M6 - Administració de SO

NF1 - Administració de serveis de directori II

SERVEIS DE DIRECTORI

Un **directori** és una base de dades especialitzada (també anomenada **repositori de dades**) que emmagatzema informació sobre objectes i que està específicament dissenyada per optimitzar les operacions de consulta.

Un **servei de directori** és el programari que emmagatzema, organitza i facilita l'accés a la informació d'un directori.

SERVEIS DE DIRECTORI

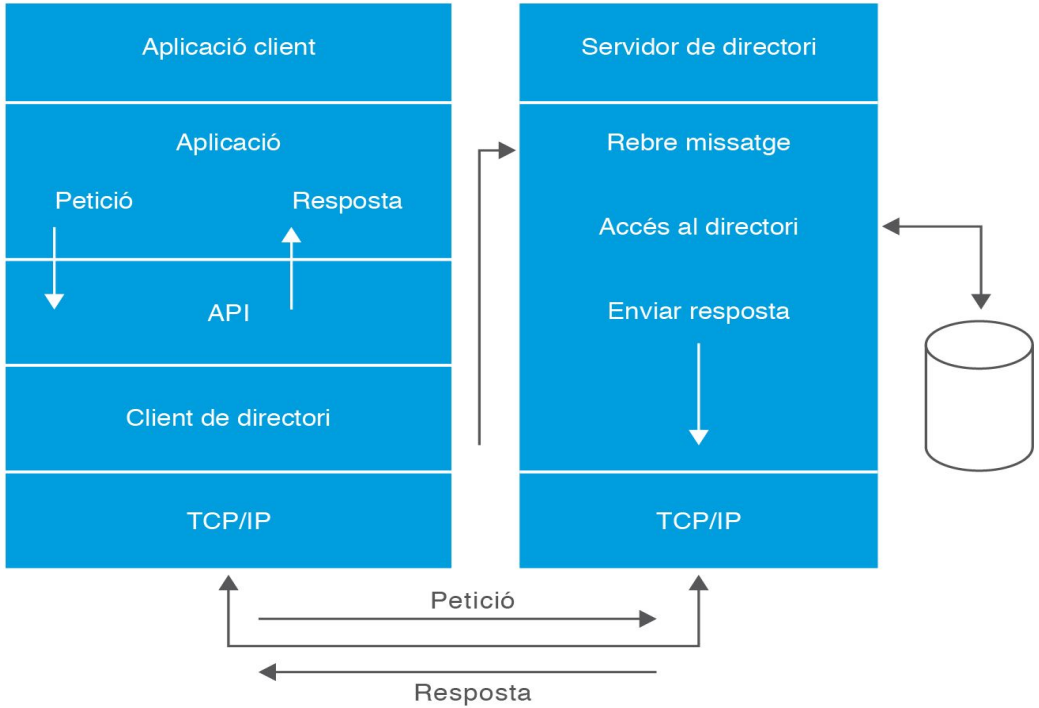
La informació que contenen està basada en objectes (cada objecte és una entrada del directori) i en els atributs d'aquests objectes.

Les actualitzacions i modificacions de les dades són simples i no gaire freqüents.

Estan optimitzats per donar una resposta ràpida a operacions de cerca i revisió.

Poden replicar la informació per augmentar-ne la disponibilitat i la fiabilitat alhora que disminueix el temps de resposta a les consultes.

SERVEIS DE DIRECTORI



SERVEIS DE DIRECTORI: Usos de Ldap

- Bases de dades de:
  - Adreces de correu electrònic .
  - Dades de recursos humans (directoris d'empresa).
  - Claus públiques de seguretat.

SERVEIS DE DIRECTORI: Usos de Ldap

- Quan utilitzar Ldap?
  - Quan és vol accedir a la base de dades des de diferents plataformes i des de múltiples ordinadors i aplicacions.
  - Els registres de la base de dades canvien poc (poques vegades al dia o menys).

SERVEIS DE DIRECTORI: Usos de Ldap

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

Ofereix:


Encriptació via protocol SSL,


Mecanismes d'autenticació per accedir d'una manera segura.

SERVEIS DE DIRECTORI: LDAP

- Acrònim anglès de lightweight directory access protocol. **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.

