BTS SIO · OPTION SISR · SESSION 2026

BAGARRY Matthias

DOSSIER TECHNIQUE

Déploiement d'une infrastructure Active Directory sous Windows Server 2019 – Domaine gefor.lan

---

0 CONTEXTE ET OBJECTIFS

Ce projet a été mené dans le cadre du PPE pour le client GEFOR (Groupe Européen de Formation), organisme de formation créé en 1993 et présent sur six sites en France. Le site de Paris 1er accueille plusieurs promotions (SIO, GPME, TC) et ne dispose d'aucun service d'annuaire centralisé.

L'objectif est de déployer une infrastructure complète sur une lame serveur fournie par GEFOR : un serveur Windows Server 2019 promu contrôleur de domaine, les services AD DS, DNS et DHCP associés, une arborescence de partages conforme à une matrice de droits, et des GPO couvrant les profils itinérants, le montage des lecteurs réseau et la planification des mises à jour.

▸ OBJECTIFS PÉDAGOGIQUES

Maîtriser la promotion d'un serveur en contrôleur de domaine et la configuration d'une forêt Active Directory. Structurer un annuaire en OU, groupes et comptes pour refléter l'organisation d'un établissement de formation. Appliquer une matrice de droits via les permissions NTFS et le principe du moindre privilège. Industrialiser l'administration avec les GPO et un script PowerShell d'import CSV.

▸ POURQUOI ACTIVE DIRECTORY

Sans AD, chaque poste gère ses comptes en local : pas de SSO, pas de politique unifiée, chaque utilisateur doit être recréé sur chaque machine. AD centralise l'authentification (Kerberos), la gestion des droits et le déploiement de politiques. L'intégration native DNS permet aux clients de localiser le contrôleur de domaine via les enregistrements SRV (_ldap._tcp, _kerberos._tcp).

1 ANALYSE ET ARCHITECTURE

Infrastructure cible : un contrôleur de domaine Windows Server 2019 unique, trois postes Windows 10 joints au domaine, un VLAN dédié fourni par le prestataire réseau, et un plan d'adressage géré par DHCP.

1.1 Environnement serveur

Ressource	Valeur allouée
Système d'exploitation	Windows Server 2019 Standard (GUI)
Hôte	Lame serveur GEFOR (local technique)
Rôle principal	Contrôleur de domaine (AD DS)
Rôles complémentaires	DNS, DHCP, Services de fichiers
Nom machine	GEFOR-SRV (NetBIOS : GEFOR)
Domaine racine	gefor.lan (nouvelle forêt)
Niveau fonctionnel	Windows Server 2016 (forêt et domaine)
Réseau	VLAN dédié, IP statique serveur

▸ POURQUOI UNE IP STATIQUE SUR LE DC

Un contrôleur de domaine doit avoir une IP fixe : il est DNS pour ses propres clients. Si son IP change, les clients ne résolvent plus le domaine et perdent l'authentification Kerberos. Les enregistrements SRV dans la zone DNS gefor.lan pointent vers cette IP pour la découverte du DC.

1.2 Architecture logique

Composant	Élément	Rôle
Forêt / Domaine	gefor.lan	Périmètre unique d'administration et de confiance
OU Stagiaires	OU_SIO / OU_GPME / OU_TC	Regroupement par promotion pour lier les GPO
OU Formateurs	OU Formateurs	Application d'une GPO spécifique (profils itinérants)
Groupes de sécurité	GRP_SIO / GRP_GPME / GRP_TC / GRP_Formateurs	Support des ACL NTFS (un groupe par profil)
Partages	Cours / Exo / Info / Commerce / Gestion	Ressources pédagogiques différenciées
GPO	Lecteurs / Profils / MAJ	Automatisation des paramètres utilisateur

[SCREENSHOT À INSÉRER]

Schéma d'architecture AD / DNS / DHCP

Commande : `Diagramme Visio ou draw.io`

→ Représenter le DC GEFOR-SRV au centre, les 3 postes Windows 10 clients, la zone DNS gefor.lan, l'étendue DHCP et les flux Kerberos/LDAP. Indiquer le VLAN dédié.

2 INSTALLATION DES SERVICES D'ANNUAIRE

Après installation du système d'exploitation et configuration réseau, les rôles ont été ajoutés via le Gestionnaire de serveur. L'ordre d'installation est important : AD DS et DNS sont déployés ensemble, DHCP dans un second temps une fois le domaine opérationnel.

2.1 Ajout du rôle AD DS

Le rôle Services de domaine Active Directory (AD DS) est ajouté depuis Gestionnaire de serveur → Gérer → Ajouter des rôles et fonctionnalités. L'installation ne promeut pas encore le serveur, elle ne fait qu'installer les binaires.

