents educacionals.
- Per dur-ne a terme l'elaboració, serà necessària la col·laboració entre diferents departaments de l'organització.
- Els diversos documents que realitzem poden tenir nivells d'especificacions i detall diferents; per tant, no cal que siguin tots iguals.

OCS

http://www.ocsinventory-ng.org/

Open computer and software inventory next generation ('inventari de maquinari i programari obert de nova generació') és una aplicació dissenyada per facilitar a un administrador d'una xarxa el manteniment de l'inventari dels ordinadors i el programari instal·lats en aquesta xarxa.

En qualsevol cas, una bona documentació referent a un domini ha de recollir els aspectes següents:

- Un inventari de tot el maquinari instal·lat en el domini. Això inclou les configuracions de maquinari dels diversos clients, com del servidor (microprocessador, memòria RAM, disc dur...). També ha d'incloure tot el maquinari de xarxa com ara encaminadors, commutadors i altres elements (impressores, NAS, projectors, escàners...).
- Un inventari amb tots els sistemes operatius instal·lats i els ordinadors als quals corresponen. La configuració de xarxa corresponent, incloent-hi la IP i el nom de cada amfitrió.
- Un esquema visual de la xarxa, que permet analitzar i planificar millores sobre aquesta xarxa.
- Un inventari del programari instal·lat en el domini, tant en el servidor de domini com en les màquines client. Això hauria d'incloure una llista detallada de tots els sistemes operatius i les aplicacions instal·lades en cada node de la xarxa, i la versió corresponent. D'aquesta manera, l'administrador del domini pot veure si el programari dels clients del domini està actualitzat o no.
- Una llista on constin el nom de tots els elements del domini, amb el nom distingit corresponent. Això inclou el nom del domini, l'extensió, l'usuari administrador, les unitats organitzatives, els usuaris i els grups.
- Un esquema visual en forma d'arbre del domini.
- També cal tenir una llista de totes les contrasenyes actualitzades, documentació que només ha de ser accessible per l'usuari administrador del domini.

Val a dir que, per dur a terme aquesta tasca, disposem d'un conjunt d'eines informàtiques que permeten crear esquemes de xarxes, esquemes visuals genèrics (per crear l'esquema del domini) i programari que permet crear inventaris del maquinari instal·lat a la xarxa d'una manera automatitzada.

2. Administració de comptes i grups LDAP

L'administració de comptes i grups LDAP consisteix en la gestió, creació, eliminació i personalització dels comptes d'usuaris i grups del servidor de directori de LDAP. Val a dir que podem dur a terme aquestes tasques d'administració utilitzant l'edició i importació de fitxers ldif utilitzant la consola (interfície en mode text), però aquest mètode és més propens a errors, és feixuc i els resultats que obtenim són els mateixos que si fem servir eines més visuals i intuïtives.

Fitxers LDIF

Una manera més complexa, però igualment vàlida, de gestionar usuaris i grups LDAP és fer-ho mitjançant els fitxers LDIF, (*LDAP data interexchange format*), que és un estàndard de fitxer de text pla per representar contingut del directori LDAP i actualitzacions d'aquest contingut.

Per dur a terme l'administració d'usuaris i grups del servei LDAP, i facilitar la tasca de l'administrador, utilitzarem l'eina **phpLDAPadmin**.

phpLDAPadmin és un client d'LDAP basat en una interfície web. Ens permet una administració fàcil, accessible des de qualsevol lloc, del servidor LDAP.

phpLDAPadmin és un client de l'LDAP basat en una interfície web que permet una administració senzilla del servidor LDAP utilitzant un navegador web, d'una manera local, per mitjà d'una xarxa d'àrea local o per Internet.

phpLDAPadmin mostra la jerarquia d'objectes del servidor de LDAP en forma d'arbre i permet fer cerques avançades i intuïtives. A més a més, com que és una aplicació web, permet funcionar sobre moltes plataformes diferents.

2.1 Administració de comptes LDAP

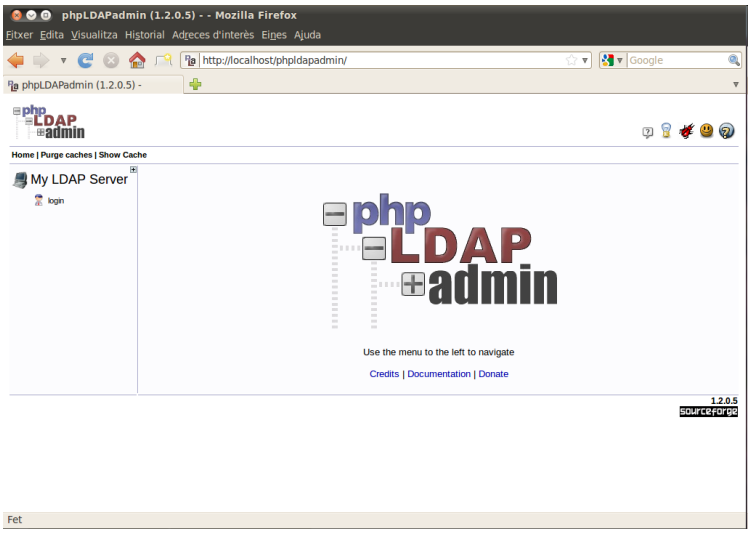
En aquest apartat gestionarem els comptes d'usuari del servidor de LDAP, incloent-hi altes, baixes i modificacions d'aquests comptes. Per poder dur a terme aquestes tasques d'administració, el primer pas consistirà a connectar-se al servidor de LDAP utilitzant phpLDAPadmin: ens caldrà obrir un navegador, tant si és en l'ordinador on tenim instal·lat el servidor de LDAP com en un altre ordinador connectat al servidor per xarxa.

En la barra d'adreces del navegador, hi escrivim l'adreça **http://localhost/phpldapadmin/**, si ho fem des del mateix servidor, i **http://ip_del_servidor/phpldapadmin**, si ho fem remotament per mitjà d'una xarxa.

Fent això, ens apareixerà la pantalla inicial de phpLDAPadmin, com podeu veure en la figura 2.1.

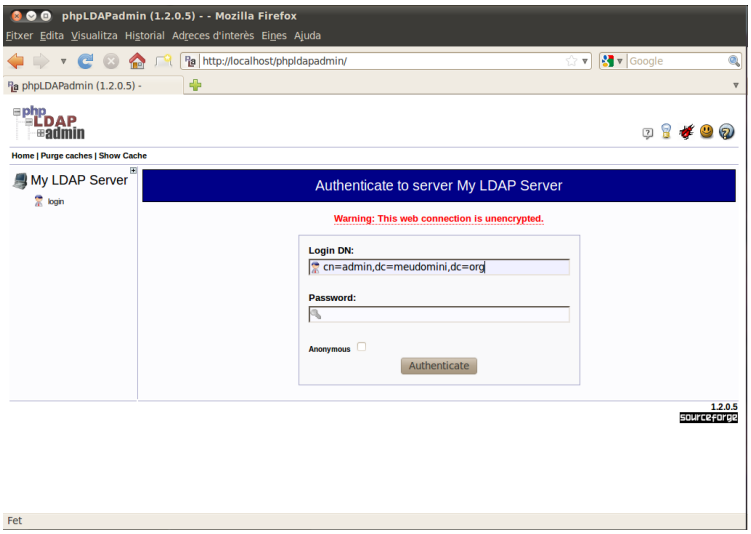
Prement l'enllaç *entrada* (*login*), podem escriure les credencials (el nom distingit o DN) de l'administrador del servidor LDAP, i la contrasenya, com veieu en la figura 2.2. Cal dir que, si hem creat de manera correcta el domini, i l'usuari admin, el nom distingit d'aquest apareixerà automàticament en la caixa de text anomenada **Login DN**. Si no és així, ens pot indicar que s'ha produït algun error a l'hora de configurar el domini.

FIGURA 2.1. Pantalla inicial phpLDAPadmin



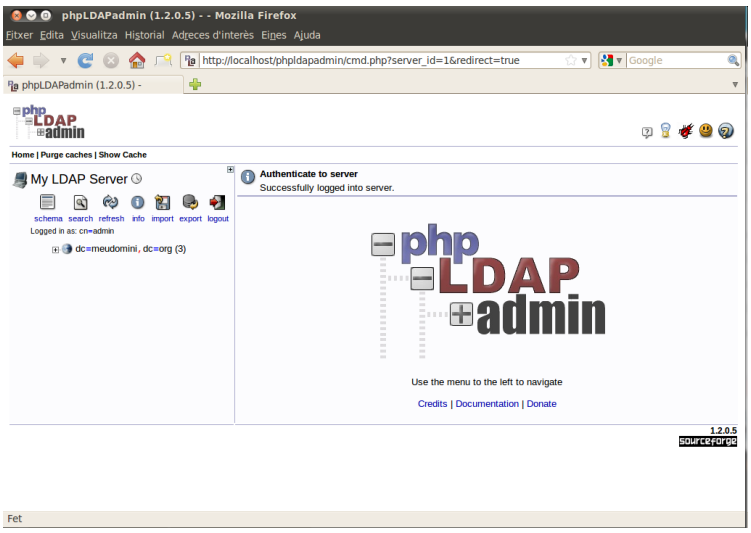
Interfície web d'administració del servidor LDAP

FIGURA 2.2. Finestra d'entrada de phpLDAPadmin



Cal escriure el nom distingit de l'usuari admin, i la contrasenya corresponent

FIGURA 2.3. Finestra inicial de phpLDAPadmin



Aspecte que mostra phpLDAPadmin un cop hem inserit les credencials de l'usuari admin.