- Protocol de xarxa (nivell aplicació) que permet l'accés a un servei de directori per tal de compartir informació en una xarxa.

SERVEIS DE DIRECTORI: LDAP

Té quatre models d'implementació:

1. El **model d'informació** descriu l'estructura de la informació emmagatzemada en el directori LDAP.

2. El **model de noms** descriu com s'organitza i identifica la informació en el directori LDAP.

SERVEIS DE DIRECTORI: LDAP

3. El **model funcional** descriu quines operacions poden ser realitzades amb la informació emmagatzemada en el directori LDAP.

4. El **model de seguretat** descriu com es pot protegir la informació continguda en el directori LDAP davant d'intents d'accés no autoritzats.

LDAP Model d'informació

- 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 o entrada de servei de directori), es representa en forma de branques.

- La branca localitzada a **l'arrel** és **l'entrada arrel**.

LDAP Model d'informació

- 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.*

LDAP Model d'informació

- 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).

LDAP Model d’informació

- **L'organització del directori segueix una estructura d'arbre invertit**
  - Un directori és un arbre d'entrades de directori (nodes de l'arbre)
  - Cada entrada és pot considerar com un objecte amb un conjunt d'atributs
  - Els atributs tenen un nom, una descripció i un o més valors.

LDAP Model de noms

- Cada entrada té un identificador únic anomenat Distinguished Name (DN).
  - ***DN** (Distinguished Name): fent una similitud amb un sistema de fitxers és el camí absolut al fitxer.*

- Cada entrada té un RDN (Relative Distinguished Name) que la distingeix de la resta d'entrades del mateix node de l'arbre.
  - ***RDN** (Relative Distinguished Name): és el camí relatiu a un fitxer.*

LDAP Model de noms

- El DN d'una entrada es forma pel RDN de la entrada més el DN del node pare. Per tant els DN són composicions de RDN:
  - **DN= RDN(fill), RDN(pare),RDN(avi), ..., RDN(arrel)**

- Els RDN són parells de valors formats per un atribut (o clau) de l'entrada més el seu valor
  - **nom_atribut=valor**

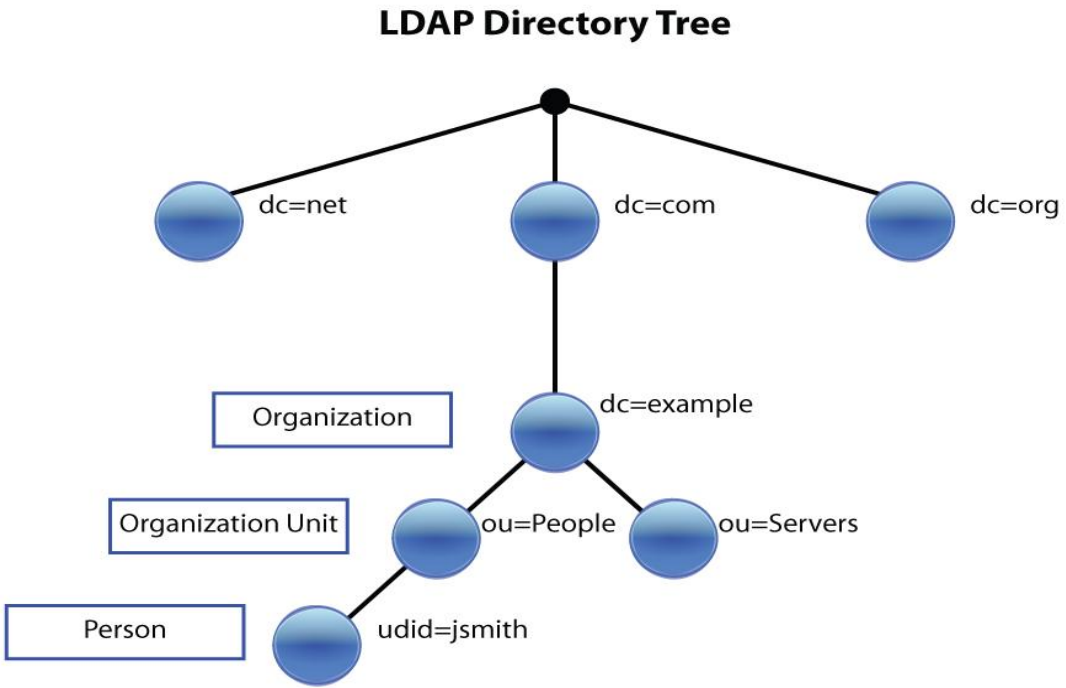
LDAP Model de noms.