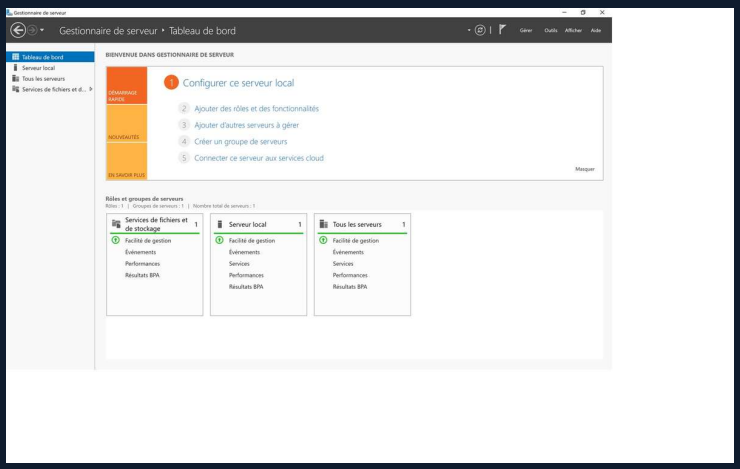

Figure 1 — *Gestionnaire de serveur — état initial (rôle Services de fichiers uniquement)*

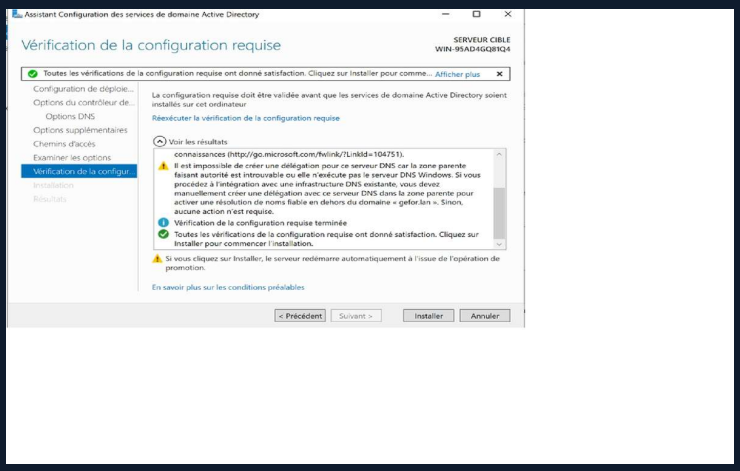

Figure 8 — *Gestionnaire de serveur — 4 rôles installés (AD DS, DHCP, DNS, Fichiers)*

2.2 Promotion en contrôleur de domaine

Une fois les binaires installés, le drapeau jaune du Gestionnaire de serveur propose « Promouvoir ce serveur en contrôleur de domaine ». L'assistant enchaîne plusieurs étapes :

Étape	Configuration retenue
Déploiement	Ajouter une nouvelle forêt (premier DC) — nom racine gefor.lan
Niveaux	Forêt et domaine en Windows Server 2016
Options DC	DNS coché, Catalogue global coché, mot de passe DSRM renseigné
Options DNS	Avertissement délégation (normal en forêt isolée, ignoré)
NetBIOS	GEFOR (attribution automatique)
Chemins	Valeurs par défaut : C:\Windows\NTDS, \SYSVOL, \NTDS logs
Vérification	Tous les contrôles passent — bouton Installer activé

▸ COMPRENDRE NTDS, SYSVOL ET DSRM

NTDS.DIT : base de données Active Directory (utilisateurs, groupes, objets). Au format ESE, comme Exchange. SYSVOL : dossier partagé répliqué entre DC contenant les scripts de connexion et les fichiers GPO (xml, pol). DSRM (Directory Services Restore Mode) : mode de démarrage hors AD, mot de passe dédié pour restaurer la base NTDS en cas de corruption. Le Catalogue global indexe les attributs inter-domaines : indispensable pour les connexions utilisateur (groupes universels).

▸ POURQUOI L'AVERTISSEMENT DE DÉLÉGATION DNS EST NORMAL

L'assistant cherche à créer une délégation dans la zone parente lan pour pointer gefor.lan vers ce DNS. Comme la zone lan n'existe sur aucun serveur public (domaine privé isolé), la délégation échoue. Ce comportement est attendu pour un premier contrôleur de domaine d'une nouvelle forêt en lab. En production avec un nom public (ex : ad.entreprise.fr), la délégation serait créée chez le registrar.

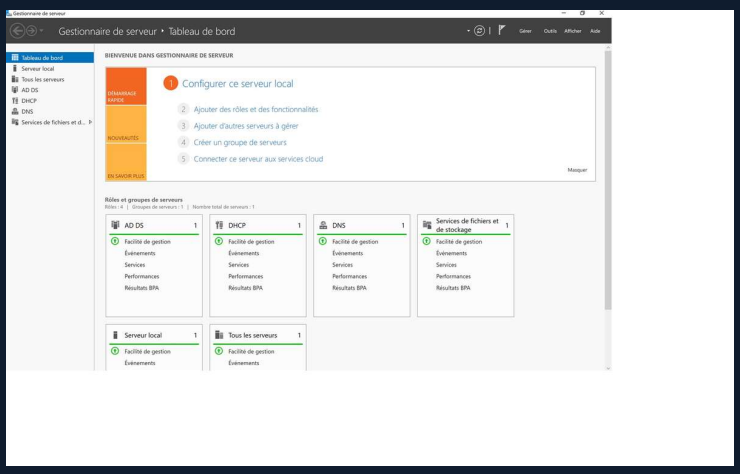

Figure 2 — *Configuration de déploiement — création de la nouvelle forêt gefor.lan*

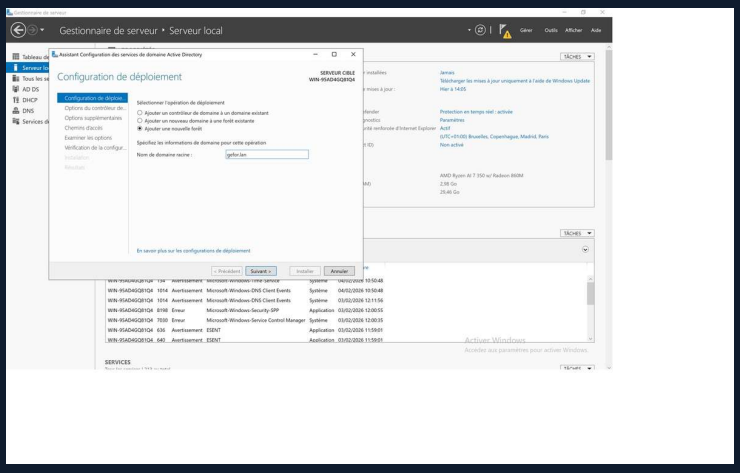

Figure 3 — *Options du contrôleur de domaine — niveau Windows Server 2016, DNS et GC cochés*