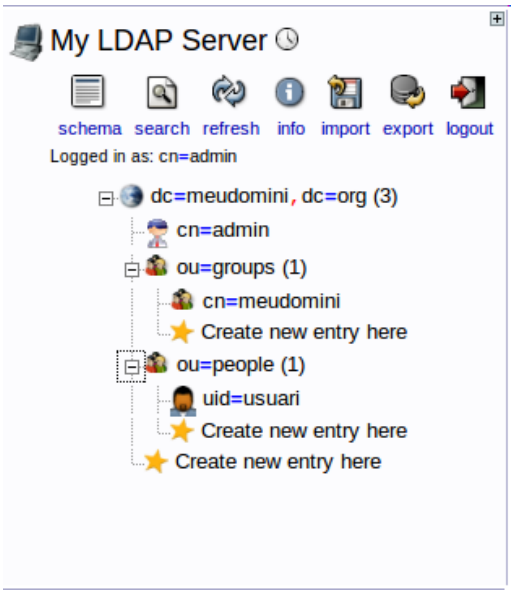
Un cop escrit el nom distingit de l'usuari admin, i la contrasenya, entrem a la interfície d'administració del servidor de LDAP via web, i podem veure el nom del domini i l'extensió que té, com mostra la figura 2.3.

Podem expandir l'arbre del directori del servidor de LDAP prement l'enllaç simbolitzat amb el símbol **+** i, d'aquesta manera, visualitzarem els objectes que hem generat a l'hora de crear el domini. Ho podeu veure en la figura 2.4.

Assegurant phpLDAPadmin

Si tenim un servidor web segur (que utilitzi certificats SSL), s'hauria de configurar per forçar l'aplicació phpLDAPadmin perquè faci servir el mode SSL i així mantenir-la segura.

FIGURA 2.4. Arbre del directori LDAP



Es mostren tots els objectes que hem creat en el domini.

2.1.1 Comptes predeterminats

Per crear un domini de LDAP és del tot imprescindible crear un usuari administrador. Per tant, podem dir que en la definició d'un domini de LDAP només hi ha un usuari predeterminat, que és l'usuari **admin** (administrador). Tots els altres usuaris es creen posteriorment.

Així doncs, la creació de l'usuari admin es fa al mateix temps que la creació del domini, mitjançant la importació del fitxer ldif corresponent. Per exemple, si creem un domini que tingui per nom **meudomini.org**, la creació de l'usuari admin es realitza quan s'importa el fitxer **frontend.meudomini.org.ldifv**, concretament, en les línies següents:

```
# Admin user.
   dn: cn=admin,dc=meudomini,dc=org
   objectClass: simpleSecurityObject
   objectClass: organizationalRole
   cn: admin
   description: administrador LDAP
   userPassword: {CRYPT}aLJLqqUipInfk
```

2.1.2 Contrasenyes

Per a l'establiment de les contrasenyes dels usuaris hem de distingir dos casos diferenciats: d'una banda tenim l'usuari administrador i, de l'altra, la resta dels usuaris.

L'establiment de la contrasenya de l'usuari administrador s'ha de dur a terme alhora que es crea el domini, i es realitza mitjançant l'ordre **slappasswd**. Haurem d'utilitzar el modificador -h juntament amb l'algorisme d'encriptació que volem. Per exemple, l'execució de l'ordre següent:

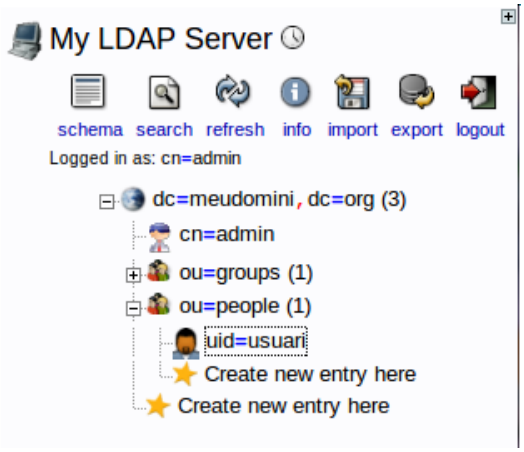
```
slappasswd –h {CRYPT}:
New password: 123456
Re–enter new password: 123456
{CRYPT}aLJLqqUipInfk
```

Establirà la contrasenya de l'usuari administrador del domini de LDAP en 123456 utilitzant el mètode d'encriptació CRYPT.

Aquest mètode d'encriptació correspon a la utilització de la funció d'encriptació de contrasenyes crypt, que està basada en l'algorisme estàndard d'encriptació de dades (DES), modificat de manera que faci difícil la cerca basada en maquinari de la clau d'encriptació.

Per tal d'establir la contrasenya de la resta d'usuaris del domini podem utilitzar l'eina gràfica phpLDAPadmin: primer de tot cal connectar-se com a usuari administrador del domini, desplegar l'arbre i seleccionar l'entrada corresponent a l'usuari. En aquest cas, hem suposat que ja havíem creat un usuari en el domini de LDAP anomenat **usuari**. Ho podeu veure en la figura 2.5.

Figura 2.5. Selecció de l'usuari en l'arbre del domini

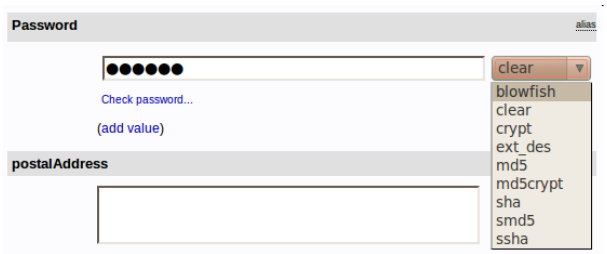


Un cop escollit l'usuari, hem de cercar la caixa de text que té per títol **Password**, i allà li podrem assignar la contrasenya que volem, tal com podeu veure en la figura 2.6.

FIGURA 2.6. Establiment de la contrasenya de l'usuari

Per defecte, la contrasenya de l'usuari s'estableix amb text pla, però si ho volem fer utilitzant el desplegable, que hi ha al costat dret de la caixa de text, podem escollir algun mètode d'encriptació de la contrasenya. Ho podeu veure en la figura 2.7.

FIGURA 2.7. Tria de la forma d'encriptació de la contrasenya



2.1.3 Bloquejos de comptes

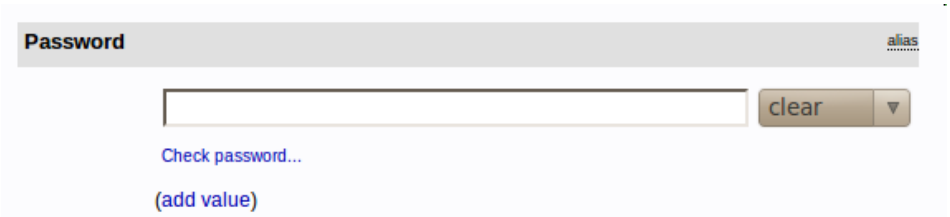
Bloquejos de comptes

Es bloquejos de compte són útils per evitar accessos que no volem als recursos del domini.

No hi ha cap manera automatitzada de bloquejar l'accés d'un usuari al servidor de LDAP. Una solució possible consisteix a iniciar la sessió en el phpLDAPadmin, com a usuari administrador, seleccionar l'usuari al qual volem bloquejar l'accés, deixar el camp de la contrasenya en blanc i actualitzar l'objecte.

D'aquesta manera, serà impossible que s'autentiqui i evitarem que pugui iniciar la sessió en el servidor. Ho podeu comprovar en la figura 2.8.

FIGURA 2.8. Eliminant la contrasenya de l'usuari

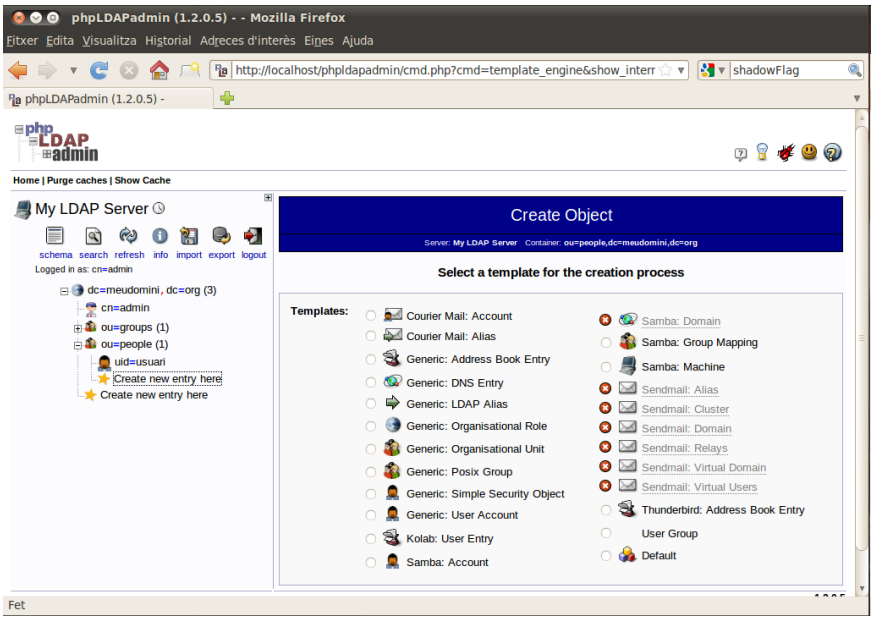


2.1.4 Comptes d'usuaris

Mitjançant phpLDAPadmin podem dur a terme tota la gestió d'usuaris en el nostre domini de LDAP: crear, eliminar i actualitzar les propietats d'un usuari determinat.