- La identificació unívoca d'una entrada depèn de la utilització correcta de parells de valors o claus.

LDAP Model de noms.

- El conjunt de claus que es fa servir normalment són:
  - ***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.*
  - ***ou*** *(organizational unit): és el departament de l'organització o companyia on treballa aquesta persona.*
  - ***mail****: és l'adreça de correu electrònic personal*

LDAP Arbre


LDAP Directory Tree
dc=net
dc=com
dc=org
Organization
dc=example
Organization Unit
ou=People
ou=Servers
Person
udid=jsmith

LDAP Model Funcional.

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 Model de seguretat.

- El model de seguretat mostra com es controla l'accés a la informació continguda en el directori.

- Abans que un client pugui accedir a les dades d'un servidor LDAP s'han de dur a terme dos processos:
  - Autenticació
  - Autorització (protecció de recursos)

LDAP Model de seguretat.

- El model de seguretat descriu aquests processos juntament amb la integritat i confidencialitat en la transmissió de dades o la limitació en l'ús de recursos.

- LDAP també ens dóna un format d'intercanvi de dades (L'LDIF: LDAP Data Interchange Format o format d'intercanvi de dades LDAP).

LDAP. LDIF.

- LDIF és un estàndard de format de text pla utilitzat per representar el contingut d'un directori LDAP i les sol·licituds d'actualització del directori (afegir una entrada, modificar-la, eliminar-la...).
  - *LDIF permet exportar i importar dades d'un directori 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.

LDAP. LDIF.

- La sintaxi del format LDIF és la següent:

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

Exemple de seqüència d'entrada

```
dn: ou=Persones, dc=empresa,dc=com
ou: Persones
objectClass: organizationalUnit
```

LDAP. LDIF.

- Els fitxers LDIF són molt sensibles als espais i les línies en blanc.
- S'ha de ser molt respectuós amb la sintaxi del format.

LDAP. LDIF.

- En els fitxers LDIF:
  - 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.

LDAP. Dominis.

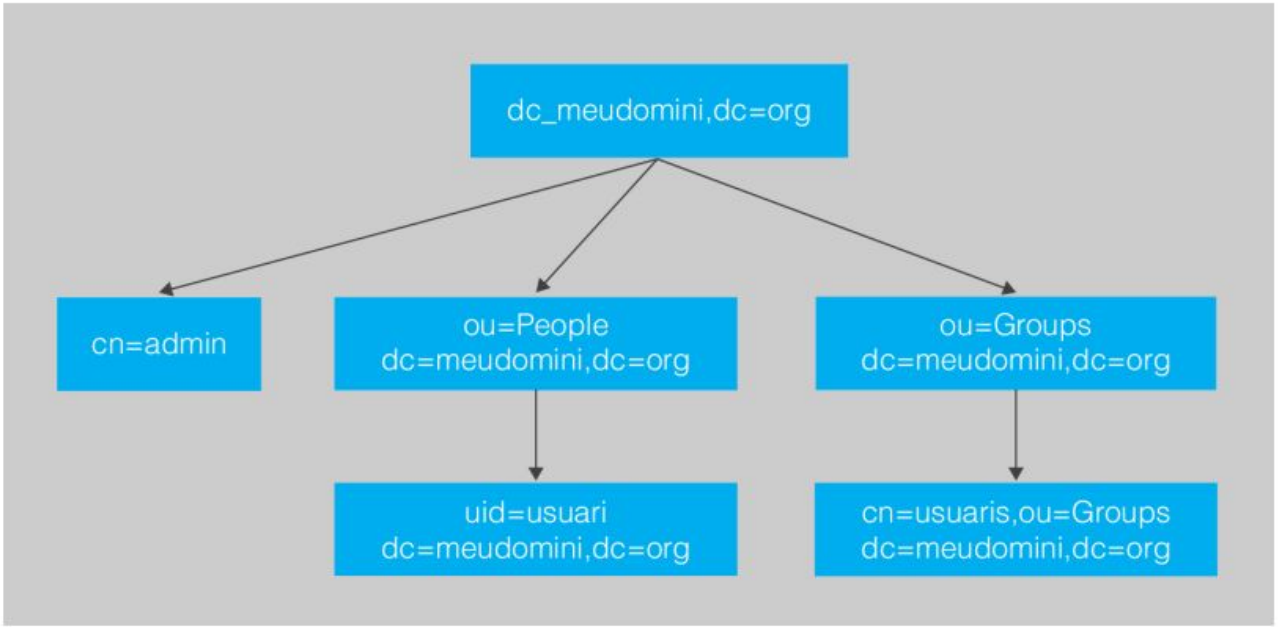
- En un domini creat emb LDAP, tenim una sèrie d'elements que són prefixats:
  - **Usuari administrador (cn=admin):** és l'usuari amb drets d'administració (pot crear, eliminar i modificar els usuaris i els grups del domini)