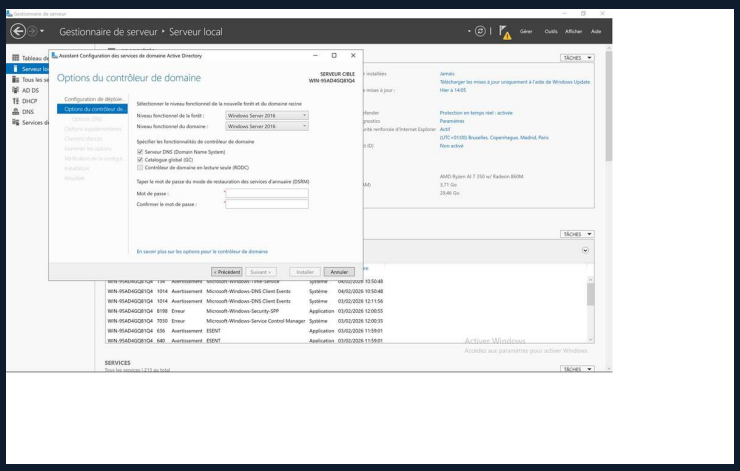

Figure 4 – *Options DNS — avertissement de délégation (normal pour une forêt racine isolée)*

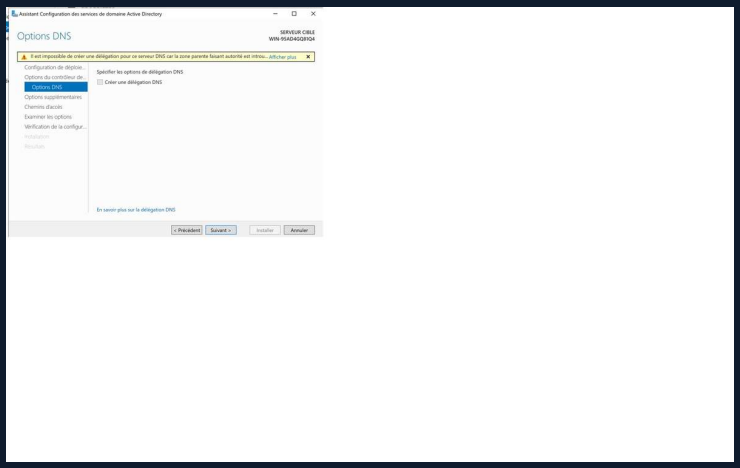

Figure 5 – *Options supplémentaires — nom de domaine NetBIOS attribué automatiquement (GEFOR)*

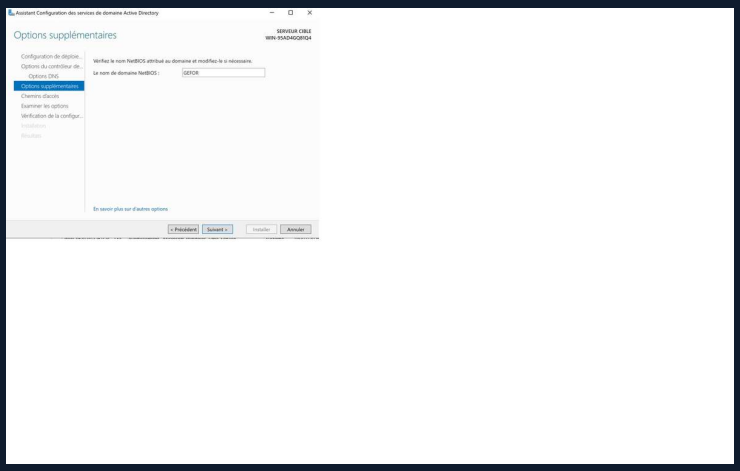

Figure 6 – *Chemins d'accès AD DS — base NTDS, journaux et SYSVOL conservés par défaut*

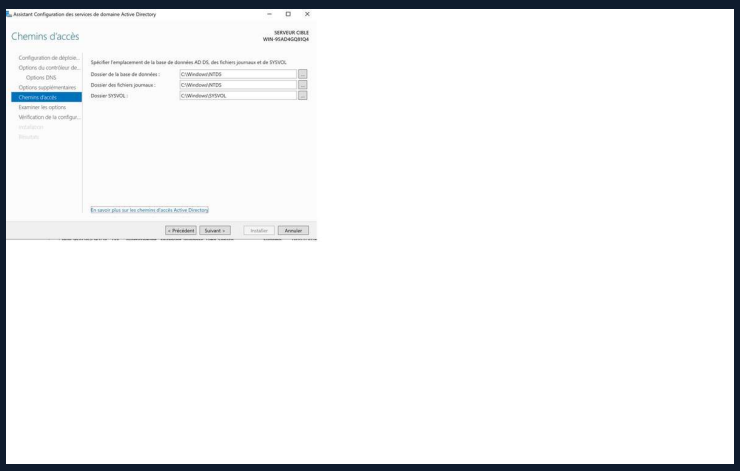

Figure 7 – *Vérification de la configuration requise — tous les contrôles sont passés*

