M6 - Administració de SO

NF1 - Administració de servei de directori

Escenaris heterogenis

- El model de xarxa determina quin és el rol dels equips que la integren.
  - Aquest depèn en major o menor mesura de les necessitats de l'organització.
- En aquest aspecte es pot distingir entre:
  - Xarxes igualitàries
  - Xarxes centralitzades

XARXES IGUALITÀRIES

- Les Xarxes Igualitàries es van dissenyar per **compartir recursos** desde màquines d'escriptori amb altres usuaris de la xarxa.

- En una Xarxa Igualitària, cada ordinador (*host*) pren el rol de **client i servidor**.

XARXES IGUALITÀRIES

- *Cadascuna de les màquines determina els recursos que ofereix a la resta i és responsable de la seva pròpia seguretat.*

- *Els usuaris poden encendre o apagar les seves màquines sense por d'interrompre altres usuaris o serveis de la xarxa (excepte quan estan accedint a recursos propis de la màquina que apaguem).*

- Aquest escenari és el més comú quan la xarxa té un nombre reduït d'ordinadors.

XARXES CENTRALITZADES

- El model de **xarxa d'igual a igual**, o d'entorn de treball, funciona relativament bé quan s'implanta en un entorn amb un grup d'usuaris **reduït** i amb pocs equips.

- A mesura que el nombre d'ordinadors connectats a la xarxa va augmentant, l'administració dels recursos, dels usuaris i dels permisos comença a ser una **tasca tediosa**.

XARXES CENTRALITZADES

- En les xarxes grans, els usuaris i les màquines s'acostumen a agrupar en **dominis**:
  - administració dels recursos
  - permisos

} **CENTRALITZATS**

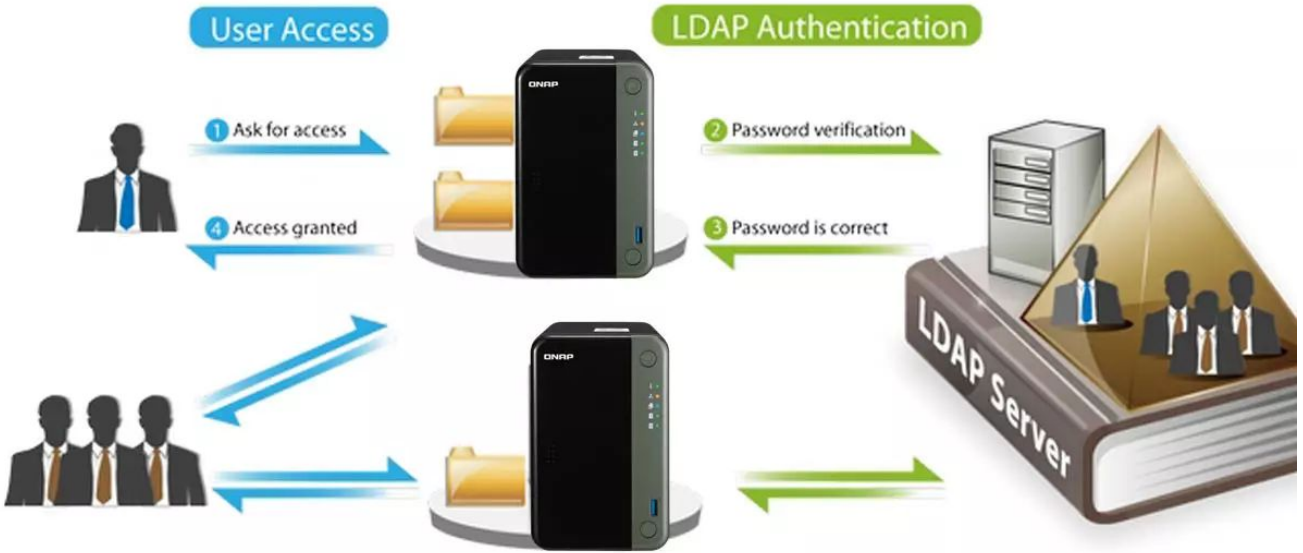
XARXES CENTRALITZADES

- Un **domini** és:
  - un conjunt d'ordinadors
    - ✔ *interconnectats en xarxa*
    - ✔ *que formen part d'una estructura jerarquitzada*
    - ✔ *gestionada de manera centralitzada des d'un servidor*