LDAP. Dominis.

- **Unitat organitzativa People (ou=People):** inclou tots els usuaris individuals del domini.

- **Unitat organitzativa Groups (ou=Groups):** inclou tots els grups d'usuaris.
  - S'han d'agrupar els usuaris en funció de característiques semblants (en funció dels drets i dels permisos d'accés a recursos)
  - Els grups del domini s'han de crear abans que els usuaris individuals.

LDAP. Dominis.

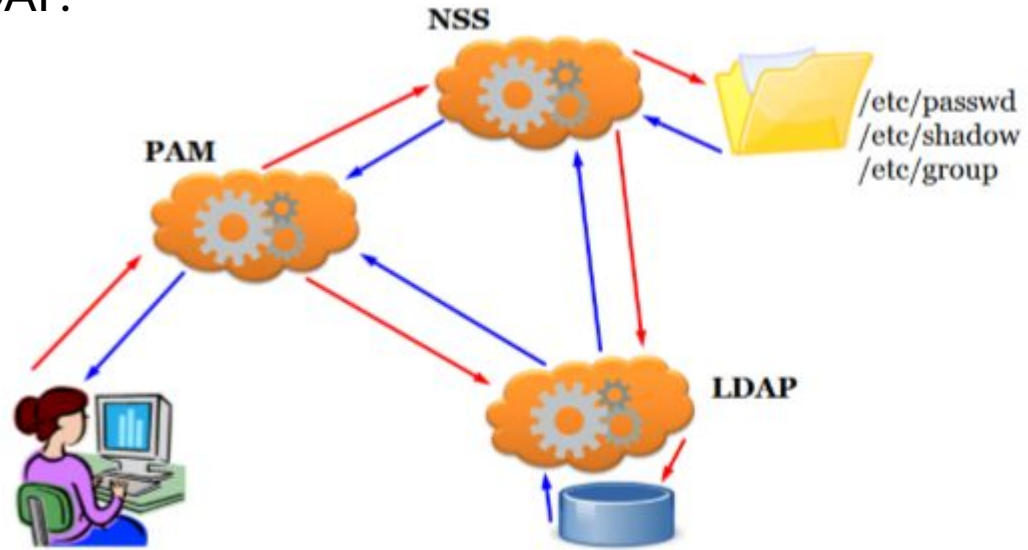


LDAP. Dominis.

- A l'hora de dissenyar un domini, com a mínim, hem d'especificar:
  - **Extensió del domini** (dc=com o dc=org ...)
  - **Nom del domini** (dc=dominiexemple o dc=insestatut)
  - Unitat organitzativa **People** (ou=People)
  - **Usuaris del sistema** (uid=eva)
  - Unitat organitzativa **Group** (ou=Group)
  - **Grups d'usuaris del sistema** (cn=informativa)

LDAP. Autenticació.

- Es fa mitjançant una combinació de les eines: PAM, NSS i LDAP.



LDAP. Autenticació.

- **PAM (Pluggable Authentication Modules)**
  - Mecanisme que proporciona interfície entre aplicacions d'usuari i mètodes d'autenticació.
  - Ho fa de forma transparent:
    - és el mateix identificar mitjançant usuari-contrasenya què amb identificació biomètrica.