2.3 Validation post-promotion

Après redémarrage, la console Utilisateurs et ordinateurs Active Directory (dsa.msc) doit afficher le domaine gefor.lan avec les conteneurs par défaut : Builtin, Computers, Domain Controllers, ForeignSecurityPrincipals, Managed Service Accounts, Users. La présence du serveur GEFOR-SRV dans le conteneur Domain Controllers confirme la réussite de la promotion.

```
REM Validation en ligne de commande
dcdiag /v                       REM Vérification complète de l'état du DC
dcdiag /test:DNS                REM Test spécifique des enregistrements DNS SRV
repadmin /showrepl              REM État de la réplication (sans objet ici, un seul DC)
nltest /dsgetdc:gefor.lan       REM Localisation du DC via DNS
```

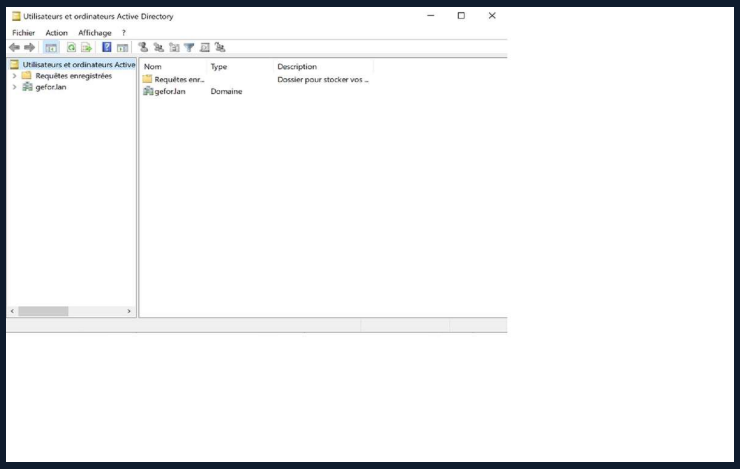

Figure 9 – *Console Utilisateurs et ordinateurs Active Directory — domaine gefor.lan visible*

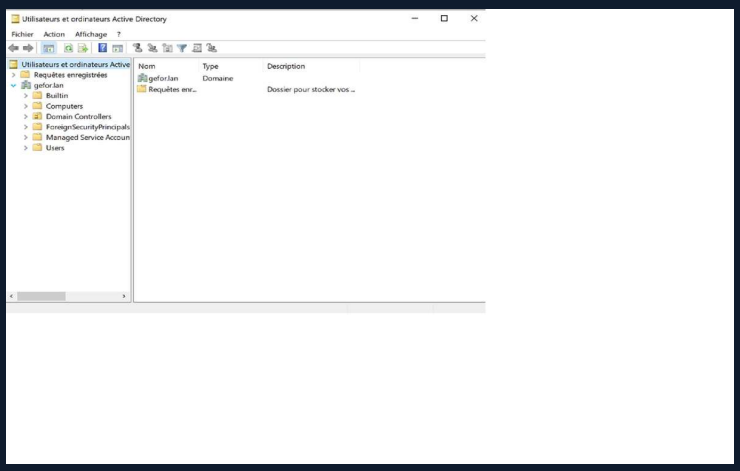

Figure 10 – *Structure du domaine gefor.lan dépliée — conteneurs par défaut (Builtin, Computers, Users...)*

3 SERVICES DNS ET DHCP

3.1 DNS intégré à l'AD

Le DNS est installé automatiquement lors de la promotion du DC. La zone gefor.lan est créée en mode « intégrée à Active Directory » : les enregistrements sont stockés dans la base NTDS et répliqués avec le reste de l'annuaire, ce qui évite de gérer un fichier de zone séparé.

▸ **ENREGISTREMENTS SRV INDISPENSABLES**

_ldap._tcp.gefor.lan → localisation des serveurs LDAP (port 389). _kerberos._tcp.gefor.lan → localisation des KDC Kerberos (port 88). _gc._tcp.gefor.lan → localisation du Catalogue global (port 3268). Sans ces enregistrements, aucun client ne peut authentifier sur le domaine. Ils sont créés automatiquement par le service Netlogon au démarrage du DC.

```
REM Vérifier les SRV depuis un poste client
nslookup -type=SRV _ldap._tcp.gefor.lan
nslookup -type=SRV _kerberos._tcp.gefor.lan

REM Résultat attendu : réponse du DC GEFOR-SRV avec priorité et poids
```

3.2 Installation et autorisation DHCP

Le rôle DHCP est ajouté via le Gestionnaire de serveur. Dans un environnement AD, l'étape critique est l'autorisation du serveur dans l'annuaire : sans cette autorisation, le service démarre mais refuse de répondre aux requêtes clients. Ce mécanisme empêche les serveurs DHCP pirates (rogue DHCP) de distribuer des baux sur un réseau d'entreprise.

```
REM Installation du rôle en PowerShell (alternative au GUI)
Install-WindowsFeature DHCP -IncludeManagementTools

REM Autorisation du serveur dans l'AD
Add-DhcpServerInDC -DnsName gefor-srv.gefor.lan -IPAddress 192.168.10.1

REM Vérification
Get-DhcpServerInDC
```

