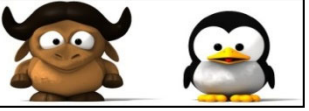


Autenticació centralitzada amb tecnologia LDAP

El problema de l'Administració d'Identitats

El problema d'Administració de Identitats

- Cada usuari te múltiples identitats en la empresa
- Múltiples administradors per a cada usuari
- No existeix un mètode segur per a compartir les identitats d'usuaris entre ambients linux, UNIX® i Windows®
- No existeix un únic punt de administració per a cada usuari

Costos en Seguretat i Taula d'Ajuda

- **Un usuari promig utilitza 5+ claus**
- **55% dels usuaris escriu la clau en paper al menys una vegada**
- **9% de tots els usuaris escriuen en paper totes les claus**
- **51% de tots els usuaris requereixen ajuda de TI per què obliden la seva clau**
- **25% de tots els consultats a les taules d'ajuda estan relacionades amb claus**

Procés Tradicional de Maneig d'Identitats

Username: brucem
Password: hockey1

Solaris

Username: bmackay
Password: hockey1

Windows

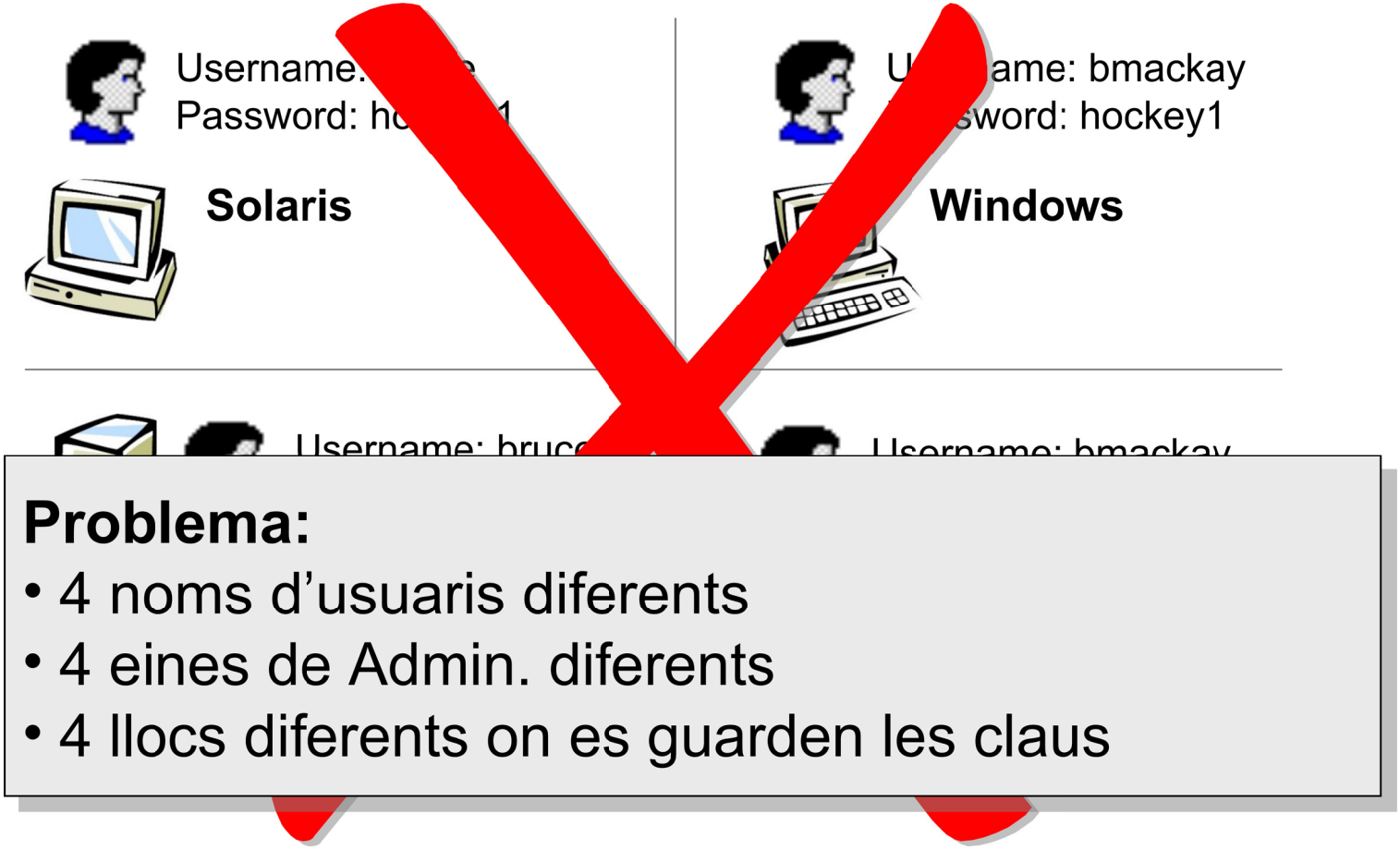
Username: brucem
Pass: hockey1

AIX

Username: bmackay
Password: hockey1

Linux

Procés Tradicional de Maneig d'Identitats



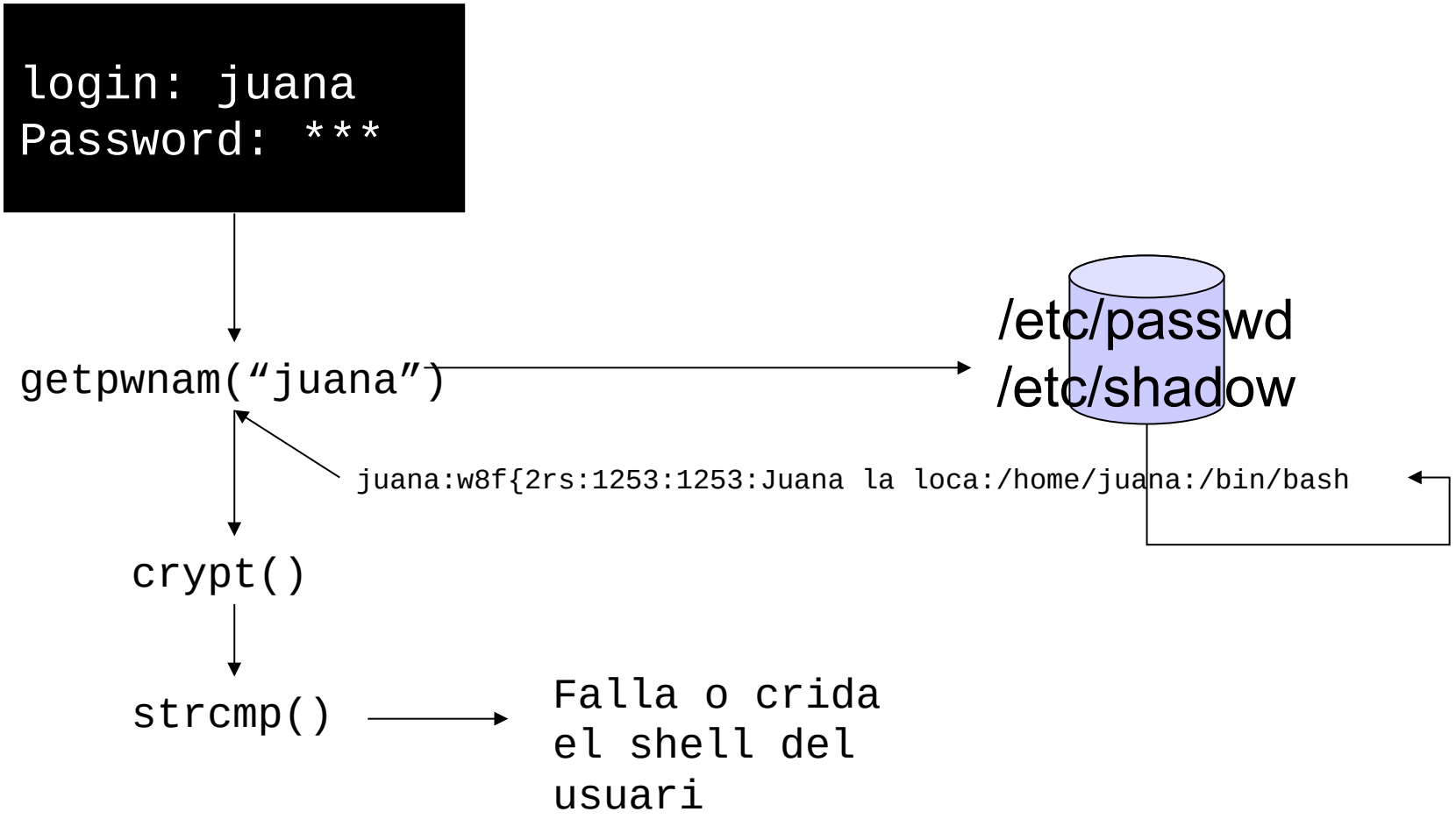
Problema:

- 4 noms d'usuaris diferents
- 4 eines de Admin. diferents
- 4 llocs diferents on es guarden les claus

