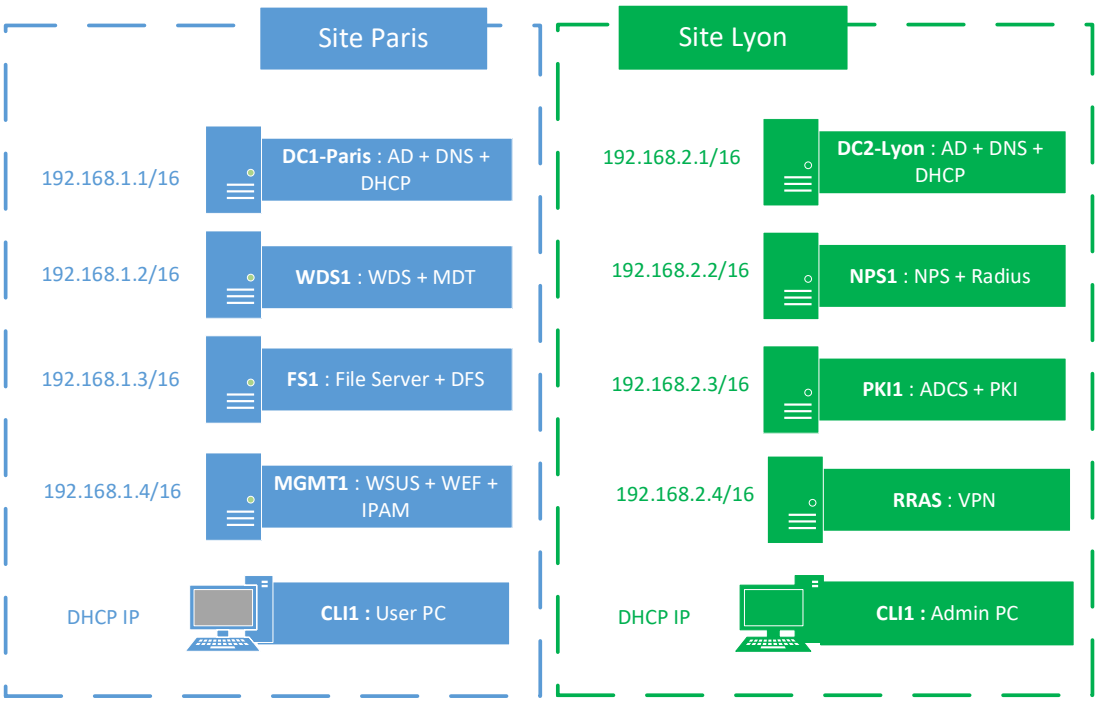
LAB ENTREPRISE

Entreprise Learn (≈250 pers.), 2 sites (Paris HQ, Lyon agence).

Architecture (VM) :

Nom	Rôles attendus
DC1-PARIS	AD DS + DNS + DHCP
DC2-LYON	AD DS + DNS + DHCP failover
FS1	Fichiers + DFS
MGMT1	WSUS + WEF (Event Forwarding) + IPAM
WDS1	WDS + MDT (déploiement postes)
PKI1	AD CS (PKI)
NPS1	NPS / RADIUS (AAA)
CL1	Client “User”
CL2	Client “IT/Admin”



Si vous manquez de RAM : NPS1 peut être fusionné avec MGMT1, mais PKI1 doit rester séparé. WDS peut être coupé une fois valide. Même chose pour DC2-Lyon / FS1 / RRAS et les deux clients peuvent être allumés qu’au moment nécessaire.

En BREF

1 AD multi-sites + DNS + DHCP failover

- Domaine unique (ex. learn.local)
- Sites AD : PARIS / LYON + subnets associés
- Réplication vérifiée (repadmin, dcdiag)
- DNS : résolution inter-sites OK + clients correctement configurés
- DHCP failover

2 OU / Groupes / Délégation

- OU propres (Users/Computers/Servers/Groups/Admins/Service Accounts)
- Séparation comptes user / comptes admin
- Délégation Helpdesk (reset, unlock, join domain) sans Domain Admin
- Modèle de groupes cohérent (AGDLP recommandé)

3 GPO + Durcissement + AppLocker

- Politiques mot de passe + verrouillage (+ FGPP pour Admins)
- Pare-feu, restrictions RDP, audit avancé, PowerShell logging
- Mapping lecteurs via GPP
- AppLocker : blocage exécution depuis %Temp% / %AppData% + exceptions par groupes

4 Serveur de fichiers pro : DFS + droits + restauration (obligatoire)

- DFS Namespace : \\learn.local\Shares
- Droits NTFS par groupes + ABE
- Shadow Copies + démonstration restauration
- Bonus conseillé : quotas

5 WSUS + anneaux de déploiement (obligatoire)

- WSUS fonctionnel
- Groupes WSUS Pilot/Prod
- Politique de validation et calendrier
- Rapport conformité

6 Centralisation logs (WEF) + mini playbook (obligatoire)

- WEF collector sur MGMT1
- Sources : serveurs + clients
- 3 événements analysés :
    - ajout groupe sensible
    - logon admin
    - échec d'authentification

7 AD CS (PKI) : certificats + autoenrollment

- PKI1 avec AD CS Entreprise
- Publication CRL accessible
- Autoenrollment via GPO :
    - certificats machine (au minimum)
    - certificats user (bonus)
- Consommation obligatoire du certificat dans AU MOINS un cas :

NPS/EAP-TLS (fortement recommandé, voir RADIUS ci-dessous) ou 2) LDAPS / RDP TLS / Authentification par certificat sur un service

8 WDS + MDT : déploiement automatisé Windows

- DEPLOY1 : WDS + MDT
- Import d'un ISO Windows 10/11
- Création d'un Task Sequence qui fait au minimum :
    - installation Windows
    - jonction au domaine
    - configuration de base (nom machine, OU cible)
    - installation d'au moins 3 apps (ex : 7zip, Firefox, Notepad++ ou équivalents)
    - application d'un profil "Entreprise" (fond d'écran/param simple = OK)
- Déploiement du client CL1 via PXE (ou ISO boot WDS si PXE compliqué)

9 IPAM : découverte + gestion IP/DNS/DHCP (obligatoire)

- Installation IPAM sur MGMT1
- Configuration du provisioning GPO d'IPAM
- Découverte des serveurs (DC1/DC2) et récupération au minimum :
    - zones DNS
    - enregistrements (au moins une vue)
- Si vous mettez DHCP (optionnel mais recommandé) : gestion DHCP via IPAM

10 RADIUS (NPS) : contrôle d'accès centralisé (obligatoire)

- Serveur NPS (NPS1) joint au domaine
- NPS enregistré dans AD
- Politiques NPS basées sur groupes (ex : VPN-Users, WiFi-Users, IT-Admins)
- 1 scénario (à valider par tests) :
    - VPN RRAS authentifié via NPS