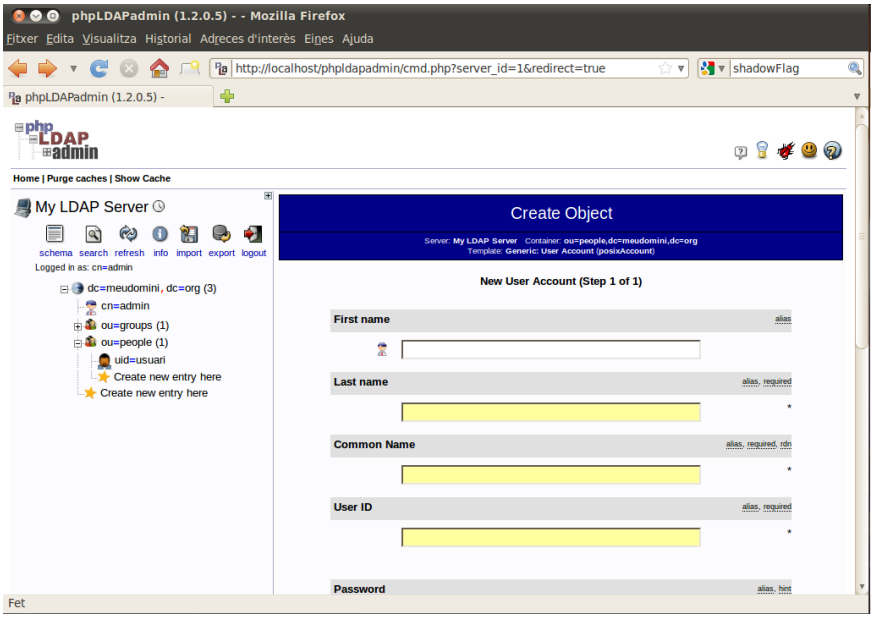
1. Creació d'un usuari. Per tal de crear un usuari nou, ens situem sota la unitat organitzativa **People** i cliquem a l'enllaç **Create new entry here**, tal com veieu en la figura 2.9.

FIGURA 2.9. Creació d'un nou usuari



Seleccionem l'opció **Generic: User Account**, i se'ns presentarà la finestra que podeu veure en la figura 2.10.

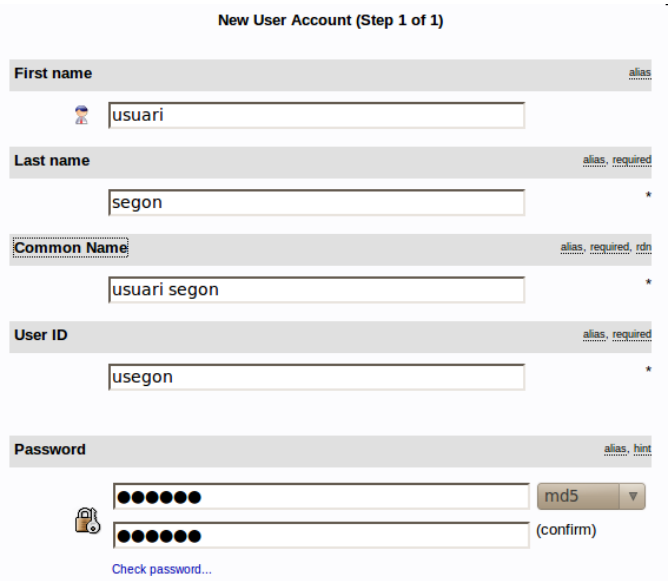
FIGURA 2.10. Creant un nou usuari



Les caixes de text que apareixen amb el fons de color groc s'han d'omplir obligatòriament. Cal dir que l'ID ('identificador d'usuari') es crea automàticament, concatenant la inicial del nom (*first name*) amb el cognom sencer (*last name*). El nom comú està format pel nom i el cognom sencers. Ho podeu veure en la figura 2.11.

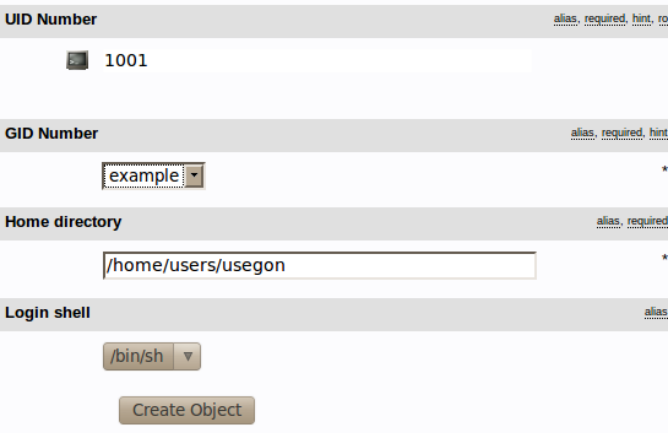
També podeu veure en la figura 2.11 com s'ha d'inserir la contrasenya dos cops per tal de confirmar-la, i hem de triar el mètode d'encriptació d'aquesta.

FIGURA 2.11. Nom i contrasenya del nou usuari



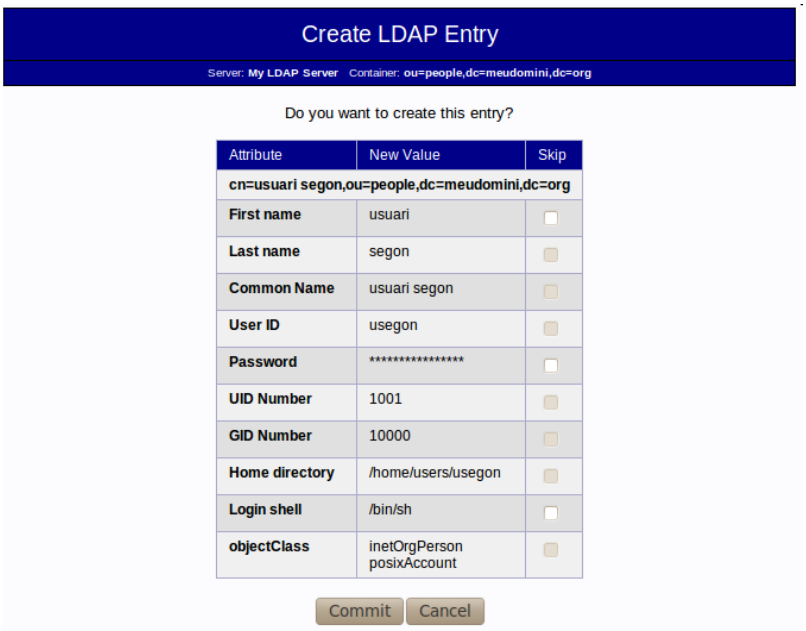
Es calcula automàticament un identificador d'usuari (*UID number*); cal especificar un identificador de grup (GID), el directori personal i l'intèrpret de ordres, com es mostra en la figura 2.12.

FIGURA 2.12. Paràmetres addicionals de creació d'usuari



Un cop completada aquesta informació, hem de prémer el botó **Create object**, i apareix la finestra de la figura 2.13.

FIGURA 2.13. Propietats de l'usuari creat



Premem el botó **Commit**, i podreu comprovar en la figura 2.14 que s'ha afegit l'objecte corresponent a l'usuari segon dins la unitat organitzativa **People**.

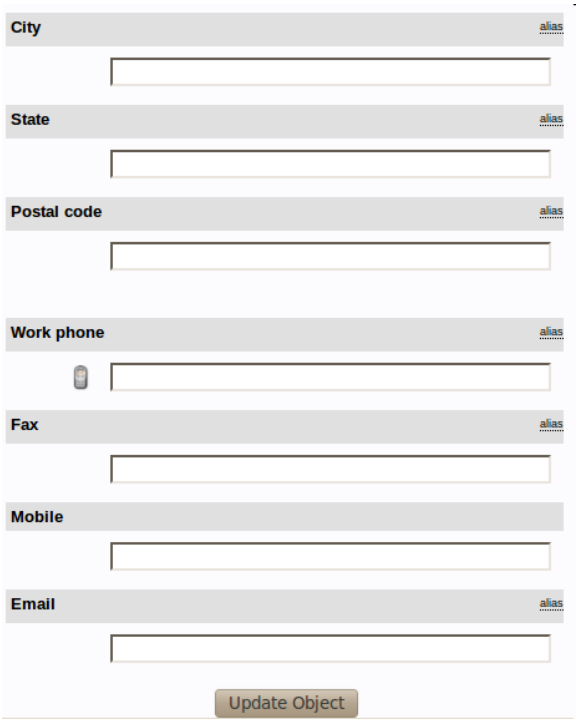
FIGURA 2.14. Arbre amb el nou objecte (usuari) creat

2. Modificació d'un compte d'usuari. Per tal de dur a terme modificacions en el compte d'un usuari que ja hem creat en el domini, només cal seleccionar l'objecte corresponent dins de l'arbre del servidor de LDAP. Això ens permetrà accedir a les propietats d'aquest objecte, modificar-ne el nom, el cognom, l'identificador d'usuari, la contrasenya, el directori personal, el número identificador d'usuari i l'intèrpret de ordres associat. Una altra opció interessant és l'anomenada **switch template**, o canvi de plantilla, que es presenta en forma d'enllaç. Si fem un clic en aquest enllaç, el sistema mostra una altra finestra com la de la figura 2.15.

FIGURA 2.15. Opcions de plantilla de l'objecte usuari

Triem l'opció **generic address book** i ens apareixeran més camps que en la plantilla genèrica. Concretament, podrem afegir una fotografia, el nom d'una organització (*organization*), un carrer (*street*), una ciutat (*city*), un estat (*state*), un codi postal (*postal code*), un telèfon de treball (*work phone*), un número de fax, un telèfon mòbil (*mobile*) i un correu electrònic. Podeu veure alguns d'aquests nous camps en la figura 2.16.