XARXES CENTRALITZADES

- Un servidor és el que s'encarrega del control d'accés als recursos □ Esquema **client-servidor**.
  - **Ex: Inici de sessió**
    - Validació credencials usuari
    - Obtenir dades creació context
  - **Desavantatges** □ dependència disponibilitat servidor
    - *Solució: servidors de reserva (backups)*

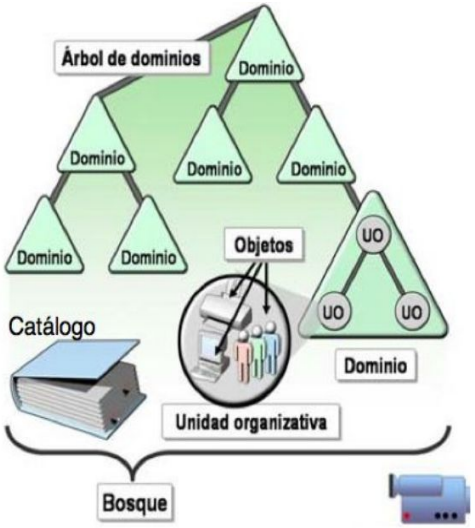
XARXES CENTRALITZADES



XARXES CENTRALITZADES

- **DOMINIS EN WINDOWS: Active Directory (AD)**
- **AD. Estructura Lògica.**
  - L'**estructura lògica**, **busca** tenir-ho tot organitzat per f**acilitar la localització i administració dels recursos.**
  - **Una de les funcions més importants d'AD és poder configurar els equips del nostre domini i poder establir permisos i restriccions als nostres usuaris.**

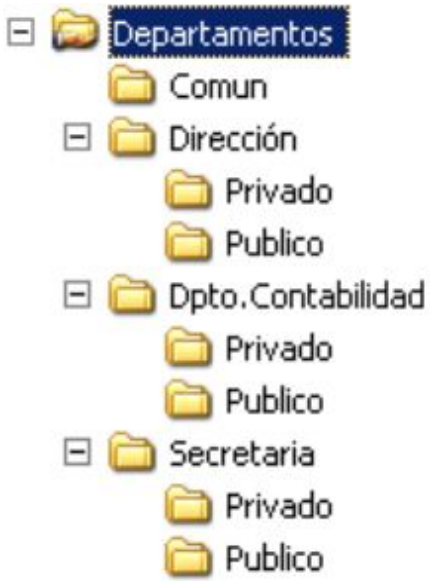
XARXES CENTRALITZADES



- **DOMINIS EN WINDOWS: Active Directory (AD)**

- **AD. Estructura Lògica**
  - Conté objectes, dominis, arbres i boscos.
  - Per tenir aquest gran control sobre tots els recursos és necessari construir una bona estructura.
  - Aquesta **estructura** és **jeràrquica** i similar a una base de dades.

XARXES CENTRALITZADES



- **DOMINIS EN WINDOWS: Active Directory (AD)**

- **AD. Estructura Lògica**
  - **Dominis**.
    - Es tracta de les unitats centrals en l'estructura lògica.

      - Simplificant, representen la unitat superior en una Empresa mitjana (PIME) i permet aplicar directives a tots els equips i usuaris d'una sola vegada.

XARXES CENTRALITZADES

- **DOMINIS EN WINDOWS: Active Directory (AD)**

- **AD. Estructura Lògica**
  - **Arbres de dominis “Domain Tree”.**
    - Són els dominis agrupats en <u>estructures jeràrquiques</u>.
      - En afegir un segon domini a un arbre, esdevé **secundari** del domini arrel de l'arbre.
      - El domini al qual està adjunt un domini secundari s'anomena domini **primari**.