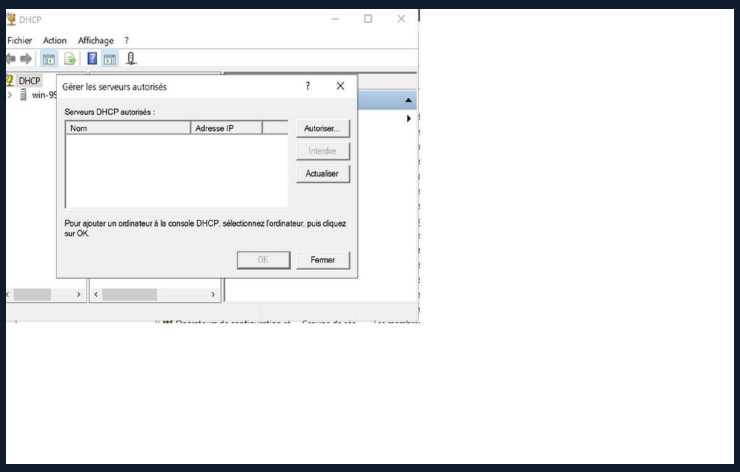

Figure 11 – *Console DHCP — fenêtre « Gérer les serveurs autorisés » avant autorisation (liste vide)*

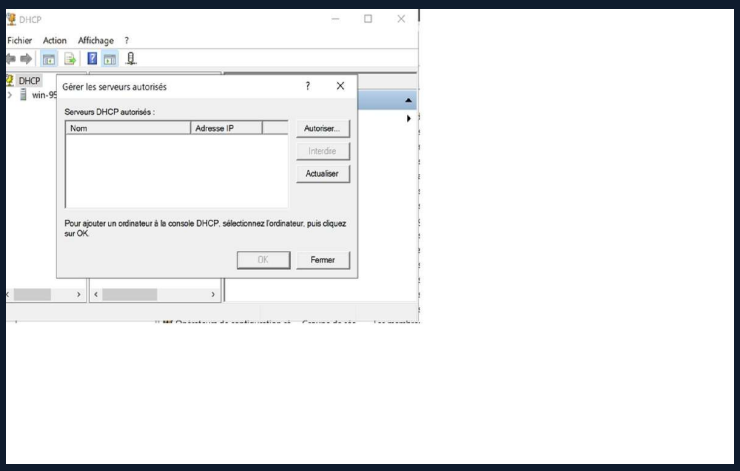

Figure 12 – *Console DHCP — confirmation de l'autorisation du serveur dans Active Directory*

3.3 Configuration de l'étendue DHCP

Paramètre	Valeur	Justification
Nom étendue	Étendue-Clients-Paris	Identification claire
Plage IP	192.168.10.100 à 192.168.10.200	100 baux pour les 3 postes + marge
Masque	255.255.255.0 (/24)	Aligné sur le plan d'adressage du VLAN

Passerelle (003)	192.168.10.254	Interface routée du VLAN
DNS (006)	192.168.10.1 (GEFOR-SRV)	Indispensable pour joindre le domaine
Domaine (015)	gefor.lan	Complète le FQDN des clients
Durée bail	8 jours	Valeur par défaut, adaptée aux postes fixes

▸ POURQUOI L'OPTION 006 (DNS) EST CRITIQUE

Si un poste client reçoit une IP mais pas le DNS du DC, il tentera une résolution sur le DNS public fourni par le routeur. Résultat : échec de la résolution gefor.lan, impossible d'authentifier Kerberos, connexion au domaine refusée. Le DNS du DC doit être distribué par DHCP — c'est une règle absolue en environnement AD.

4 STRUCTURATION DE L'ANNUAIRE

L'arborescence reflète l'organisation de GEFOR : séparation stagiaires / formateurs, puis sous-classement par promotion. Cette structure conditionne l'application des GPO (une GPO liée à OU_SIO ne s'applique qu'aux stagiaires SIO).

4.1 Unités d'organisation (OU)

```
gefor.lan/
├── OU Stagiaires
│   ├── OU_SIO        → liée à GPO_LecteursReseau_SIO
│   ├── OU_GPME       → liée à GPO_LecteursReseau_GPME
│   └── OU_TC         → liée à GPO_LecteursReseau_TC
├── OU Formateurs     → liée à GPO_ProfilsItinerants
└── OU Ordinateurs    → liée à GPO_MajHebdo
```

▸ OU VS GROUPES : DIFFÉRENCE FONDAMENTALE

OU : conteneur structurel, sert à appliquer des GPO et à déléguer l'administration. Un objet appartient à une seule OU. Groupe : objet de sécurité, sert à attribuer des droits (NTFS, partage, applicatifs). Un utilisateur peut appartenir à plusieurs groupes. Règle classique : utiliser les OU pour la logique administrative, les groupes pour les autorisations.

4.2 Groupes de sécurité

Groupe	Portée	Membres
GRP_SIO	Globale	Stagiaires de la promotion SIO
GRP_GPME	Globale	Stagiaires de la promotion GPME
GRP_TC	Globale	Stagiaires de la promotion TC
GRP_Formateurs	Globale	Formateurs de l'établissement

▸ PORTÉE DES GROUPES : POURQUOI GLOBALE

Domaine local : sert pour les permissions sur les ressources du domaine (ACL). Globale : regroupe des utilisateurs d'un même domaine, s'utilise à travers la forêt. Universelle : membres de toute la forêt, indexée dans le Catalogue global. Le schéma recommandé Microsoft est AGDLP : Accounts → Global → Domain Local → Permissions. Ici, forêt simple avec un seul domaine, l'approche Globale suffit.