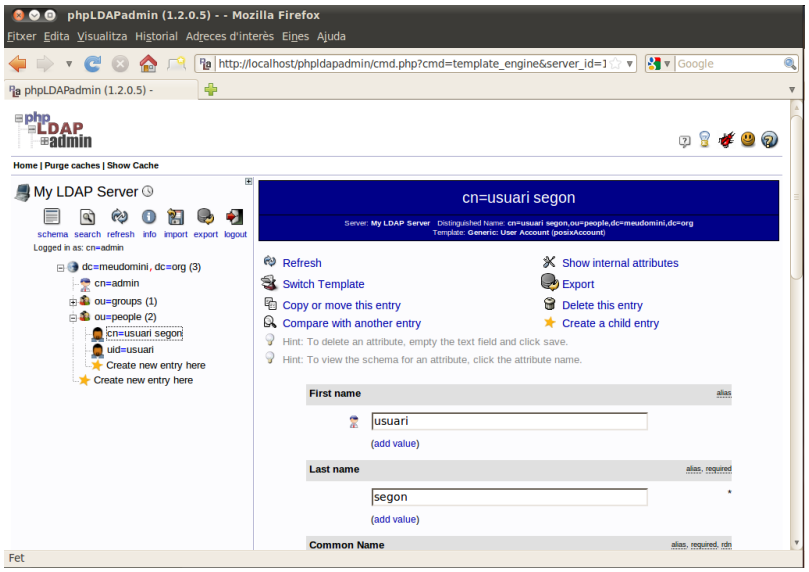
FIGURA 2.16. Camps addicionals per a l'objecte usuari



Quan haurem acabat de fer totes les modificacions necessàries, premem el botó **update object**.

3. Eliminació d'un compte d'usuari. Quan una persona deixa de ser usuari del sistema d'una manera permanent, convé eliminar l'objecte usuari corresponent de la base de dades del servidor de LDAP. D'aquesta manera, ens assegurem que els objectes que hi són presents corresponen a usuaris actuals del sistema, evitem accessos indeguts i, a més, mantenim actualitzada la base de dades, minimitzant l'espai que ocupa. Per tal d'eliminar un usuari de LDAP, només cal accedir a l'arbre de LDAP dins del phpLDAPadmin i seleccionar l'objecte corresponent a l'usuari, com podeu veure en la figura 2.17.

FIGURA 2.17. Selecció i eliminació d'un objecte d'usuari LDAP



Seleccionem l'enllaç anomenat **Delete this entry** i el sistema ens demanarà confirmació, com mostra la figura 2.18.

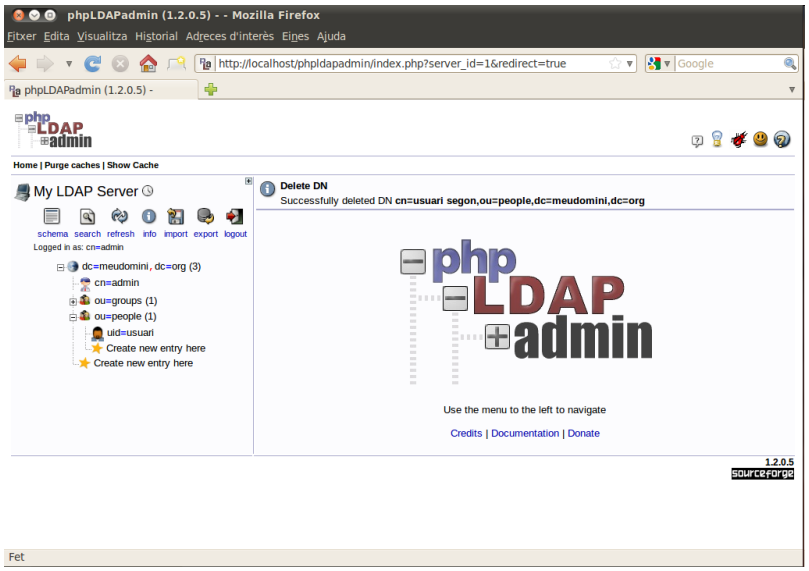
FIGURA 2.18. Confirmació d'eliminació d'objecte usuari

Usuaris

Correctament configurat, els usuaris que hem creat dins del directori LDAP es poden validar localment o per mitjà de la xarxa en el servidor, iniciant la sessió com si es tractés d'un usuari local.

Premem el botó **Delete** i el sistema ens mostrarà un missatge informatiu sobre si ha pogut dur a terme la petició. A més a més, l'objecte haurà desaparegut de l'arbre de l'LDAP. Ho podeu veure en la figura 2.19.

FIGURA 2.19. Resultat de l'eliminació d'un objecte usuari



2.1.5 Comptes d'equips

LDAP permet l'autenticació basada en nodes de la xarxa. L'autenticació basada en nodes permet restringir a qui es permet iniciar la sessió en una màquina que fa servir LDAP per dur a terme l'autenticació. Bàsicament, es tracta d'afegir un atribut a cadascun dels usuaris del servidor LDAP, que inclogui en quins dels nodes de la xarxa se'ls permet iniciar la sessió.

Cadascun dels sistemes dels clients comprova el valor camp i el compara amb el nom de l'amfitrió, permetent o denegant l'inici de sessió segons aquest atribut. Hi ha dos mètodes que serveixen per forçar l'autenticació basada en el node de la xarxa (amfitrió): el primer és utilitzar **libpam-ldap** i el segon es fer servir un filtre pam (**pam_filter**) a LDAP.

Autenticació mitjançant libpam-ldap

Si fem servir la directiva **pam_check_host_attr** per tal de forçar l'autenticació en funció de l'amfitrió, els usuaris seran informats explícitament que no poden iniciar la sessió en aquell node amb un missatge d'error semblant a: Accés denegat per aquest amfitrió.

Per tal d'utilitzar **libpam-ldap** cal utilitzar l'atribut **host**. Amb la documentació d'aquest paquet podem trobar un esquema que ens dóna aquest atribut, i està localitzat en el fitxer `/usr/share/doc/libpam-ldap/ldapns.schema`, el qual es pot afegir al fitxer `slapd.conf`, si cal. Per definir aquest atribut podem utilitzar phpLDAPadmin o bé podem crear un fitxer anomenat `nodes.ldif` amb el contingut següent:

```
dn: uid=user_to_change,ou=Users,dc=example,dc=com
changetype: modify
add: host
host: hostname
```

on hem de substituïr "hostname" pel nom del node. Fet això, aplicarem els canvis utilitzant l'ordre següent:

```
ldapmodify -H ldaps://ldapserver -D "cn=admin,dc=example,dc=com" -x -W -f nodes
    .ldif
```

En el client, hem de modificar el fitxer `/etc/ldap.conf` (o qualsevol altre fitxer de configuració, tal com hem definit en el pam.d) de manera que inclogui la línia següent:

```
pam_check_host_attr yes
```

Cal tenir en compte que el fitxer `/etc/nsswitch.conf` no hauria de contenir **ldap** en l'entrada corresponent a **shadow**; si no és així, sempre ens podrem autenticar independentment de quin sigui el node.

Autenticació mitjançant un filtre de pam (pam_filter)

Si fem servir la directiva **pam_filter** en el fitxer `/etc/ldap.conf` és possible forçar PAM perquè permeti només els comptes d'usuari amb els atributs que escollim. Els usuaris als quals no es permet l'accés al node des d'on intenten iniciar sessió, no rebran cap error. En aquest cas, PAM els informarà que han entrat una contrasenya incorrecta. Podem crear, utilitzant l'atribut libpam-ldap host, un filtre que coincideixi amb el nom del node o qualsevol (*) en el fitxer `/etc/ldap.conf`:

```
1 pam_filter |(host=thehostname)(host=\*)
```

2.1.6 Perfils d'usuari

Un perfil d'usuari fa referència al conjunt de preferències que té aquest usuari determinat: el fons d'escriptori, l'aspecte de l'entorn gràfic, les aplicacions instal·lades, els permisos sobre aquestes aplicacions i sobre els recursos. Quan instal·lem un sistema operatiu, els perfils d'usuari es creen i es carreguen localment, és a dir, en el mateix disc dur de l'ordinador on hem instal·lat el sistema operatiu. Quan disposem d'una xarxa d'àrea local amb molts ordinadors, és molt difícil gestionar aquests perfils, i és aconsellable fer-ne una gestió centralitzada.

Per fer això, cal disposar d'un controlador de domini, o en el nostre cas concret, d'un servidor amb un servei de directori LDAP instal·lat. La manera que té un servidor de LDAP de gestionar els usuaris, els grups, els comptes de màquines, els perfils d'usuaris i les seves carpetes personals és integrant el protocol SAMBA. Aquest protocol permet que, mitjançant el servei LDAP, usuaris tant d'estacions GNU/Linux com estacions amb Windows es puguin autenticar, carreguin els seus perfils i accedeixin a carpetes personals en el servidor.