XARXES CENTRALITZADES

- **DOMINIS EN WINDOWS: Active Directory (AD)**
- **AD. Estructura Lògica**
  - **Arbres de dominis “Domain Tree”.**
    - Un domini secundari pot tenir al seu torn el seu propi domini secundari, etc.
      - El nom d'un domini secundari es combina amb el nom del seu domini primari per formar el seu propi nom únic ***DNS***.
        - *Ex: rubi.miempresa.com, terrassa.miempresa.com.*
      - D'aquesta manera, l'arbre disposa d'un a ***espai de noms contigu.***

XARXES CENTRALITZADES

- **DOMINIS EN WINDOWS: Active Directory (AD)**
- **AD. Estructura Lògica**
  - **Arbres de dominis “Domain Tree”.**
    - Un domini secundari pot tenir al seu torn el seu propi domini secundari, etc.
      - El nom d'un domini secundari es combina amb el nom del seu domini primari per formar el seu propi nom únic ***DNS***.
        - *Ex: rubi.miempresa.com, terrassa.miempresa.com.*
      - D'aquesta manera, l'arbre disposa d'un a ***espai de noms contigu.***

XARXES CENTRALITZADES

- **DOMINIS EN WINDOWS: Active Directory (AD)**

- **AD. Estructura Lògica**
  - **Bosc “Forest”.**
    - Consta d'un o d'un conjunt d’arbres de domini amb relacions de confiança entre ells.

    - Defineix l’esquema,
      - conté la definició i els atributs de tots els objectes,
      - conté la informació de replicació
      - manté el catàleg global que proporciona capacitats de cerca per a ell mateix.

    - ~~És un espai de noms no contigu.~~

XARXES CENTRALITZADES

- **DOMINIS EN WINDOWS: Active Directory (AD)**

- **AD. Estructura Lògica**

  - **Catàleg**.
    - És un repositori d'informació que conté una mena d'índex de tots els objectes i els seus atributs associats (més significatius) de tot el directori.

    - Serveix com a referència ràpida per trobar un determinat recurs (per exemple, una impressora) de manera més eficient que no haver d'anar preguntant domini per domini.

XARXES CENTRALITZADES

- **DOMINIS EN WINDOWS: Active Directory (AD)**

- **AD. Estructura Lògica.**
  - **Objectes**.
    - Són els components més bàsics de l'estructura lògica.

    - Pot ser un usuari, una carpeta compartida, una impressora, un equip etc.
      - Cadascú amb els seus atributs particulars associats (classe Impressora: marca, ip, nivell tinta ...)

XARXES CENTRALITZADES

- **DOMINIS EN WINDOWS: Active Directory (AD)**

- **AD. Estructura Lògica.**
  - **Objectes**.
    - Cada objecte en AD té una identitat única (GUID, Globally Unique Identifier).

      - *Els objectes es poden moure o canviar el nom, però el seu GUID mai canvia.*
      - *Els objectes es coneixen internament pel GUID, no pel seu nom actual.*
      - *El GUID és un atribut,objectGUID, que forma part de tot objecte i no es pot modificar ni esborrar i farà de "KEY" per les BBDD*

XARXES CENTRALITZADES

- **DOMINIS EN WINDOWS: Active Directory (AD)**

- **AD. Estructura Lògica.**
  - **Unitats Organitzatives (UO)**.
    - És un objecte que conté altres objectes i ens servirà per organitzar la nostra estructura.
      - *Això simplifica l'administració i la fa més lògica i propera a la nostra empresa.*
    - Es basen en 3 criteris fonamentals:
      - Ubicació geogràfica (Perú, Canadà, etc...)
      - Àrea o Departament (Comptabilitat, Ventes, Gerència, etc...)
      - Càrrec o funció (empleats, Gerents, Administradors, alumnes, etc.)
    - **No hi ha limit d'OUs “nested”**

XARXES CENTRALITZADES

- **DOMINIS EN WINDOWS: Active Directory (AD)**

- **AD. Estructura Lògica.**
  - **Usuari.**
    - Representa un usuari de la xarxa i funciona com un magatzem d'informació d'identificació i autenticació.
  - **Equip.**
    - Representa un equip de la xarxa i proporciona el compte de màquina necessària perquè el sistema entreu al domini.