[SCREENSHOT À INSÉRER]

Arborescence OU et groupes dans la console AD

Commande : `dsa.msc → domaine gefor.lan déplié`

→ Capturer l'arborescence complète avec OU Stagiaires (et ses 3 sous-OU), OU Formateurs, et les 4 groupes GRP_* dans leur OU respective.

5 PARTAGES ET MATRICE DE DROITS

Cinq répertoires partagés sont créés sur le serveur. Les droits sont appliqués à deux niveaux : partage SMB et ACL NTFS. En pratique, les ACL NTFS portent la logique fine et les permissions de partage sont laissées à « Tout le monde / Contrôle total » (les NTFS sont toujours les plus restrictives des deux).

5.1 Matrice cible

Groupe	Cours	Exo	Info	Commerce	Gestion
Formateurs	L/É	L/É	L/É	L/É	L/É
SIO	L	L/É	L/É	✕	✕
GPME	L	L/É	✕	✕	L/É
TC	L	L/É	✕	L/É	✕

L : lecture seule · L/É : lecture + écriture · ✕ : accès refusé (absence d'ACL)

5.2 Création des partages et ACL

```
# Création des dossiers sur le serveur
New-Item -Path C:\Partages\Cours     -ItemType Directory
New-Item -Path C:\Partages\Exo       -ItemType Directory
New-Item -Path C:\Partages\Info      -ItemType Directory
New-Item -Path C:\Partages\Commerce  -ItemType Directory
New-Item -Path C:\Partages\Gestion   -ItemType Directory

# Partages SMB (niveau partage large, contrôle fin par NTFS)
New-SmbShare -Name Cours    -Path C:\Partages\Cours    -FullAccess Everyone
New-SmbShare -Name Exo      -Path C:\Partages\Exo      -FullAccess Everyone
New-SmbShare -Name Info     -Path C:\Partages\Info     -FullAccess Everyone
New-SmbShare -Name Commerce -Path C:\Partages\Commerce -FullAccess Everyone
New-SmbShare -Name Gestion  -Path C:\Partages\Gestion  -FullAccess Everyone
```

Les ACL NTFS sont ensuite appliquées via icacls ou la GUI. Exemple pour le dossier Exo (accessible en L/É à tout le monde sauf Formateurs qui conserve un accès complet) :

```
# Désactivation de l'héritage puis application des ACL explicites
icacls C:\Partages\Exo /inheritance:r

icacls C:\Partages\Exo /grant:r "GEFOR\GRP_Formateurs:(OI)(CI)F"
icacls C:\Partages\Exo /grant:r "GEFOR\GRP_SIO:(OI)(CI)M"
icacls C:\Partages\Exo /grant:r "GEFOR\GRP_GPME:(OI)(CI)M"
icacls C:\Partages\Exo /grant:r "GEFOR\GRP_TC:(OI)(CI)M"
icacls C:\Partages\Exo /grant:r "SYSTEM:(OI)(CI)F" "GEFOR\Domain Admins:(OI)(CI)F"
```

▸ **DÉCRYPTAGE DES FLAGS ICACLS**

F = Full control (Contrôle total) — réservé aux Formateurs et admins. M = Modify (Modification) — lecture + écriture + suppression, pour les stagiaires autorisés. R = Read (Lecture seule) — utilisé sur le dossier Cours pour les stagiaires. (OI) = Object Inherit : propagation aux fichiers. (CI) = Container Inherit : propagation aux sous-dossiers. /inheritance:r : supprime l'héritage avant application (évite les droits parasites).

▸ NTFS VS PARTAGE SMB : LA RÈGLE DU PLUS RESTRICTIF

Quand un utilisateur accède à un partage, Windows calcule l'intersection des permissions SMB et NTFS. Si le partage autorise Lecture mais NTFS autorise Contrôle total, l'effectif est Lecture. En pratique : laisser SMB large (Everyone FullAccess) et affiner uniquement côté NTFS. Moins d'erreurs, administration plus simple.

[SCREENSHOT À INSÉRER]

ACL effectives sur un dossier partagé

Commande : `Propriétés du dossier → Sécurité → Avancé → Accès effectif`

→ Choisir l'utilisateur stagiaire1@gefor.lan et un dossier Gestion : le résultat doit indiquer l'absence de droit (ligne vide / refusé). Prouve l'efficacité de la matrice.

6 STRATÉGIES DE GROUPE (GPO)

Trois GPO couvrent les besoins du cahier des charges : montage automatique des lecteurs, profils itinérants pour les formateurs, planification hebdomadaire des mises à jour.

6.1 GPO Lecteurs réseau

Chaque promotion dispose de sa propre GPO liée à son OU. Les lecteurs sont mappés via Préférences de stratégie de groupe (GPP) → Configuration utilisateur → Paramètres Windows → Mappages de lecteurs. Un ciblage par groupe évite qu'un stagiaire SIO voie apparaître un lecteur Gestion s'il est accidentellement dans une autre OU.