Hi ha tres paquets necessaris per integrar Samba amb LDAP: **samba**, **samba-doc** i **smbldap-tools**. Per instal·lar aquests paquets escriurem des d'un terminal, i com a usuari administrador (*root*), el següent:

```
1 apt-get install samba samba-doc smbldap-tools
```

Configuració d'OpenLDAP

Per tal que SAMBA faci servir OpenLDAP com a proveïdor de la comprovació d'usuaris i contrasenyes, els objectes d'usuari en el directori de LDAP han de tenir atributs addicionals. Suposem que volem configurar Samba com un servidor de domini de Windows NT. Vegem, doncs, els passos per aconseguir-ho:

1. Els atributs Samba es defineixen en el fitxer **samba.schema** que és una part del paquet **samba-doc**. El fitxer d'esquema (*schema*) s'ha de descomprimir (està

comprimit en format zip) i s'ha de copiar al directori `/etc/ldap/` amb el mateix nom. Per fer això escrivim des d'un terminal:

```
cp /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz /etc/ldap/schema/
gzip -d /etc/ldap/schema/samba.schema.gz
```

2. Ara l'esquema samba (*schema*) s'ha d'afegir a la branca **cn=config** de l'arbre de ldap. De primer creem un fitxer de configuraicó anomenat `schema_convert.conf`, que contingui les línies següents:

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/collective.schema
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/duaconf.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema
include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/samba.schema
```

Tot seguit creem un directori temporal per desar la sortida que generarà la inclusió d'aquest fitxer de configuració:

```
mkdir /tmp/ldif_output
```

Ara utilitzarem slapcat per convertir els fitxers d'esquema a un format que pugui entendre LDAP:

```
slapcat -f schema_convert.conf -F /tmp/ldif_output -n0 -s "cn={12}samba,cn=
    schema,cn=config" > /tmp/cn=samba.ldif
```

Editem el fitxer generat amb aquesta ordre `/tmp/cn=samba.ldif` i canviem els atributs següents (eliminant el {12}, són a les tres primeres línies):

```
dn: cn=samba,cn=schema,cn=config
...
cn: samba
```

I eliminem les línies següents del final del fitxer:

```
structuralObjectClass: olcSchemaConfig
entryUUID: b53b75ca-083f-102d-9fff-2f64fd123c95
creatorsName: cn=config
createTimestamp: 20080827045234Z
entryCSN: 20080827045234.341425Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20080827045234Z
```

Finalment, fent servir la utilitat ldapadd, afegim el nou esquema al directori LDAP:

```
ldapadd -x -D cn=admin,cn=config -W -f /tmp/cn\=samba.ldif
```

3. Creem un fitxer anomenat `samba_indexes.ldif` amb el contingut següent:

```
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: uidNumber eq
olcDbIndex: gidNumber eq
olcDbIndex: loginShell eq
olcDbIndex: uid eq,pres,sub
olcDbIndex: memberUid eq,pres,sub
olcDbIndex: uniqueMember eq,pres
olcDbIndex: sambaSID eq
olcDbIndex: sambaPrimaryGroupSID eq
olcDbIndex: sambaGroupType eq
olcDbIndex: sambaSIDList eq
olcDbIndex: sambaDomainName eq
olcDbIndex: default sub
```

4. Utilitzem ldapmodify per carregar els nous índexs:

```
ldapmodify –x –D cn=admin,cn=config –W –f samba_indexes.ldif
```

5. Si el procediment s'ha seguit correctament, podem visualitzar els nous índexs fent servir l'ordre **ldapsearch**:

```
ldapsearch –xLLL –D cn=admin,cn=config –x –b cn=config –W olcDatabase={1}hdb
```

6. Ens assegurem que el servidor samba està instal·lat i iniciat:

```
smbd status
smbd start/running process 2113
```

En aquest cas, el servidor SAMBA s'està executant i té el número de procés 2113.

7. Tot seguit hem de configurar el paquet **smbldap-tools package** d'una manera adequada perquè sigui coherent amb el nostre entorn. Aquest paquet inclou uns fitxers *script* de configuració que ens faran preguntes sobre les opcions necessitades. Per executar l'*script* escrivim en una consola:

```
gzip –d /usr/share/doc/smbldap–tools/configure.pl.gz
perl /usr/share/doc/smbldap–tools/configure.pl
```

8. Ens demanarà on està localitzat el fitxer de configuració del samba; deixem l'opció per defecte (`/etc/samba/smb.conf`), prement retorn.

9. Ens demanarà on és el directori on hi ha la configuració per defecte de samba-ldap; també deixem l'opció per defecte (`/etc/smbldap-tools/`).

10. Tot seguit ens demanarà el nom del grup de treball o domini al qual s'ha de connectar samba; escrivim **meudomini**.

11. Després ens preguntarà el nom NetBIOS del controlador SAMBA (el mateix que el servidor LDAP): **alumne-desktop**.

12. Nom de la unitat de xarxa que assignarem als clients; per defecte, la unitat H:.

13. Després ens demanarà el directori personal de l'usuari un cop aquest inicii

sessió; deixem l'opció per defecte (**meudomini\nom_usuari**), on **nom_usuari** és el nom d'usuari amb què hem iniciat la sessió.

14. També ens demanarà el directori on s'emmagatzemen els perfils d'usuari (**meudomini.org\profiles\nom_usuari**).

15. Prefix del directori de l'usuari; deixem l'opció per defecte (`/home/nom_usuari`).

16. Permisos per defecte del directori personal de l'usuari; per defecte és 700 (lectura, escriptura, execució per l'usuari, cap permís per als altres usuaris).

17. Nom per defecte de l'*script* inicial de l'usuari; ho podem deixar a l'opció per defecte: (**nom_usuari**).

18. Temps de validació de contrasenya: 45 dies, que és l'opció per defecte.

19. Sufix LDAP; farem servir l'extensió (**.org**).

20. Sufix de grup LDAP; podem posar, per exemple, usuaris.

21. Sufix de l'usuari LDAP; el podem deixar buit.

22. Sufix de la màquina LDAP; el deixem buit.

23. Sufix Idmap; deixem l'opció per defecte (**ou=Idmap**).

24. Lloc on volem desar l'identificador d'usuari i l'identificador de grup pels nous usuaris i grups; deixem l'opció per defecte.

25. Nom o adreça IP del servidor LDAP; podem escriure 127.0.0.1.

26. Port per defecte de LDAP; deixem l'opció per defecte (389).

27. Nom distingit de l'usuari admin (**cn=admin,dc=meudomini,dc=org**).

28. Contrasenya de l'usuari admin de LDAP.

29. Servidor LDAP esclau; ho deixem en blanc, com la resta d'opcions que fan referència a aquest servidor esclau.

30. Suport de TLS (connexions encriptades). Si està activat TLS escollim 1; si no, escollim 0.

31. Identificador del grup de treball (SID); el podem obtenir amb l'ordre **net getlocalsid alumne-desktop**.

32. Forma d'encriptació de les contrasenyes unix; escollim l'opció per defecte (SSHA).

33. Després pregunta l'identificador d'usuari, de grup, intèrpret d'ordres i directori amb el perfil d'usuari per defecte; deixem les opcions per defecte.

34. Finalment escollim l'extensió del correu del domini (**meudomini.org**).

Un cop haurem contestat totes les preguntes, s'han d'haver

creat dos fitxers: `/etc/smbldap-tools/smbldap.conf` i `/etc/smbldap-tools/smbldap_bind.conf`. L'*script* de configuració ha generat aquests fitxers; per tant, si ens hem equivocat en alguna de les respostes, els podem editar directament, o podem tornar a executar l'*script* (fitxer per lots).

35. Ara haurem d'executar l'*script* anomenat **smbldap-populate** que afegirà els usuaris i grups necessaris que Samba requereix. És recomanable fer una còpia de seguretat del fitxer ldif (*LDAP data interchange format*), amb l'eina *slapcat before* executant l'ordre següent:

```
slapcat -l backup.ldif
```

36. Un cop hem fet la còpia de seguretat, executem l'*script*:

```
smbldap-populate
```

Cal tenir en compte que podem crear un fitxer LDIF que contingui els nous objectes de Samba executant l'ordre **smbldap-populate -e samba.ldif**. Això ens permet mirar els canvis que aplicarem al sistema i assegurar-nos que tot està bé. Si hem seguit tots aquests passos, el directori LDAP tindrà tota la informació necessària per autenticar usuaris SAMBA.

Hi ha diverses maneres de configurar Samba, però per configurar Samba perquè faci servir LDAP hem d'editar el fitxer de configuració principal de Samba `/etc/samba/smb.conf`, comentant l'opció **passdb backend** i afegint-hi les línies següents:

```
#   passdb backend = tdbsam

# LDAP Settings
passdb backend = ldapsam:ldap://ubuntu-server
ldap suffix = dc=meudomini,dc=org
ldap user suffix = ou=People
ldap group suffix = ou=Groups
ldap machine suffix = ou=Computers
ldap idmap suffix = ou=Idmap
ldap admin dn = cn=admin,dc=meudomini,dc=org
ldap ssl = start tls
ldap passwd sync = yes
...
add machine script = sudo /usr/sbin/smbldap-useradd -t 0 -w "%u"
```

37. Reiniciem el servei samba per aplicar els nous canvis:

```
restart smbd
restart nmbd
```

El servei nmbd serveix per proveir serveis de resolució de noms de NetBIOS fent servir el protocol IP.

38. Ara cal que Samba conegui la contrasenya d'administrador de LDAP; escrivim des d'un terminal:

```
smbpasswd -w 123456
```

39. Hem de reemplaçar 123456 amb la contrasenya d'administrador de l'LDAP. Si tenim usuaris LDAP i volem que s'autentiquin usant Samba, hem de definir un seguit d'atributs en el fitxer `samba.schema`. Afegim els atributs Samba als

usuaris existents emprant la utilitat **smbpasswd**, reemplaçant nom_usuari pel nom d'usuari real, i escrivint la seva contrasenya:

```
smbpasswd -a nom_usuari
```

40. Per afegir un nou usuari, grup i compte de màquina, hem de fer servir les utilitats que conté el paquet **smbldap-tools**. Per afegir un usuari al directori LDAP amb atributs Samba, escrivim el següent, reemplaçant nom_usuari amb el nom d'usuari real:

```
smbldap-useradd -a -P nom_usuari
```

L'opció -a afegeix els atributs Samba, i l'opció -P permet entrar la contrasenya per l'usuari un cop s'ha creat.

41. Si volem eliminar un usuari del directori LDAP, escrivim:

```
smbldap-userdel username
```

Si fem servir l'opció -r amb aquesta ordre, podem eliminar el directori personal de l'usuari.

42. Podem fer servir la utilitat **smbldap-groupadd** per afegir un nou grup d'usuaris, reemplaçant nom_grup amb el nom de grup que vulguem:

```
smbldap-groupadd -a nom_grup
```

Igual que en el cas de la utilitat **smbldap-useradd**, l'opció -a afegeix els atributs Samba.

43. Per afegir un usuari a un grup, utilitzem **smbldap-groupmod**:

```
smbldap-groupmod -m nom_usuari nom_grup
```

Hem de reemplaçar el nom_usuari amb el nom d'usuari real, i nom_grup amb el nom del grup real. L'opció -m permet afegir més d'un usuari al mateix temps, separant-los per comes.

44. Per eliminar un usuari d'un grup també podem utilitzar **smbldap-groupmod**:

```
smbldap-groupmod -x username groupname
```

45. Finalment, la utilitat **mbldap-useradd** permet afegir comptes d'equips Samba:

```
smbldap-useradd -t 0 -w username
```

Configuració de SAMBA perquè faci de controlador de domini

Malgrat tots els passos que hem dut a terme per configurar l'OpenLDAP, encara ens fa falta instal·lar alguns paquets perquè Samba esdevingui un controlador de domini.

1. Instal·lem el paquet **libpam-smbpass**:

```
apt-get install samba libpam-smbpass
```

2. Després configurem Samba editant el fitxer `/etc/samba/smb.conf`. El mode de seguretat s'hauria d'inicialitzar a user i el grup de treball s'hauria de relacionar amb l'organització:

```
workgroup = meudomini
   ...
security = user
```

3. En la secció comentada "Domains" afegim el següent:

```
domain logons = yes
logon path = \\%N\%U\profile
logon drive = H:
logon home = \\%N\%U
logon script = logon.cmd
add machine script = sudo /usr/sbin/useradd -N -g machines -c Machine -d /var/
    lib/samba -s /bin/false %u
```

Vegem el significat de totes aquestes línies a la taula 2.1.

TAULA 2.1. Opcions de configuració del fitxer /etc/samba/smb.conf

Opció	Significat
domain logons	Proveeix el servei **netlogon** per tal que Samba actuï com un controlador de domini.
logon path	Posa el perfil de Windows en el directori personal de l'usuari. També és possible configurar un directori compartit que contingui tots els perfils en un sol directori.
logon drive	Especifica la ruta local del directori personal.
logon home	Especifica la localització del directori personal.
logon script	Determina el fitxer per lots (*script*), que s'ha d'executar localment un cop l'usuari ha iniciat sessió. Cal que aquest *script* se situï en el directori compartit especificat per [netlogon].
add machine script	Un fitxer per lots (*script*), que crearà automàticament el compte de màquina confiable, per tal que una estació de treball s'uneixi al domini

4. Cal que el grup de màquines s'hagi creat fent servir la utilitat **addgroup**. A més a més, cal donar permisos de manera explícita al grup d'administradors del domini per permetre que l'*script* d'afegir màquina funcioni. Això es pot aconseguir executant:

```
net rpc rights grant "EXAMPLE\Domain Admins" SeMachineAccountPrivilege
    SePrintOperatorPrivilege \
SeAddUsersPrivilege SeDiskOperatorPrivilege SeRemoteShutdownPrivilege
```

Perfils mòbils Windows

Els perfils mòbils en sistemes Windows permeten personalitzar l'escriptori, canviant el fons, l'aspecte de les finestres i els programes disponibles per a cada estació.

Val a dir que això crea per defecte perfils mòbils; és a dir, independentment de la màquina des de la qual l'usuari s'autentica, es carregarà el perfil des del servidor.

Per tal de carregar un determinat perfil mòbil de Windows a un usuari quan aquest

inicïi la sessió, de primer creem aquest perfil localment i, un cop fet això, copiem la carpeta personal de l'usuari (dins de *Documents and settings* en el cas de Windows XP, i dins de *Users* en el cas de Vista i 7), al directori del servidor especificat per la línia **logon path** del fitxer de configuració del SAMBA.

PDC

El terme *PDC* és un acrònim de l'anglès que significa '*primary domain controller*' ('controlador de domini primari'); és en una xarxa d'ordinadors, l'ordinador que fa de servidor de domini. El PDC pot ser un ordinador que funcioni amb Windows Server i Active Directory, o bé amb una distribució de GNU/Linux i OpenLDAP.

2.1.7 Carpetes personals

Per tal que els usuaris puguin accedir a les carpetes personals, hem d'editar el fitxer `/etc/smb/smb.conf` i descomentar les línies sota la secció [homes]:

```
[homes]
   comment = Home Directories
   browseable = no
   read only = no
   create mask = 0700
   directory mask = 0700
   valid users = %S
```

Com que hem configurat el servidor com un servidor de domini, hem de configurar la compartició de [netlogon]. Per tal d'habilitar-ho, descomentem:

```
[netlogon]
   comment = Network Logon Service
   path = /srv/samba/netlogon
   guest ok = yes
   read only = yes
   share modes = no
```

Cal dir que el camí on inicialment es comparteixen tots els fitxers d'inici de sessió (*netlogon*), és `/home/samba/netlogon`, però segons l'estàndard de jerarquia del sistema de fitxers (FHS), el directori `/srv` és la localització correcta.

També haurem de crear el directori *netlogon*, i un fitxer per lots anomenat `logon.cmd`, que de moment estarà buit:

```
mkdir –p /srv/samba/netlogon
   touch /srv/samba/netlogon/logon.cmd
```

Podem utilitzar qualsevol instrucció de Windows en el fitxer per lots d'inici de sessió **per tal de configurar l'entorn del client**.

Com que, per defecte, l'usuari **root** està deshabilitat, per tal que una estació de treball s'uneixi al domini cal crear un grup de sistema que es correspondrà amb un grup d'administradors del domini de Windows. Farem servir la utilitat **net** des d'un terminal executant el següent:

```
net groupmap add ntgroup="Domain Admins" unixgroup=sysadmin rid=512 type=d
```

S'ha de canviar **sysadmin** per qualsevol nom de grup que vulguem. A més a més, l'usuari que s'ha d'unir al domini ha de formar part del grup **sysadmin**, a més de ser un membre del grup d'administradors del sistema. Els grups d'administrador permeten la utilització de **sudo**.

Per acabar, cal reiniciar el servei Samba per habilitar el nou controlador de domini:

```
restart smbd
   restart nmbd
```

D'aquesta manera, podrem afegir clients Windows al domini, com ho faríem si tinguéssim un servidor de Windows NT.

2.1.8 Plantilles d'usuari

A l'hora de crear un usuari del domini podem utilitzar plantilles diferents. Si per gestionar els usuaris utilitzem phpLDAPadmin, ens adonarem que disposa de tot un seguit de plantilles que ens faciliten aquesta tasca. Podem observar les diverses plantilles per a la creació d'objectes en el domini LDAP en la figura 2.9. D'entre totes aquestes plantilles, no totes serveixen per crear usuaris del sistema; podem utilitzar les que detallem en la taula 2.2.

TAULA 2.2. Plantilles utilitzables per a la creació d'usuaris

Tipus de plantilla	Significat
Generic: User Account	Compte genèric de creació d'usuaris
Samba: Account	La podem utilitzar si hem integrat Samba amb LDAP, de manera que els usuaris creats amb Samba són usuaris del domini.
Default	Plantilla de creació d'objectes LDAP per defecte; serveix també per a usuaris
Courier Mail: Account	Compte de correu electrònic, no serveix perquè un usuari inicií la sessió interactiva en el sistema

XML

XML és un acrònim anglès que significa *eXtensible Markup Language*; és a dir, llenguatge de marques extensible. És un llenguatge d'etiquetes, desenvolupat pel World Wide Web Consortium (W3C), que prové de la simplificació i adaptació de l'experimentat SGML, i permet definir la gramàtica de llenguatges específics (de la mateixa manera que HTML és, alhora, un llenguatge definit per SGML).

Totes les plantilles que presenta phpLDAPadmin estan emmagatzemades en el subdirectori `/usr/share/phpldapadmin/templates/`. Aquestes plantilles són un conjunt de fitxers xml, on els nodes pare són les característiques, paràmetres i atributs. Vegem, per exemple, el fitxer xml que s'utilitza per crear un compte d'usuari LDAP (`posixAccount.xml`):

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE template SYSTEM "template.dtd">

<template>
<askcontainer>1</askcontainer>
<description>New User Account</description>
<icon>ldap-user.png</icon>
<invalid>0</invalid>
<rdn>cn</rdn>
```

```
<!--<regexp>^ou=People,o=.*,</regexp>-->
<title>Generic: User Account</title>
<visible>1</visible>

<objectClasses>
<objectClass id="inetOrgPerson"></objectClass>
<objectClass id="posixAccount"></objectClass>
</objectClasses>

<attributes>
<attribute id="givenName">
    <display>First name</display>
    <icon>ldap-uid.png</icon>
    <onchange>=autoFill(cn;%givenName% %sn%)</onchange>
    <onchange>=autoFill(uid;%givenName|0-1/l%%sn/l%)</onchange>
    <order>1</order>
    <page>1</page>
</attribute>
<attribute id="sn">
    <display>Last name</display>
    <onchange>=autoFill(cn;%givenName% %sn%)</onchange>
    <onchange>=autoFill(uid;%givenName|0-1/l%%sn/l%)</onchange>
    <!-- <onchange>=autoFill(homeDirectory;/home/users/%uid|0-1/l%/%uid%)</
        onchange> -->
    <order>2</order>
    <page>1</page>
</attribute>
<attribute id="cn">
    <display>Common Name</display>
    <order>3</order>
    <page>1</page>
</attribute>
<attribute id="uid">
    <display>User ID</display>
    <onchange>=autoFill(homeDirectory;/home/users/%uid%)</onchange>
    <order>4</order>
    <page>1</page>
    <spacer>1</spacer>
</attribute>
<attribute id="homeDirectory">
    <display>Home directory</display>
    <!-- <onchange>=autoFill(homeDirectory;/home/users/%gidNumber|0-0/T%/%uid
        |3-%)</onchange> -->
    <order>8</order>
    <page>1</page>
</attribute>
<attribute id="uidNumber">
    <display>UID Number</display>
    <icon>terminal.png</icon>
    <order>6</order>
    <page>1</page>
    <readonly>1</readonly>
    <value>=php.GetNextNumber(/;uidNumber)</value>
</attribute>
<attribute id="gidNumber">
    <display>GID Number</display>
    <!-- <onchange>=autoFill(homeDirectory;/home/users/%gidNumber|0-0/T%/%uid
        |3-%)</onchange> -->
    <order>7</order>
    <page>1</page>
    <value><![CDATA[=php.PickList(/;(&(objectClass=posixGroup));gidNumber;%cn
        %;;;;cn)]]></value>
</attribute>
<attribute id="loginShell">
    <display>Login shell</display>
    <order>9</order>
    <page>1</page>
    <!-- <value><![CDATA[=php.PickList(/;(&(objectClass=posixAccount));
        loginShell;%loginShell%;;;;loginShell)]]></value> -->
    <type>select</type>
```

```
75      <value id="/bin/sh">/bin/sh</value>
76      <value id="/bin/csh">/bin/csh</value>
77      <value id="/bin/tsh">/bin/tsh</value>
78  </attribute>
79  <attribute id="userPassword">
80      <display>Password</display>
81      <!-- <helper>
82          <display>Encryption</display>
83          <id>enc</id>
84          <value>=php.PasswordEncryptionTypes()</value>
85      </helper> -->
86      <icon>lock.png</icon>
87      <order>5</order>
88      <page>1</page>
89      <post>=php.PasswordEncrypt(%enc%;%userPassword%)</post>
90      <spacer>1</spacer>
91      <verify>1</verify>
92  </attribute>
93  </attributes>
94
95  </template>
```