Autenticació Tradicional

- /etc/passwd
- NIS
- PAM/NSS

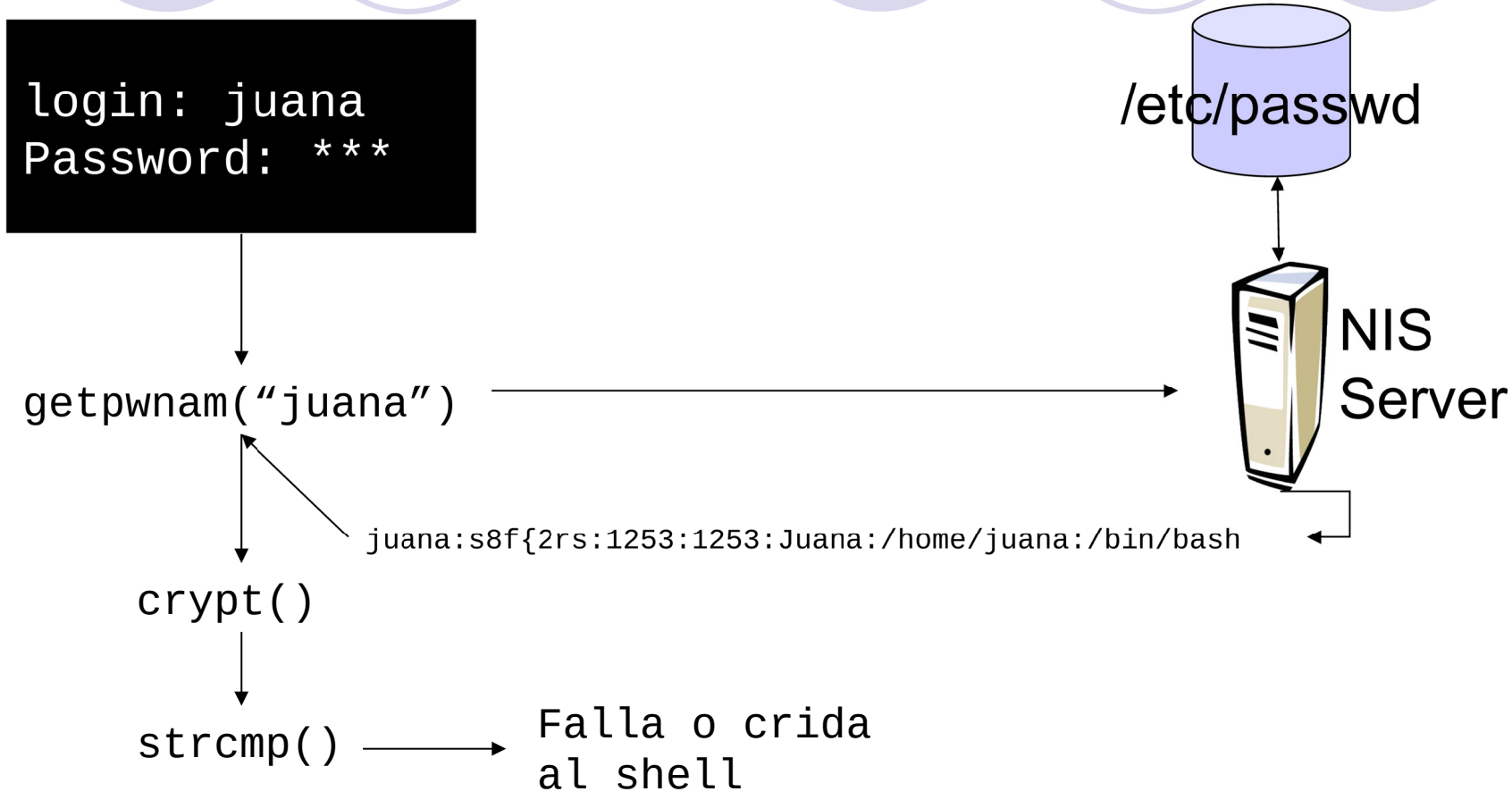
Autenticació /etc/passwd



/etc/passwd Pros/Contres

- Avantatges:
  - Molt simple
- Desavantatges:
  - Dissenyat per a autenticació local
  - Cada màquina ha de tenir l'arxiu /etc/passwd
  - El mateix arxiu ha de replicar-se per a les comptes comuns
  - /etc/passwd no és extensible