XARXES CENTRALITZADES

- **DOMINIS EN WINDOWS: Active Directory (AD)**

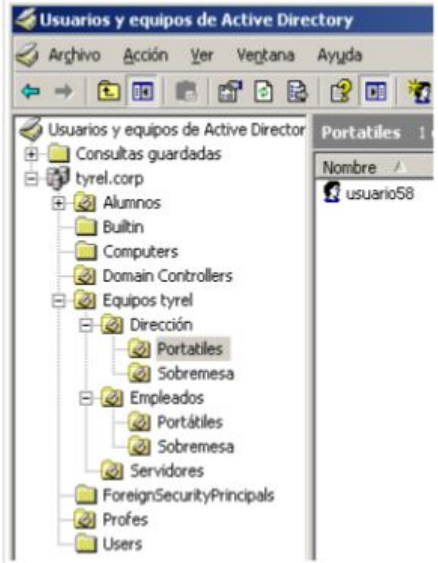
- **AD. Estructura Lògica.**
  - **Grup.**
    - Objecte contenidor que representa una agrupació lògica d'usuaris, equips o fins i tot altres grups (o els tres) que és independent de l'estructura de l'arbre d'Active Directory.
      - Els grups poden contenir objectes de diferents unitats organitzatives i dominis.
  - **InetOrgPerson.**
    - Classe d'objecte que facilita la transició des de serveis de directori aliens a Microsoft, sempre que utilitzin els protocols LDAP o X.500.

XARXES CENTRALITZADES

- **DOMINIS EN WINDOWS: Active Directory (AD)**

- **AD. Estructura Lògica.**
  - En AD (adoptat del protocol LDAP) cadascun dels objectes del directori té un identificador únic anomenat **GUID (identificador únic global).**
    - *És un nombre de 128 bits*
      - *Exemple: {25892e17-80f6-415f-9c65-7395632f0223}*
  - **Es sol fer servir el DN** (Distinguished Name), nom simbòlic que també identifica a fi de manera inequívoca basant a la ruta dins del domini.

XARXES CENTRALITZADES



- **DOMINIS EN WINDOWS: Active Directory (AD)**

- **AD. Estructura Lògica.**
  - Veiem un exemple.

*El **DN de l'usuario58** a la figura seria:*

LDAP :/ / cn = usuario58, ou = Portatils, ou = Direcció, ou = Equips Tyrel, dc = tyrel, dc = corp

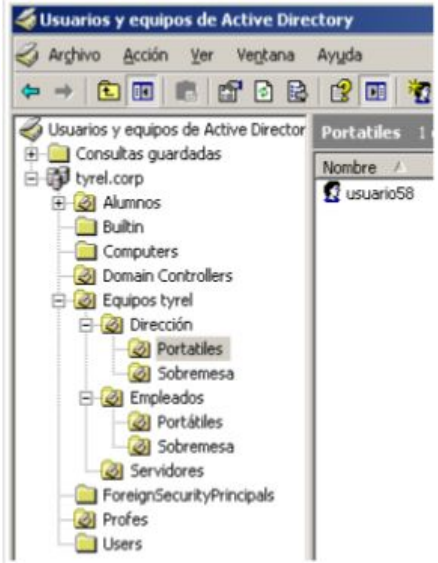
Els elements més habituals són:

- **dc (component del domini): s'usa per als dominis.**
- **ou (unitat organitzativa)**

Tot el que no sigui el domini o les OU sol etiquetar-se com cn.

- **cn (nom comú)**

XARXES CENTRALITZADES



- **DOMINIS EN WINDOWS: Active Directory (AD)**

- **AD. Estructura Lògica.**
  - Veiem un exemple.

El DN de l'usuario58 a la figura seria:
LDAP :/ / cn = usuario58, ou = Portatils, ou = Direcció, ou = Equips Tyrel, dc = tyrel, dc = corp

També hi ha el **RDN (Relative Distinguished Name),** que és simplement el nom de l'objecte sense tenir en compte la seva ruta (**cn = usuario58**).

XARXES CENTRALITZADES

- **DOMINIS EN UNIX: LDAP**

  - El sistema NIS (***Network Information Service)*** original ha demostrat tenir greus limitacions inherents al seu disseny, especialment en referència a l'escalabilitat i la seguretat.

  - Aquest fet va provocar que el reemplacessin altres tecnologies molt més potents i escalables com ara **LDAP**.

XARXES CENTRALITZADES

- **DOMINIS EN UNIX: LDAP**

  - Un domini LDAP s'estructura de manera similar a un domini NIS:
    - Hi ha servidors mestres, esclaus i clients.
    - Els clients poden obtenir informació dels mestres o esclaus, però tots els canvis han d'aplicar-se als servidors mestres.