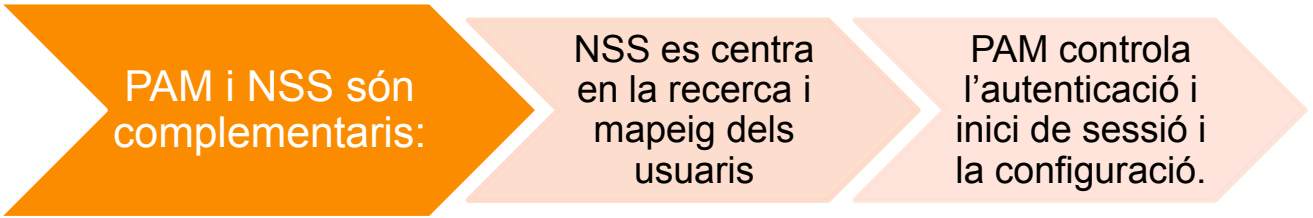
LDAP. Autenticació.

❑ NSS (Name Service Switch)

- ❑ Permet la resolució de noms d'usuaris i contrasenyes (o grups) mitjançant l'accés a diferents origens d'informació.

- ❑ S'han de fer canvis als fitxers:
  - ❑ /etc/passwd
  - ❑ /etc/shadow
  - ❑ /etc/group

LDAP. Autenticació.



LDAP. Autenticació. Preparació servidor i client

- Instal·lació de llibreries NSS i PAM, interacció amb LDAP i dependències:
- ***apt-get install libnss-ldap libpam-ldap ldap-utils -y***
- Aquest procés inicia l'assistent que permet configurar el comportament de:
  - ***ldap-auth-config per Ubuntu***
  - ***libnss-ldap per Debian***
- Per qualsevol modificació:
  - ***dpkg-reconfigure ldap-auth-config***

LDAP. Autenticació. Preparació servidor i client

- Modificar arxius configuració NSS i PAM
  - **NSS:**
    - ***/etc/nsswitch.conf***
      - Buscar passwd:, group:, shadow: i ***afegir ldap***
  - **PAM:**
    - Perquè l'usuari pugui canviar el seu password:
      - ***/etc/pam.d/common-password***
        - Buscar [success=1 ..] a dintre ***use_authtok*** i ***treure-l'***

LDAP. Autenticació. Preparació servidor i client

- Per crear carpetes per cada usuari a l'inici de sessió:
  - ***/etc/pam.d/common-session*** afegir la linia:
    - ***session optional pam_mkhomedir.so skel=/etc/skel umask =077***

LDAP. Autenticació. Preparació servidor i client

- Comprovar dades fitxers:
  - ***/etc/ldap.conf***
  - ***/etc/ldap/ldap.conf***
    - ***host***
    - ***dc***
    - ***uri***
    - ***rootbinddn***
    - ***ldap_version***
    - ***bind_policy soft***

LDAP. Autenticació. Exclusiu al servidor.

- Configuració autenticació client mitjançant l'script auth-client-conf que ajuda a modificar arxius de configuració de PAM i NSS:
  - ***sudo auth-client-config -t nss -p lac_ldap***
- Un cop executat, cal actualitzar polítiques de PAM:
  - ***Sudo pam-auth-update***

LDAP. Autenticació. Exclusiu al client.

- Habilitar dimoni libnss-ldap amb el paquet sysv-rc-conf
  - ***apt-get install sysv-rc-conf -y***

- Un cop instal·lat:
  - ***sysv-rc-conf libnss-ldap on***

- I ja podríem verificar al terminal, els usuaris.

LDAP. Autenticació. Exclusiu al client.

- Ús de gestor de sessions (interfície d'autenticació) ***LightDM***:
  - Només deixa fer **login** a **usuaris que ja coneix**.
  - Per permetre l'**ús amb qualsevol usuari** s'han de **modificar dos arxius**:
    - ***Afegir: greeter-show-manual-login=true*** a:
      - ***/usr/share/lightdm/lightdm.conf.d/50-ubuntu.conf***
      - ***/usr/share/lightdm/lightdm.conf.d/50-unity-greeter.conf***