active directory

- Un Domain Controler est une machine qui a un OS Server qui est dans le domaine Active Directory et qui possède l'Active Directory.
- Un Member Server est une machine qui a un OS Server qui est dans le domaine Active Directory et qui ne possède pas l'Active Directory.
- Un Stand Alone Server est une machine qui a un OS Server et qui n'est pas dans le domaine Active Directory → Workgroup

Il n'y a pas de SAM (Security Account Manager) local dans un Domain Controler. Mais bien sur un Member Server, Stand Alone Server et sur un client !

Un Active Directory est une base de données où on va retrouver tous les objets du domaine : Utilisateurs, Groupes, Machines

La structure Logique : Domaine - Arbre - Forest - OU (Organizational Unit)

Décomissioner un Domain Controler :

ntdsutil.exe → metadata cleanup → remove selected server <DCServerName>

Firewall

Inter-DC traffic:

- permit tcp <src> <dst> eq 53,88,135,137,139,389,445,464,636,3268-3269,5722,9389,49152-65535
- permit udp <src> <dst> eq 53,88,123,137-138,389,445,464,49152-65535

Arguably that list at this point is excessive:

- NetBIOS shouldn't be required any more, so that's tcp 137,139 and udp 137-138 that could be dropped
- SMB should be TCP-only so that's udp 445 to potentially drop
- DFS-R just works off RPC now instead of having a dedicated port, so that's tcp 5722 to potentially drop

Everything else in the list is essential though

- 53: DNS
- 88: Kerberos
- 123: NTP
- 135 + 49152-65535: RPC
- 389,636: LDAP & LDAPS
- 445: SMB
- 464: Kerberos password change
- 3268,3269: Global Catalog LDAP & LDAPS
- 9389: AD Web Services