Network Information System NIS



NIS Pros/Contres

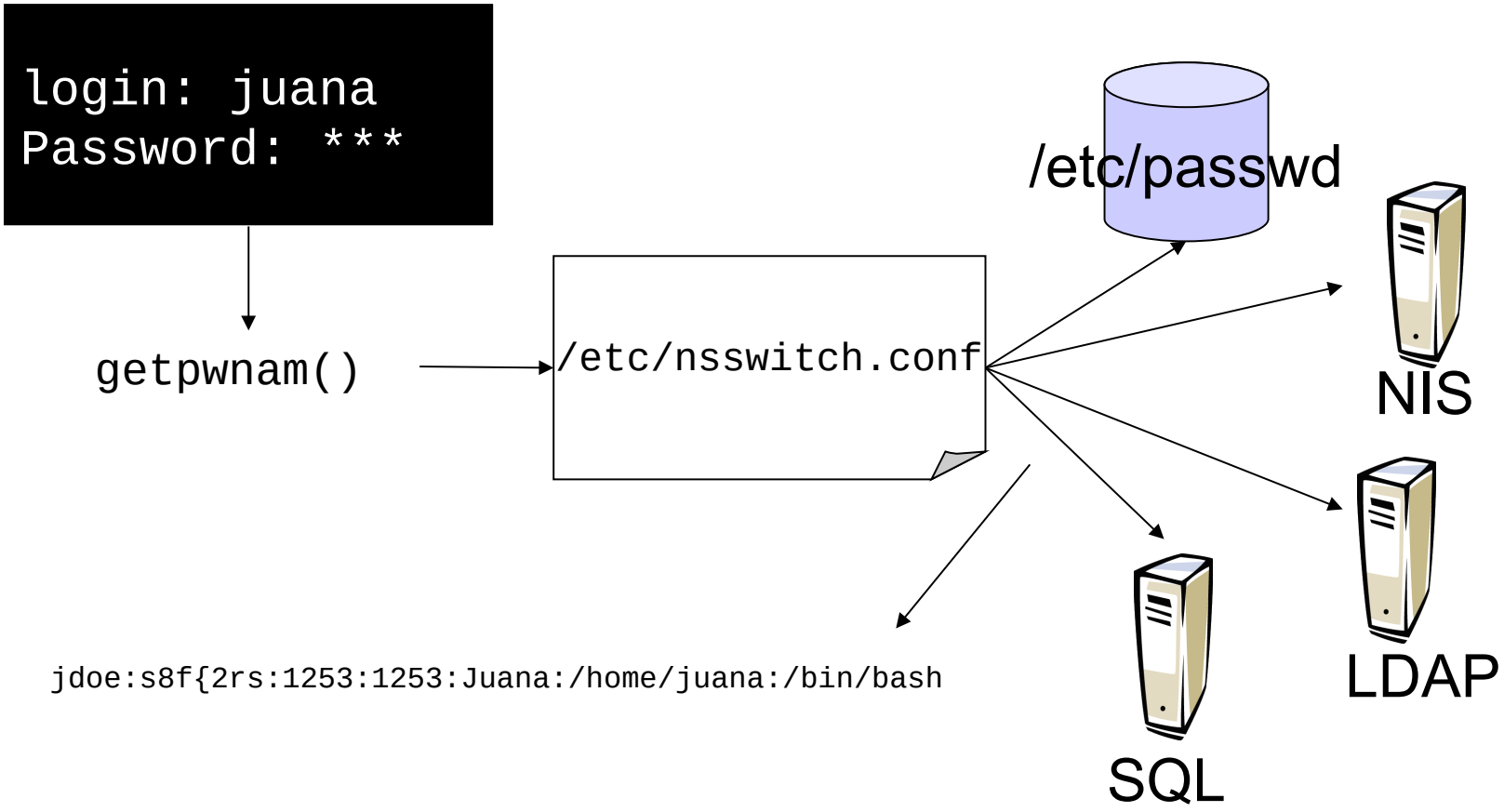
Avantatges:

- Permet distribuir l'arxiu mestre /etc/passwd i /etc/shadow entre diferents servidors
- Compatible amb la majoria de Unix/linux

Desavantatges :

- Molts furats de seguretat
- Canvis en eines administratives
- Incompatible amb sistemes diferents a UNIX
- No treballa en mode desconectat

Name Service Switch (NSS)



NSS Pros/Contres

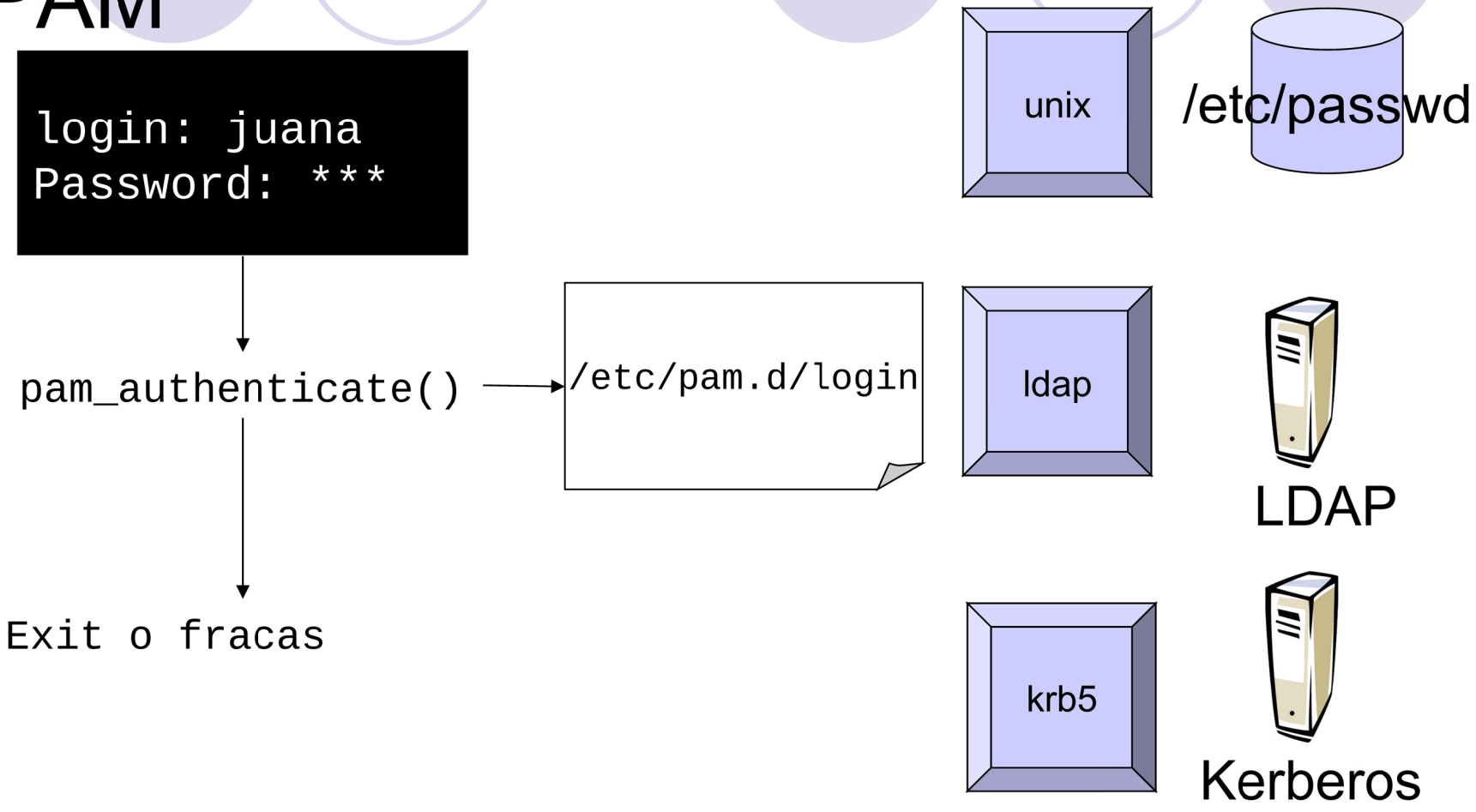
Avantatges:

- Permet que una entrada de /etc/passwd s'obtingui de qualsevol font
- 100% transparent a les aplicacions

Desavantatges:

- No disponible en tots els Unix/Linux
- Quan es busca en múltiples fonts de dades la sincronització és un problema

Pluggable Authentication Modules PAM



PAM Pros/Contres

Avantatges:

- Permet autenticar directament contra qualsevol font de dades
- Fàcilment configurable segons /etc/pam.d
- Aplicacions PAM no necessiten “mecanismes específics” de codi per a autenticar-se

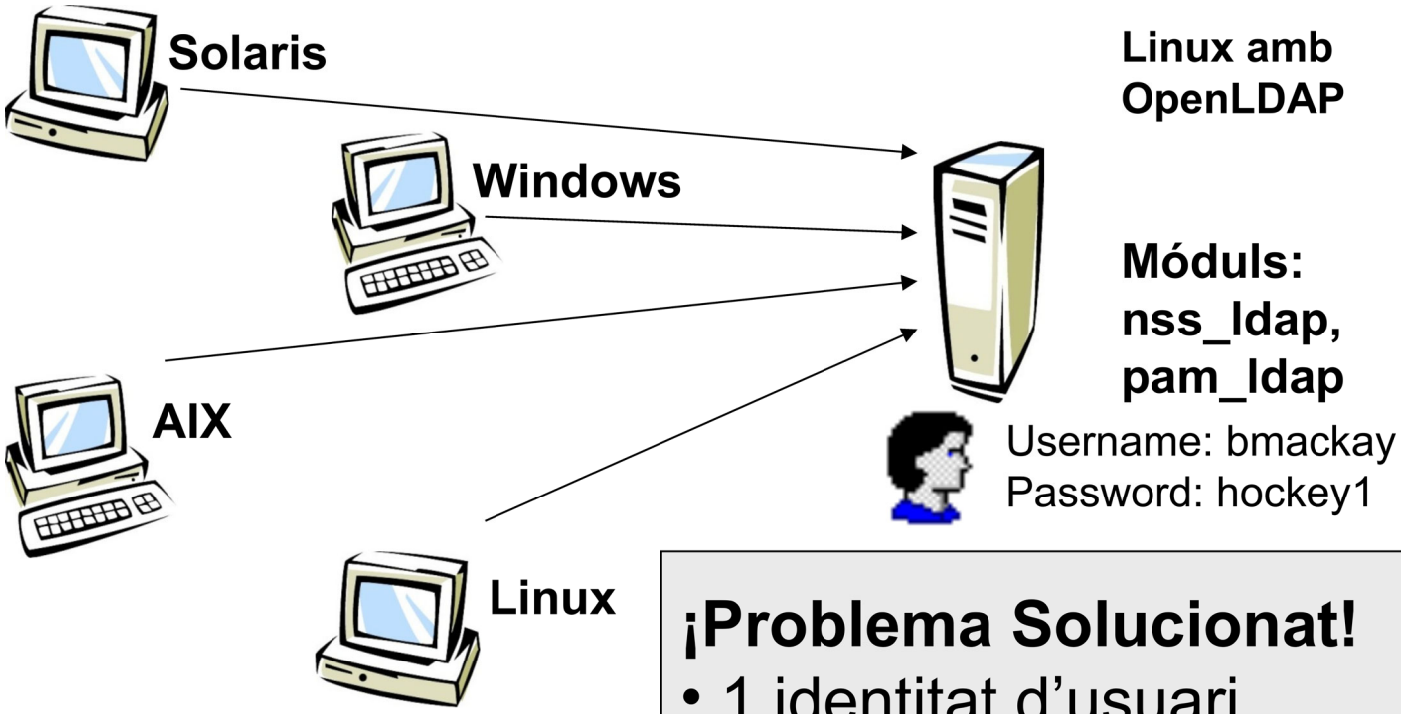
Desavantatges:

- Les utilitats i serveis per a autenticar-se han de ser “PAM enabled” (es a dir escrits en PAM API)

RFC2307

Proposta amb OpenLDAP i PAM_LDAP

Proposta amb OpenLDAP



¡Problema Solucionat!