Podem veure refletit en el codi del fitxer posixAccount.xml cadascun dels camps que hem d'omplir quan creem un usuari utilitzant la plantilla **Generic: User Account**.

A més de les plantilles per defecte, podem crear plantilles personalitzades i utilitzar-les en phpLDAPadmin. Per fer això, podem copiar alguna de les plantilles existents, reanomenar-la afegint el prefix **custom_** al nom del fitxer i editant-lo, afegint o eliminant els camps que considerem convenient.

2.1.9 Variables d'entorn

Les variables d'entorn que afecten els usuaris es poden establir en el fitxer de configuració de samba. Vegem una llista de les variables d'entorn que podem utilitzar per als usuaris que es connecten a un domini LDAP amb SAMBA i el significat corresponent:

- %U : Nom d'usuari que ha iniciat la sessió.
- %G : Nom del grup primari al qual pertany l'usuari %U.
- %h : Nom del node de la xarxa (*host name*), en el qual s'està executant SAMBA.
- %m : Nom netbios de la màquina client.
- %L : Nom netbios del servidor.
- %M : Nom d'Internet de la màquina client.
- %R : Nivell de protocol escollit després de la seva negociació; pot ser CORE, COREPLUS, LANMAN1, LANMAN2 o NT1.
- %d : Identificador del procés del servidor.

- %a : Arquitectura de la màquina remota: pot ser samba, el sistema de fitxers Linux (CIFS), OS/2, Windows per a grups de treball (WfWg), Windows 9x/-Me (Win95), Windows NT (WintNT), Windows 2000 (Win2K), Windows XP (WinXP), Windows XP 64 bit (WinXP64), Windows 2003 incloent-hi 2003R2 (Win2K3) i Windows Vista (Vista); qualsevol altre s'anomenarà UNKNOWN.
- %I : Adreça IP de la màquina client.
- %i : Adreça IP local a la qual el client està connectat.
- %T : Data i hora actuals.
- %D : Nom del domini o grup de treball de l'usuari actual.
- %w : El separador *winbind*.
- %$ (envvar) : El valor de la variable d'entorn **envar**.
- %$: El nom del servei actual.
- %P : El directori arrel del servei actual.
- %u : El nom d'usuari del servei actual.
- %g : El nom del grup primari de %u.
- %H : El directori personal de l'usuari %u.
- %N : El nom del directori personal NIS.
- %p : La ruta al directori de l'usuari del servei, obtinguda a partir de l'entrada NIS auto.map. L'entrada NIS auto.map es dividirà com %N:%p.

2.2 Administració de grups LDAP

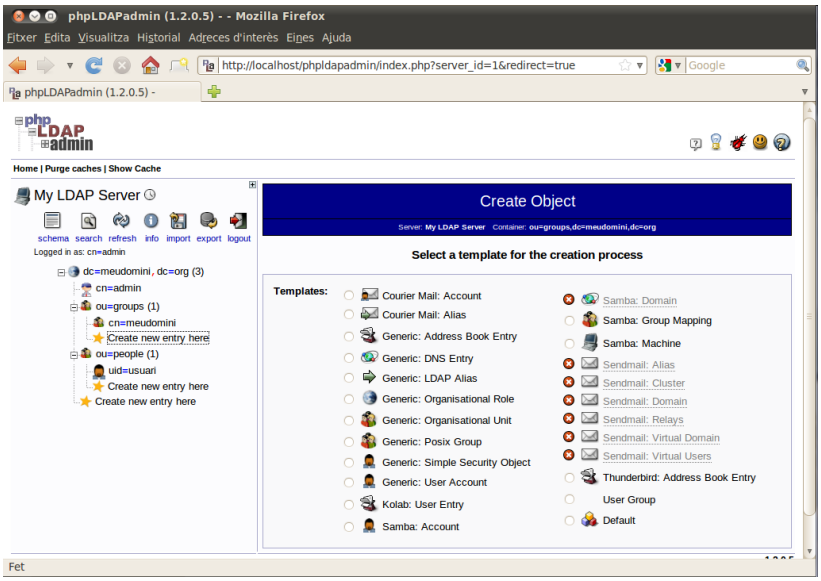
Els grups són una manera ràpida de donar als usuaris accesos comuns a certes prestacions o funcionalitats dins d'un directori LDAP. L'administració dels grups d'LDAP també es pot dur a terme mitjançant phpLDAPadmin.

Ens permet crear un grup nou, modificar-ne els paràmetres i eliminar-lo. També podem assignar usuaris a un grup determinat.

En qualsevol cas, per tal de poder crear un grup d'usuaris cal que s'hagi creat prèviament una unitat organitzativa anomenada **Groups**. Si s'acompleix aquest requeriment, podem crear, modificar i eliminar grups d'usuaris en el directori del servidor LDAP.

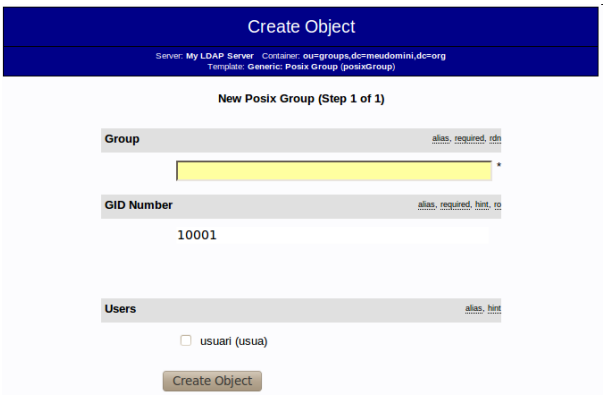
1. Creació d'un grup d'usuaris Per tal de crear un nou grup d'usuaris, ens hem de situar a sota de la unitat organitzativa **groups** i clicar a l'enllaç **Create new entry here**. Ens apareixerà la finestra de la figura 2.20.

FIGURA 2.20. Creació d'un nou objecte grup d'usuaris



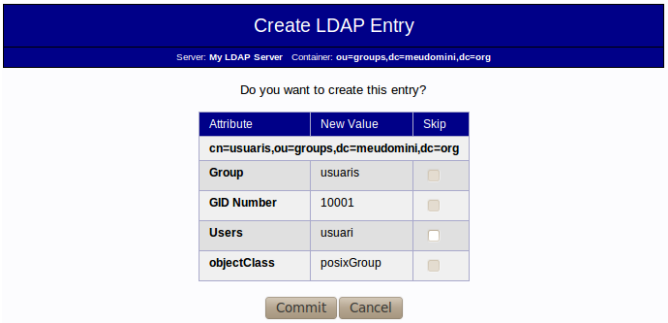
Triem l'opció **Generic: Posix Group** i el sistema mostrarà la finestra de la figura 2.21.