Lettre	Cible	SIO	GPME	TC	Formateurs
H:	\\GEFOR-SRV\Cours	✓	✓	✓	✓
I:	\\GEFOR-SRV\Exo	✓	✓	✓	✓
J:	\\GEFOR-SRV\Info	✓	✗	✗	✓
K:	\\GEFOR-SRV\Commerce	✗	✗	✓	✓
L:	\\GEFOR-SRV\Gestion	✗	✓	✗	✓

6.2 GPO Profils itinérants (Formateurs)

Un formateur doit retrouver son environnement (bureau, documents, paramètres) quel que soit le poste de l'établissement. Les profils itinérants stockent le profil utilisateur sur un partage réseau qui est copié vers le poste à l'ouverture de session et synchronisé à la fermeture.

```
# Création du partage dédié aux profils
New-Item -Path C:\Profils -ItemType Directory
New-SmbShare -Name Profils$ -Path C:\Profils -FullAccess Everyone

# $ à la fin = partage masqué (ne s'affiche pas dans le voisinage réseau)
# ACL NTFS : créateur propriétaire + GRP_Formateurs en modification
icacls C:\Profils /grant:r "GEFOR\GRP_Formateurs:(OI)(CI)M"
icacls C:\Profils /grant:r "CREATOR OWNER:(OI)(CI)F"
```

Dans AD, pour chaque formateur : onglet Profil → Chemin de profil : \\GEFOR-SRV\Profils$\%username%

▸ ATTENTION AUX LIMITES DU PROFIL ITINÉRANT

Le profil copie l'ensemble des fichiers AppData\Roaming à chaque connexion/déconnexion : lent sur les gros profils. En production, on préfère souvent les Profils utilisateur itinérants + redirection de dossiers (Documents, Bureau) pour ne pas copier les fichiers volumineux. Dans le cadre pédagogique GEFOR, le profil itinérant seul est suffisant et simple à expliquer au jury.

6.3 GPO Mises à jour Windows

Configuration utilisateur → Modèles d'administration → Composants Windows → Windows Update. Planification automatique chaque vendredi à 19 h 00, en dehors des heures de cours. L'objectif est d'éviter qu'une MAJ interrompe un TP en journée.

```
Configurer les mises à jour automatiques : Activé
Configurer la mise à jour automatique : 4 (téléchargement + installation planifiée)
Jour d'installation planifiée : 6 (vendredi)
Heure d'installation planifiée : 19:00

Pas de redémarrage automatique avec utilisateurs connectés : Activé
```

[SCREENSHOT À INSÉRER]

Console GPMC avec les 3 GPO liées

Commande : `gpmc.msc`

→ Capturer la console avec les GPO_Lecteurs, GPO_Profils, GPO_MajHebdo visibles dans l'arbre, et les liens vers les OU appropriées dans le panneau de droite.

7 AUTOMATISATION POWERSHELL

Le script d'import prend en entrée un CSV (colonnes Nom, Prenom, diplome) fourni par l'administration. Il génère le login selon la convention p.nom (première lettre prénom + nom), crée le compte dans l'OU de la promotion correspondante, l'affecte au bon groupe et écrit un log horodaté.

7.1 Format du CSV attendu

```
Nom;Prenom;diplome
MARTIN;Lucas;SIO
DUPONT;Sarah;GPME
BERNARD;Antoine;TC
LEROY;Camille;SIO
```

7.2 Script PowerShell

```
# Import-Stagiaires.ps1 — Création en masse depuis CSV
Import-Module ActiveDirectory

$csvPath  = "C:\Scripts\stagiaires.csv"
$logPath  = "C:\Scripts\import_$(Get-Date -Format 'yyyyMMdd_HHmmss').log"
$mdpDefaut = ConvertTo-SecureString "Gefor2026!" -AsPlainText -Force

# Table de correspondance diplôme -> OU / Groupe
$mapping = @{
    'SIO'  = @{ OU='OU=OU_SIO,OU=Stagiaires,DC=gefor,DC=lan';  Groupe='GRP_SIO' }
    'GPME' = @{ OU='OU=OU_GPME,OU=Stagiaires,DC=gefor,DC=lan'; Groupe='GRP_GPME' }
    'TC'   = @{ OU='OU=OU_TC,OU=Stagiaires,DC=gefor,DC=lan';   Groupe='GRP_TC' }
}

Import-Csv $csvPath -Delimiter ';' | ForEach-Object {
    $prenom  = $_.Prenom.Trim()
    $nom     = $_.Nom.Trim()
    $diplome = $_.diplome.Trim().ToUpper()
    $login   = ($prenom.Substring(0,1) + '.' + $nom).ToLower()

    if (-not $mapping.ContainsKey($diplome)) {
        Add-Content $logPath "[ERREUR] $login : diplôme inconnu ($diplome)"
        return
    }

    try {
        New-ADUser -Name "$prenom $nom" `
            -SamAccountName $login `
            -UserPrincipalName "$login@gefor.lan" `
            -GivenName $prenom -Surname $nom `
            -Path $mapping[$diplome].OU `
            -AccountPassword $mdpDefaut `
            -ChangePasswordAtLogon $true `
            -Enabled $true

        Add-ADGroupMember -Identity $mapping[$diplome].Groupe -Members $login
        Add-Content $logPath "[OK] $login créé et ajouté à $($mapping[$diplome].Groupe)"
    }
    catch {
        Add-Content $logPath "[ERREUR] $login : $($_.Exception.Message)"
    }
}

Write-Host "Import terminé — log disponible : $logPath"
```

▸ POINTS DE VIGILANCE DU SCRIPT

Mot de passe par défaut + ChangePasswordAtLogon $true : oblige le stagiaire à en définir un au premier login. Le try/catch isole chaque ligne : une erreur sur un compte n'interrompt pas tout l'import. Le log horodaté garantit la traçabilité pour l'administration. En cas de doublon (login déjà existant), New-ADUser lève une exception capturée par le catch. Amélioration possible : gérer les doublons de login (p.dupont × 2) en ajoutant un numéro incrémental.