  - Hi ha moltes implementacions d'un servei de directori LDAP, però una de les més utilitzades és **OpenLDAP**.

XARXES CENTRALITZADES

- **DOMINIS EN UNIX: OpenLDAP**

  - És un programari de codi lliure que permet adaptar-se a diverses necessitats.

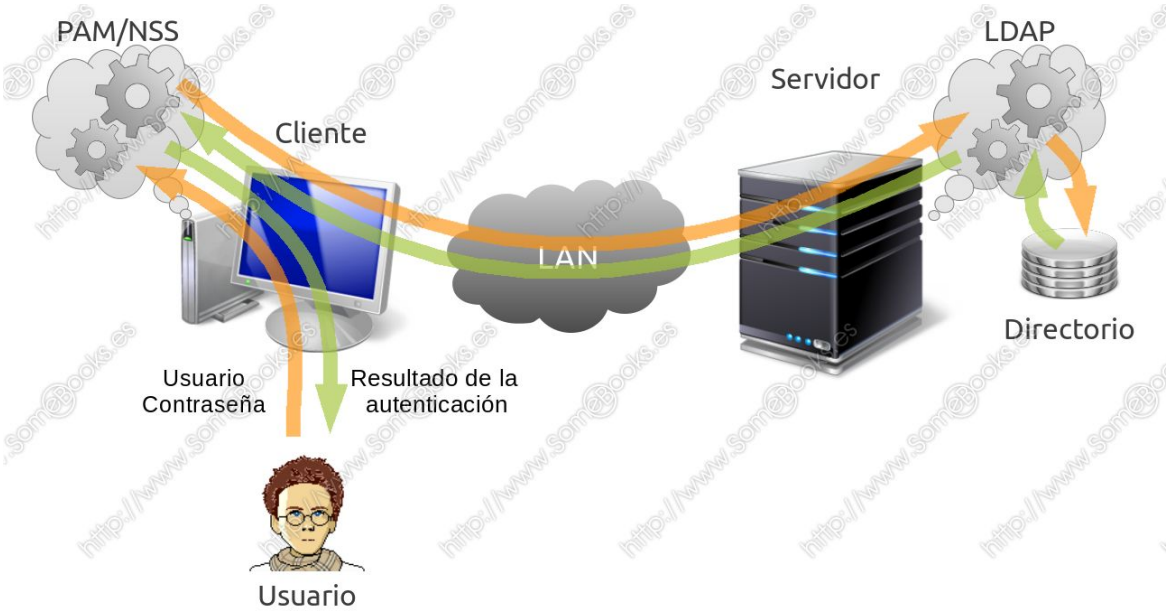
  - Es tracta d'un servei de directori **robust**, **ràpid** i **escalable**.

NSS (***N**ame **S**ervice **S**witch*) és un servei que permet la resolució de noms d'usuari i contrasenyes (o grups) mitjançant l'accés a diferents orígens d'informació.

PAM (***P**luggable **A**uthentication **M**odules*) estableix una interfície entre els programes d'usuari i diferents mètodes d'autenticació. D'aquesta manera, el mètode d'autenticació es fa transparent per als programes.

XARXES CENTRALITZADES

- **DOMINIS EN UNIX: OpenLDAP**



NSS (***N**ame **S**ervice **S**witch*) és un servei que permet la resolució de noms d'usuari i contrasenyes (o grups) mitjançant l'accés a diferents orígens d'informació.

PAM (***P**luggable **A**uthentication **M**odules*) estableix una interfície entre els programes d'usuari i diferents mètodes d'autenticació. D'aquesta manera, el mètode d'autenticació es fa transparent per als programes.

XARXES CENTRALITZADES

DOMINIS EN UNIX: OpenLDAP

- *Bàsicament, PAM complementa en alguns aspectes el funcionament de NSS ja que mentre aquest se centra en la cerca i mapatge dels usuaris, PAM controla l'autenticació, l'inici de sessió i la seva configuració.*
- *En l'actualitat, PAM és el mètode que utilitzen la majoria de les aplicacions i eines de GNU/Linux que necessiten relacionar-se, d'alguna manera, amb l'autenticació dels usuaris.*