

## CONCEPTES D'ACTIVE DIRECTORY

**Domini:** conjunt d'objectes que comparteixen una base de dades de seguretat comuna.

El domini té un nom DNS. El domini té una estructura piramidal que comença per root (.) seguit d'un domini de primer nivell (.net,.com,...).

**TLD (Top Level Domain):** domini de primer nivell, terminació del nom d'un domini (.com, .net,...)

**Active Directory:** nom de la base de dades de seguretat d'un domini. Entre altres coses, a AD es guarden els següents objectes: dominis, usuaris (+passwords), grups, equips, impressores, unitats organitzatives, carpetes compartides, contactes

**Controlador de Domini (DC):** màquina que guarda la base de dades Active Directory.

**Servidor Membre:** és un servidor que no executa els serveis de domini d'Active Directory (que no s'ha promocionat). Per tant, la seva funció serà com la de qualsevol estació de treball del domini (com un membre del domini).

**SAM (Security Account Manager):** nom de la base de dades de seguretat local (la que tenia el W7, W8 i W10 i els servers abans de promocionar).

**Controlador de Domini Addicional:** qualsevol controlador de domini instal·lat en un domini ja existent. Té una còpia del AD sincronitzada amb les altres màquines DC.

**Domini Secundari (sub-domini):** seria el nom d'un espai directament per sota d'altre nom de domini (el domini principal).

Per exemple, el nostre subdomini **asix.cicles.com** seria un domini secundari del **domini principal cicles.com**.

**Arbre de Dominis:** un conjunt de dominis que comparteixen un mateix espai de noms.

Per exemple, tenim l'empresa *Capsule*. Podem crear amb l'arbre de dominis els següents dominis:

capsule.com -> fa referència a la central.

sucursal1.capsule.com -> fa referència a una de les delegacions.

sucursal2.capsule.com -> fa referència a la segona delegació.

dept3.sucursal4.capsule.com -> fa referència al departament 3 de la delegació 4.

Cadascun dels anteriors noms és un domini diferent, amb el seu propi DC (controlador de domini) i el seu administrador, però tots dins del mateix arbre.

**Bosc:** espai comú on es troben un o més arbres. És un conjunt d'un o més arbres que tenen **relacions de confiança** entre ell i que no formen un espai de noms contigu. Tots els seus membres comparteixen un **esquema, configuració i catàleg global** comuns. Es podria dir que és la unió de dos o més dominis diferents.

Per exemple, suposem que la nostra empresa es divideix en dues filials: *Capsule* i *RedRibbon*. El bosc serà un **esquema multi-domini** diferenciat entre les dues filials: capsule.com i redribbon.com.

El nom del bosc és el mateix del nom del primer domini. El primer domini del bosc es coneix com "**forest-root**". Té un grup d'usuaris que són els "**administradores de la organizacion**" (en algunes traduccions de windows es diu "**administradores de empresa**").

- l'administrador de la organització és administrador de tots els dominis del bosc però
- l'administrador d'un domini pare no és administrador del domini fill.

**Relacions de Confiança:** aprofiten per que els usuaris d'un domini puguin accedir al recursos d'altres dominis. ALERTA: dona la possibilitat d'accedir a la BD, però calen els permisos corresponents.

**Entorn de Convivència:** bosc de dominis amb DC de diferents tecnologies (2000 Server, Server 2003, Server 2008, Server 2012, Server 2016 o Server 2019). La tecnologia de les estacions de treball (2000 Professional, XP, Seven, 8, 10) és indiferent.

**Catàleg Global (GC):** És un DC que té una còpia de tots els objectes AD de tots els dominis del seu bosc (estiguin o no en el seu domini) amb un subconjunt dels atributs més importants. Amb la creació d'un GC s'evita buscar la informació en altres ubicacions físiques. Per defecte és el primer DC del bosc.

**FQDN** (Fully Qualified Domain Name): el nom complet del domini: subdomini.domini

**NetBIOS** (Network Basic Input/Output System): interface d'accés als recursos de xarxa anterior al Active Directory. Són els noms sense el format TLD.

**RODC** (Read-Only Domain Controller): controlador adicional que només té accés de lectura a la base de dades

**Possibles motius per instal·lar un RODC:**

- falta de seguretat física de l'equip
- falta d'ample de banda de la xarxa
- falta de confiança o d'experiència per portar-lo l'administrador del lloc