- 1 identitat d'usuari
- 1 eina d'Admin.
- 1 emmagatzematge de claus

Ambients Ideals

- Utilització d'un ambient mixt UNIX i Windows
- Cerca d'un ambient heterogeni segur
- Canvis o rotació de personal
- Maneig de 50+ usuaris UNIX/Linux

Missatges Claus

- Estableix una única identitat per a usuaris UNIX, Linux i Windows
- Proveeix alt nivell de seguretat en la xarxa (SSL i Kerberos)
- Centralitza l'administració d'identitats de usuaris UNIX, Linux i Windows
- Brinda suport per a múltiples plataformes
- S'integra en forma transparent en les estacions de treball dels usuaris

Casos d'exit

- Guardia di Finanza: 3,000 usuaris
- UK Ministry Of Defense: 1,600 usuaris que accedeixen a varies aplicacions, incloent una d'estadístiques de tripulació aérea
- Dynatronics - EEUU: Autenticant 40 usuaris que accedeixen aplicacions contables en Linux

- LDAP

Què és LDAP?

- Es un protocol lleuger d'accés a directoris que permet gestionar informació jeràrquica per a mantenir-la actualitzada i disponible en la xarxa
- LDAP = Lightweight Directory Access Protocol
- És una versió simplificada del pesat X.500 DAP protocol del modelo OSI de 1990

Què és LDAP?

- LDAP va néixer en Julio de 1993 amb el RFC 1487 (RFC 1777)
- La informació es guarda en una BD de tipus jeràrquica
- El promig de lectura en la BD es major a la d'escriptura

Perquè serveix LDAP?

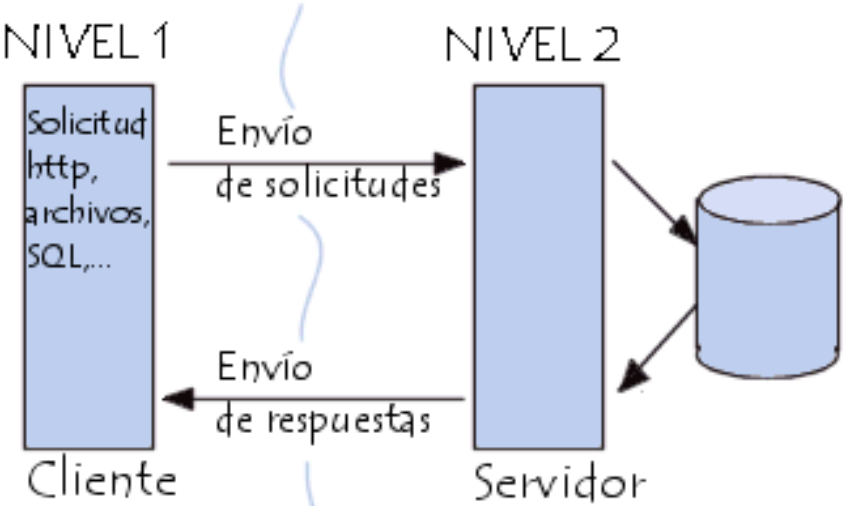
- Si ets un administrador: es pot administrar de forma centralitzada usuaris, grups, dispositius
- Pots aïllar las aplicacions dels directoris ex: correu electrònic
- Si ets un IT manager: Et permet renunciar a estar amarrat a un sol proveïdor i/o sistema operatiu
- Disminueix costos. Baixa el TCO (*Total Cost of Ownership*) al reduir el total de diferent directoris que es necessiten administrar

Perquè serveix LDAP?

- Si ets un desenvolupador: Et permet renunciar a estar amarrat a un sol proveïdor i/o sistema operatiu
- Estalvia temps de desenvolupament ja que no ha de desenvolupar un altre vegada el seu propi sistema de directoris per a usuaris, grups, objectes, etc

Arquitectura

- Es basa en l'arquitectura client servidor de dos nivells
- És un pro
- Hi ha dos tics i els dinà
- Offline di ajuden a Directori ia de televis llibreries, biblioteques, etc



Arquitectura

- Online directoris:
- Canvien de forma dinàmica, han de ser flexibles, ha de ser segurs i han de personalitzar-se al gust de l'usuari
- Han de ser actualitzat per l'usuari propietari de la informació
- Ex: Directori d'empleats en una empresa per a localitzar-les quan canvien les seves dades de tel, fax, etc, directori d'hotels per als que passa un funcionari, etc

Productes Comercials

- Netscape´s Directory Server
- Innosoft Distributed Directory Server
- Lucent Technologies Internet Directory Server
- Sun Microsystem´s Directory services
- IBM´s DSSeries LDAP Directory
- Microsoft Active Directory server
- Novell Suse Open Exchange - Mail
- SCOoffice Server - Mail
- Tarantella – Broker d'aplicacions

Competidors

- iPlanet de Netscape
- eDirectory de Novell
- Novell directory
- Active directory de Microsoft

Website: www.openldap.org

- Software en format rpm o font es pot obtenir de www.openldap.org:
- És heretat de la versió 3.3 de la Univ.Michigan
- A Julio de 2010 la versió actual és la OpenLDAP 2.4.23