[SCREENSHOT À INSÉRER]

Exécution du script et log généré

Commande : `.\Import-Stagiaires.ps1`

→ Deux captures : (1) console PowerShell avec « Import terminé », (2) contenu du fichier log avec plusieurs lignes [OK] et éventuellement une ligne [ERREUR] volontaire (diplôme inconnu).

8 VALIDATION TECHNIQUE (RECETTE)

Les tests valident le fonctionnement complet de la solution sur les 3 postes clients et la conformité à la matrice de droits.

ID	Fonctionnalité	Protocole de test	Résultat attendu
T01	Authentification domaine	Ouverture session avec un compte de chaque groupe sur les 3 postes	Login réussi sur gefor.lan pour tous les profils
T02	Mappage lecteurs réseau	Explorateur après connexion utilisateur	Lettres H/I/J/K/L présentes selon la promotion
T03	Permissions stagiaires	Stagiaire SIO tente l'écriture dans Cours, l'accès à Gestion	Refus d'écriture sur Cours, refus d'accès Gestion
T04	Permissions formateurs	Formateur crée/modifie/supprime dans les 5 partages	Accès total (L/É) sur l'ensemble
T05	Profils itinérants	Formateur crée un fichier sur poste 1, se reconnecte sur poste 2	Fichier retrouvé à l'identique
T06	GPO Mises à jour	gpresult /r sur un poste client	Planification vendredi 19h00 héritée
T07	DHCP	Poste client en IP auto, ipconfig /all	IP dans la plage, DNS = 192.168.10.1, domaine gefor.lan
T08	Script import CSV	Exécution avec CSV de 4 stagiaires	4 comptes créés, log [OK] pour chacun

8.1 Commandes de diagnostic

Commande	Usage
gpresult /r	GPO appliquées à l'utilisateur/ordinateur courant
gpupdate /force	Rafraîchissement immédiat des stratégies
dcdiag /v	Diagnostic complet du contrôleur de domaine
ipconfig /all	Vérification IP/DNS/domaine côté client
nslookup gefor.lan	Test de résolution DNS du domaine
net use	Liste des lecteurs réseau montés
whoami /groups	Groupes du compte connecté
Get-ADUser -Filter * -SearchBase ...	Liste PowerShell des comptes d'une OU

[SCREENSHOT À INSÉRER]

Preuve de l'héritage GPO sur un poste client

Commande : `gpresult /r depuis une session stagiaire`

→ Capturer la sortie avec les sections « Objets stratégie de groupe appliqués » listant GPO_LecteursReseau_SIO, et le groupe d'ordinateur GPO_MajHebdo.

9 PROBLÈMES RENCONTRÉS ET SOLUTIONS

9.1 Avertissement de délégation DNS

Lors de la promotion du DC, l'assistant a signalé l'impossibilité de créer une délégation DNS pour gefor.lan. Après analyse (absence de zone parente .lan sur un DNS public), la poursuite de l'installation sans délégation a été validée. Le comportement est normal en forêt racine isolée et n'a aucun impact sur le fonctionnement interne.

9.2 DHCP non opérationnel après installation

Après installation du rôle DHCP, les clients ne recevaient pas d'IP. La cause : dans un environnement AD, tout serveur DHCP doit être explicitement autorisé pour éviter les serveurs DHCP pirates. Résolution via DHCP → Action → Gérer les serveurs autorisés, puis redémarrage du service DHCPServer.

9.3 Bureau à distance refusé après jonction au domaine

Les utilisateurs du domaine ne pouvaient pas se connecter en RDP sur les postes Windows 10 malgré l'activation manuelle du Bureau à distance sur chaque poste. Cause : la politique locale était écrasée par une GPO du domaine. Résolution : création d'une GPO dédiée « Ordinateur → Paramètres Windows → Sécurité → Attribution des droits utilisateur → Autoriser l'ouverture de session par les services Bureau à distance » ajoutant le groupe Utilisateurs du domaine.

10 BILAN ET PERSPECTIVES

L'infrastructure répond aux quatre axes du cahier des charges : annuaire opérationnel sur gefor.lan, partages avec matrice de droits conforme, règles de sécurité appliquées via GPO, automatisation de l'import par script PowerShell. Tous les tests de recette sont validés.

▸ PISTES D'AMÉLIORATION EN ENVIRONNEMENT DE PRODUCTION

Déploiement d'un second DC pour la tolérance de panne AD (réplication multi-maître). Passage aux profils itinérants + redirection de dossiers pour limiter la charge à la connexion. Mise en place de WSUS pour maîtriser les mises à jour au lieu d'aller chercher directement Windows Update. Politique de mots de passe durcie via Fine-Grained Password Policy pour les formateurs. Sauvegarde de l'état système du DC (Windows Server Backup) et test régulier de restauration DSRM. Supervision avec un outil type Zabbix ou PRTG sur les compteurs AD (réplication, GC, NTDS).

▸ COMPÉTENCES BTS SIO SISR MOBILISÉES

B1.1 — Gérer le patrimoine informatique (inventaire des rôles, documentation)
B1.2 — Répondre aux incidents et aux demandes (recette, diagnostic, résolution)
B2.1 — Concevoir une solution d'infrastructure (architecture AD, OU, GPO)
B2.2 — Installer, tester et déployer une solution d'infrastructure réseau
B2.3 — Exploiter, dépanner et superviser une solution d'infrastructure réseau
B3.1 — Protéger les données à caractère personnel (matrice NTFS, moindre privilège)
B3.3 — Assurer la cybersécurité (hardening, GPO de sécurité, DHCP autorisé)