FIGURA 2.21. Edició dels paràmetres del nou grup



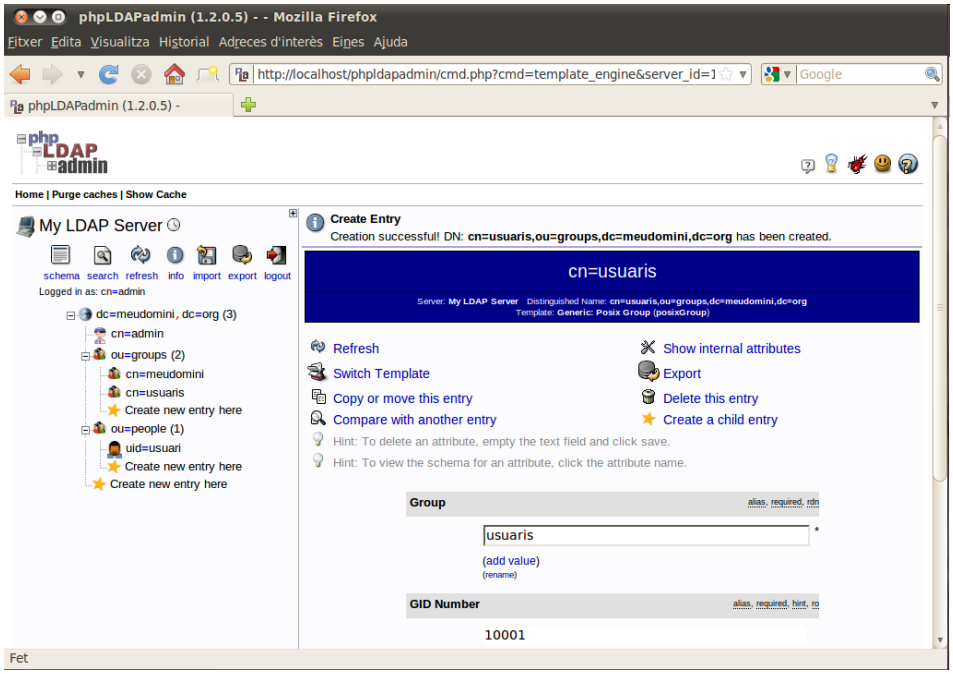
Podrem especificar el nom del grup (en el nostre exemple utilitzarem usuaris), i podrem seleccionar quins usuaris volem que pertanyin al nou grup, clicant el botó de selecció corresponent. Un cop fet això, premem el botó **Create object**, i el sistema mostra una pantalla de confirmació de creació del grup d'usuaris, com podeu comprovar en la figura 2.22.

FIGURA 2.22. Confirmació de la creació del grup d'usuaris



Prement el botó **Commit**, el sistema ens informarà de l'èxit en la creació del nou grup d'usuaris i, a més, podrem comprovar que s'ha creat aquest nou grup d'usuaris perquè apareix l'entrada en l'arbre. Es pot veure en la figura 2.23.

FIGURA 2.23. Resultat de la creació del nou grup



2. Modificació dels paràmetres d'un grup. Per tal de modificar els paràmetres d'un grup d'usuaris que hem creat, només cal seleccionar l'entrada corresponent dins de l'arbre del directori LDAP, com mostra la figura 2.24.

FIGURA 2.24. Propietats del grup d'usuaris

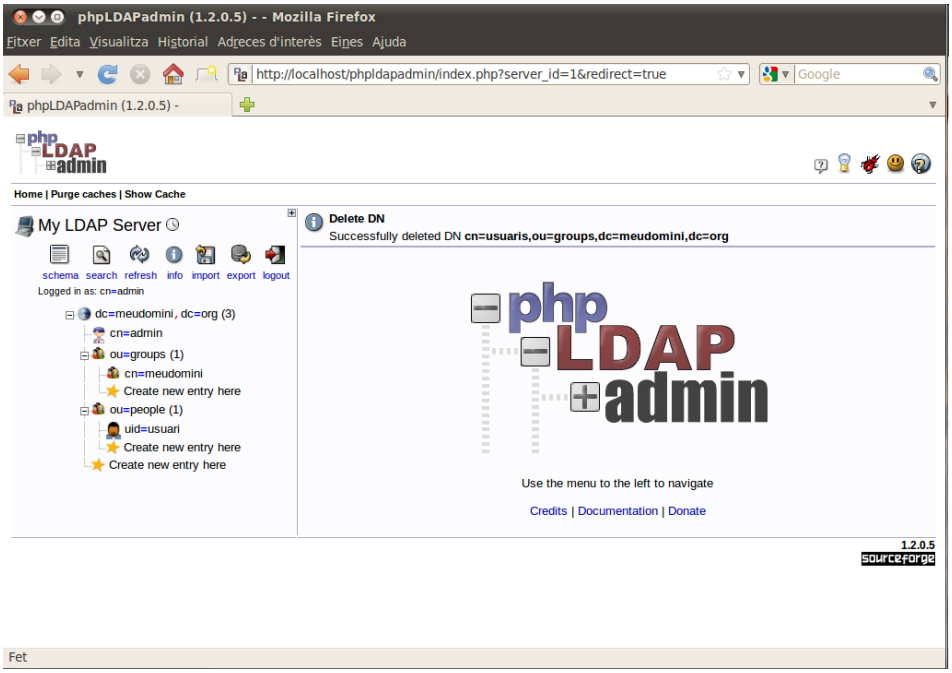
En aquest apartat podrem modificar el nom del grup d'usuaris i seleccionar quins usuaris volem assignar a aquest grup. Un cop fetes les modificacions pertinents, premem el botó **Update object** per completar els canvis.

3. Eliminació d'un grup d'usuaris. Per eliminar un grup d'usuaris, seleccionem l'objecte corresponent dins de l'arbre LDAP, i cliquem a l'enllaç **Delete this entry**. Si fem això, el sistema ens demanarà una confirmació, com es mostra en la figura 2.25.

FIGURA 2.25. Confirmació eliminació grup d'usuaris

Prement el botó **Delete**, el sistema ens informarà de l'eliminació del grup d'usuaris, com veieu en la figura 2.26.

FIGURA 2.26. Resultat eliminació grup d'usuaris



2.2.1 Tipus

En un domini LDAP, els grups d'usuaris que podem crear segueixen l'estàndard POSIX; per tant, tots els grups que creem són d'aquest tipus. Els grups d'usuaris POSIX són equivalents als grups d'usuaris que es poden crear localment amb qual-

sevol ordinador que funcioni amb GNU/Linux, i que mitjançant phpLDAPadmin podrem fer correspondre també a grups d'usuaris de LDAP.

Dit d'una altra manera, mitjançant phpLDAPadmin, podem crear grups d'usuaris del domini, que es correspondrien a grups d'usuaris locals si utilitzéssim l'eina corresponent per a la gestió d'usuaris de manera local (eina *groupadd*).

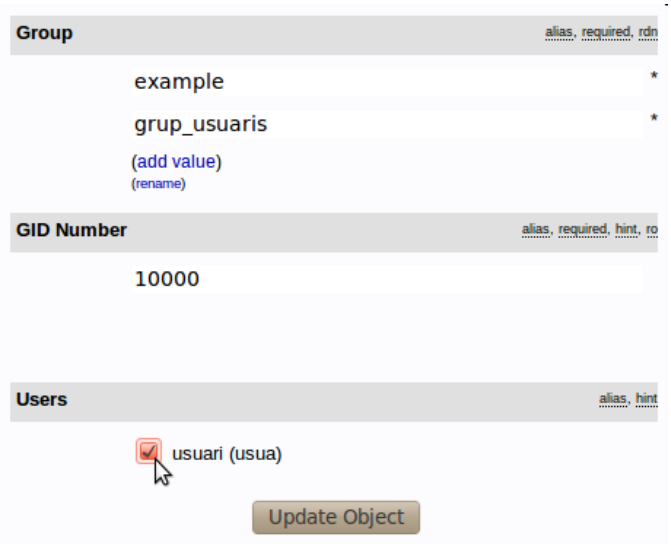
2.2.2 Estratègies d'imbricació

Entenem el concepte d'imbricació d'una manera general com la inclusió d'una estructura dins una altra de tipus semblant. En particular, inclusió d'una subrutina (o bloc d'instruccions) dins d'una altra. En el cas d'un domini, la imbricació pot fer referència a la inclusió d'un usuari dins d'un grup o unitat organitzativa, la inclusió d'usuaris dins d'un grup o, fins i tot, la creació d'un subdomini dins del domini principal.

Les estratègies d'imbricació s'han de tenir en compte a l'hora de crear aquest mateix domini, i són un conjunt de regles que serveixen per fer un bon disseny d'aquest domini i, per tant, podem pensar que és un requeriment a l'hora d'implementar-lo.

Per definir el domini cal tenir en compte que, com a mínim, s'han de crear dues unitats organitzatives: l'una contindrà tots els grups d'usuaris (ou=groups), i l'altra, tots els usuaris del domini (ou=people).

Figura 2.27. Assignació d'usuaris a un grup



Per tant, en primer lloc haurem de pensar quins grups d'usuari volem definir dins del nostre domini i els haurem de crear dins de la unitat organitzativa *groups*. En cap cas hi ha la possibilitat de crear un grup dins d'un altre; tots els grups són "fills" d'aquesta unitat organitzativa.

Un cop fet això, afegirem tots els usuaris dins de la unitat organitzativa *people*.

Tots els usuaris han de ser “fills” d’aquesta unitat organitzativa.

Finalment, caldrà establir la relació entre els usuaris i els grups als quals pertanyen. Això ho podem fer, des del mateix phpLDAPadmin, obrint l’enllaç corresponent, i seleccionant els usuaris que volem que pertanyin al grup. Ho podeu veure en la figura 2.27.

2.2.3 Grups predeterminats

A l’hora de crear un domini no hi ha cap grup predeterminat, si bé és cert que com a mínim s’ha de crear l’usuari admin, aquest no pertany a cap grup en concret i, per tant, la definició dels grups (sempre sota la unitat organitzativa *people*) és lliure i depèn del criteri de l’administrador del domini. En qualsevol cas, és aconsellable agrupar els usuaris segons els departaments, o tipus d’usuaris, per facilitar-ne la gestió.