Format de presentació

- LDIF: Format de representació de dades
- Codi ASCII que es pot passar com missatges d'e-mail (8 bit clean)
- Una entrada LDIF està formada per varies línies
- Inicia amb la paraula "DN", seguit del nom únic que identifica la línea ó entrada en la BD

Format de presentació

- El registre DN ha d'ocupar una sola línea
- Després segueixen els atributs de l'entrada
- Cada atribut ha d'anar en una línia diferent
- Cada atribut ha d'estar seguit pel signe ":" i a continuació el seu valor

Exemple

- **dn:o=Acis,c=CO**
- o:Acis
- objectclass:organization
- **dn: cn=Juana, o=Acis, c=CO**
- cn: Juana
- sn: Zamora
- telephoneNumber: 781 784 7547
- objectclass:inetOrgPerson

Explicació

- Dn: significa distinguished (Distinguit)
- ObjectClass: (Tipus d'objecte)
- Cn: significa Common name (Nom Comú)
- Sn: significa surname (Cognom)
- Telephonenumber: (Número de tel)
- Uid: Compte de l'usuari
- userPassword: Clau de l'usuari
- Mail: (e-mail de l'usuari)

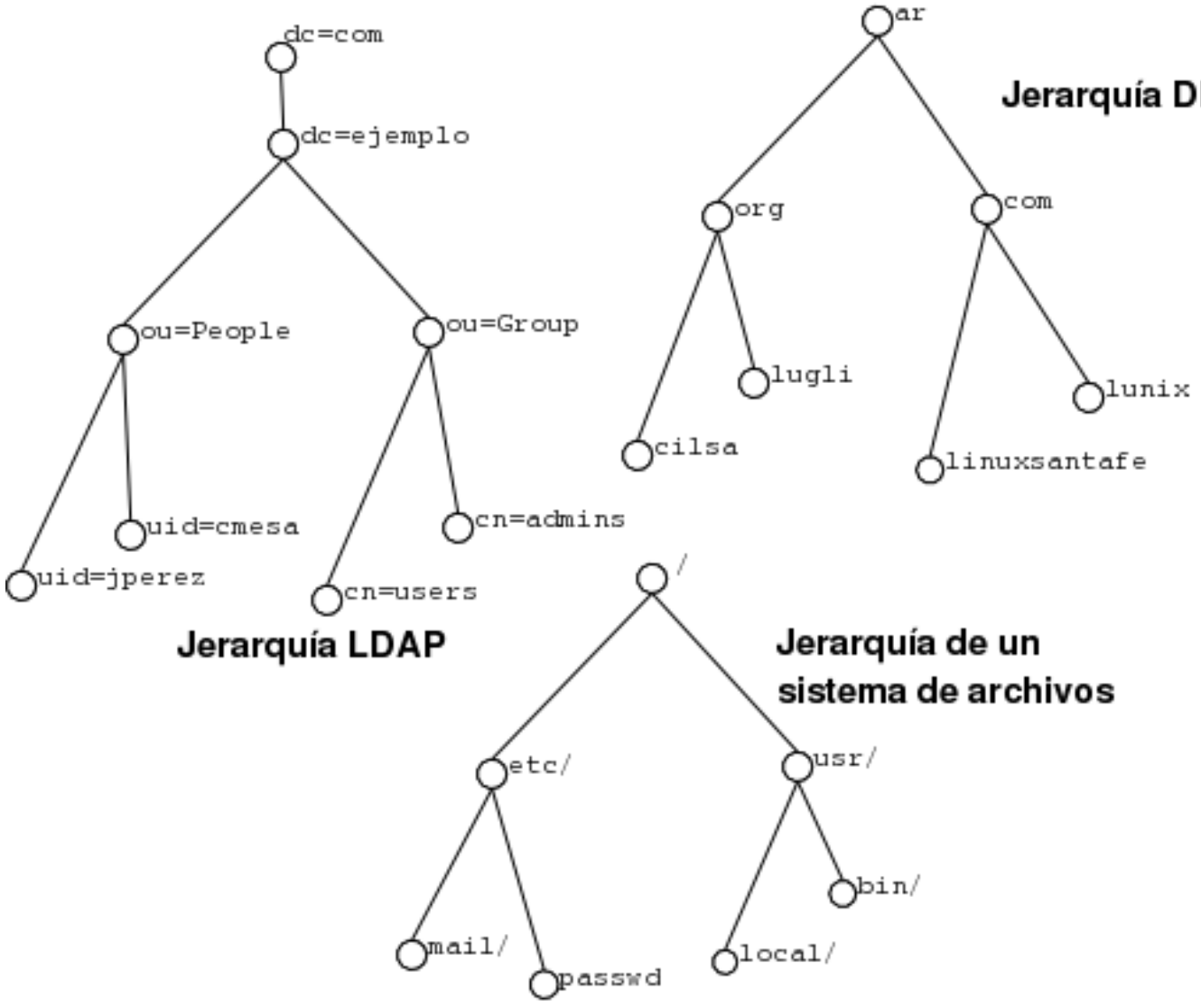
Explicació

- Description: (Descripció de l'objecte)
- O: Significa organization (Nom de l'empresa)
- C: significa country (país)
- És a dir primer és té un tipus d'atribut i després el valor de l'atribut

Explicació

- El significat de cada atribut està definit en els arxius de tipus “schema” residents en el directori: /etc/openldap/schema/core.schema, /etc/openldap/schema/cosine.schema, /etc/openldap/schema/inetorgperson.schema

Exemple


dc=com
dc=ejemplo
ou=People
ou=Group
uid=cmesa
uid=jperez
cn=admins
cn=users
Jerarquía LDAP
ar
org
com
lugli
cilsa
lunix
linuxsantafe
Jerarquía DNS
/
etc/
usr/
mail/
passwd
bin/
local/
Jerarquía de un sistema de archivos

- Arxius de configuració

Arxius de configuració: slapd

- El procés servidor en binari de ldap es diu: slapd
- Escolta pel port tcp 389
- slapd significa: Stand-alone LDAP Daemon

Configuració

- El shell d'arrencada /etc/init.d/ldap crida al servei slapd i aquest a la vegada busca l'arxiu de configuració /etc/openldap/slapd.conf
- Ambient per defecte /etc/openldap/ldap.conf
- Directori de dades: /var/lib/openldap

Arxius de configuració: slapd.conf

- # Indica els atributs i objectes que LDAP pot manejar per cada registre
- Include /etc/openldap/schema/core.schema
- Include /etc/openldap/schema/cosine.schema
- Include /etc / openldap / schema / inetorgperson.schema
- # Permet compatibilidad amb l'antiga versió 2 – Falla en RH 9.x
- allow bind_v2

Arxius de configuració: slapd.conf

- # Tipus de xifrat en els passwords dels usuaris
- password-hash {Format}
- # On format pot ser algun algoritme de xifrat simètric com: {SSHA}, {SHA}, {SMD5}, {MD5}, {CRYPT}, {CLEARTEXT}

Slapd.conf

- # Indica el format de la base de dades
- database ldbm
- # Esta és la base de la clau principal
- suffix o=Acis, c=CO
- # És el directori on resideix els arxius de la base de dades LDAP
- directory /var/lib/ldap

Slapd.conf

- # Aquest és la base del registre per a l'administrador
- rootdn cn=root, o=Acis, c=CO
- # Aquest és el password de l'administrador
- rootpw {SSHA}msyaU45hcXmiq8ahe9OkewOCKKA4A5EY

Slapd.conf

- La clau de l'usuari administrador es pot xifrar

amb la comanda:

slappasswd –h Format > arxiu

- On Format pot ser algun algoritme de xifrat

simètric:

- {SSHA}, {SHA}, {SMD5}, {MD5}, {CRYPT}, {CLEARTEXT}

Slapd.conf

- Nota: Mai utilitzis {CLEARTEXT} donat que si un intrús veu l'arxiu pla pot coneixer la clau de l'administrador.
- Es recomana en canvia l'algoritm més fort {SSHA}

/etc/openldap/ldap.conf

- L’arxiu client /etc/openldap/ldap.conf ha d’estar configurat de la següent forma:
- HOST 127.0.0.1
- BASE o=Acis, c=CO
- PORT 389

Arxiu de dades: ldif

- **dn:** **o=Acis,c=CO**
- o: Acis
- postalAddress: Calle 93 con 13A
- objectclass: organization
- **dn:** **cn=Juana, o=Acis, c=CO**
- cn: Juana
- sn: Zamora
- description: Soport en Windows
- uid: acarvaja
- **userPassword**:{SSHA}msyaU45hcXmiq8ahe9OkewOCKKA4A5EY
- displayname: Armando Carvajal - sistemes
- mail: acarvaja@acis.org.co
- carLicense: 77036182
- homePhone: 571 528 3101
- objectclass:inetOrgPerson

Comandes:

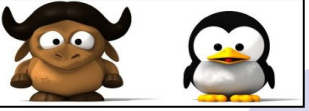
- Consultar si “openldap” esta instal·lat:
- # rpm –q openldap
- Hacer backup de la base de dades en format LDIF:
- # slapcat –l backup.ldif
- Pujar les dades fets per un backup en format LDIF:
- # slapadd –l backup.ldif

Comandes:

- Per a generar un password xifrat de tipus hash:
- # slappasswd –h metode de xifrat
- Per a xifrar el password del client al servidor:
- # stunnel –c –d 389 –r localhost:636

Altres comandes:

- Per a veure tots els registres de la BD:
- #ldapsearch –x –b ´o=Acis,c=CO´ ´objectclass=*´
- Per a veure els usuaris de la BD:
- #ldapsearch –x –b ´o=Acis,c=CO´ ´uid=*´
- Per a addicionar registres des de l'arxiu bd.ldif:
- #ldapadd –x –D ´uid=acarvaja,o=Acis,c=CO´ -W –f bd.ldif



Webgrafia i/o material

- www.ldapguru.com
- www.openldap.org
- Bibliografia
  - Understanding And Deploying LDAP Directory Services, Timothy A. Howes Ph.D, New Riders, 1999, Netscape Communications Corporation, First Edition
  - Implementing LDAP, Marck Wilcox, Editorial Wrox