# 3. Active Directory

Promotion DC, objets AD, jonction au domaine

- Active Directory : promouvoir un contrôleur de domaine
- Active Directory : utilisateurs, groupes et OU
- Joindre un poste au domaine

# Active Directory : promouvoir un contrôleur de domaine

## Vocabulaire

| Terme | Définition |
|---|---|
| **AD DS** | *Active Directory Domain Services* : l'annuaire qui centralise les comptes, ordinateurs, groupes et stratégies |
| **Contrôleur de domaine (DC)** | Serveur qui héberge une copie de l'annuaire et authentifie les utilisateurs (Kerberos) |
| **Domaine** | Ensemble d'objets partageant la même base AD et le même nom DNS (`hp.lan`) |
| **Arborescence** (*tree*) | Domaine parent + domaines enfants (`hp.lan`, `bxl.hp.lan`) |
| **Forêt** | Ensemble d'arborescences : c'est la **limite de sécurité**. Le premier domaine créé est le *domaine racine de la forêt* |
| **OU** (*Organizational Unit*) | « Dossier » dans le domaine pour ranger les objets, déléguer des droits et appliquer des GPO |
| **NetBIOS** | Nom court du domaine (`HP`), utilisé dans `HP\hugo` |
| **NTDS.dit** | Fichier de la base AD (`C:\Windows\NTDS`) |
| **SYSVOL** | Partage répliqué entre DC qui contient les scripts et les GPO |

## Prérequis avant promotion

- ☐ **Nom définitif** de la machine (`SRV01`) : on évite de renommer un DC après coup.
- ☐ **IP fixe** (10.19.1.254 /24, GW 10.19.1.1).
- ☐ **DNS préféré = lui-même** (`10.19.1.254` ou `127.0.0.1`). Le serveur deviendra son propre DNS.
- ☐ Machine **sysprepée** si c'est un clone (SID unique).
- ☐ Heure et fuseau horaire corrects.
- ☐ Snapshot « avant promotion ».

# Choisir le nom de domaine

- Utiliser un nom DNS complet : `hp.lan`, `lab.hugo-pierret.be`...
- La recommandation Microsoft est un **sous-domaine d'un domaine qu'on possède** ( `ad.hugo-pierret.be` ).
- **Éviter** `.local`, qui entre en conflit avec mDNS/Bonjour, et les noms en une seule partie ( `HP` tout seul).

# Promotion en GUI

1. **Gestionnaire de serveur** → Ajouter des rôles → **Services AD DS**.
2. Cliquer sur le drapeau jaune ⚠ → **Promouvoir ce serveur en contrôleur de domaine**.
3. **Ajouter une nouvelle forêt** → nom de domaine racine `hp.lan`.
4. Niveaux fonctionnels, options **DNS** + **Catalogue global** (cochés), mot de passe **DSRM**.
5. Délégation DNS : l'avertissement est normal pour une nouvelle forêt.
6. Nom NetBIOS ( `HP` ), chemins (laisser par défaut), vérification des prérequis, **Installer**. Le serveur redémarre.

# Promotion en PowerShell

```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools


Install-ADDSForest `
    -DomainName "hp.lan" `
    -DomainNetbiosName "HP" `
    -InstallDns `
    -SafeModeAdministratorPassword (Read-Host -AsSecureString "Mot de passe DSRM") `
    -Force
```

Autres cas (pour plus tard) :

- `Install-ADDSDomainController -DomainName hp.lan -InstallDns -Credential (Get-Credential)` : **ajouter un 2e DC** dans un domaine existant.
- `Install-ADDSDomain` : créer un domaine enfant.

# DSRM

*Directory Services Restore Mode* : mode de démarrage spécial pour **réparer ou restaurer AD**, base AD hors ligne. Le mot de passe DSRM est celui de l'administrateur **local** utilisé dans ce mode.

Il est différent du mot de passe Administrateur du domaine : **à noter quelque part !**

# Ce qui change après la promotion

- Le compte `Administrateur` local devient `HP\Administrateur` (administrateur du domaine).
- Plus de comptes locaux : `lusrmgr.msc` ne fonctionne plus sur un DC.
- La zone DNS `hp.lan` est créée, ainsi que `_msdcs.hp.lan` avec les enregistrements SRV.
- Les partages `SYSVOL` et `NETLOGON` apparaissent (`net share`).
- La carte réseau peut afficher DNS `127.0.0.1` : c'est normal, c'est le serveur lui-même.

# Vérifications

```
Get-ADDomain
Get-ADForest
Get-ADDomainController
dcdiag                                          # tests de santé du DC (tout doit être
"passed")
nslookup -type=SRV _ldap._tcp.dc._msdcs.hp.lan  # le DC est-il annoncé dans le DNS ?
netdom query fsmo                               # qui détient les 5 rôles FSMO
```

# Rôles FSMO (pour info)

5 rôles uniques, tous sur le premier DC :

- **Par forêt** : Contrôleur de schéma, Maître d'attribution des noms de domaine.
- **Par domaine** : Émulateur PDC (heure, mots de passe), Maître RID (distribue les blocs de SID), Maître d'infrastructure.

# Questions de révision

1. Quelle est la différence entre un domaine et une forêt ?
2. Quel DNS doit être configuré sur la carte réseau du DC avant la promotion ?
3. À quoi sert le mot de passe DSRM ?
4. Quel enregistrement DNS vérifier pour s'assurer que le DC est bien annoncé ?
5. Pourquoi éviter un nom de domaine en `.local` ?
6. Quelle commande teste la santé d'un contrôleur de domaine ?

# Active Directory : utilisateurs, groupes et OU

Console : `dsa.msc` (Utilisateurs et ordinateurs Active Directory, « ADUC »).

> Menu **Affichage → Fonctionnalités avancées** : affiche l'onglet **Éditeur d'attributs**, l'onglet **Objet** (chemin, protection contre la suppression) et des conteneurs cachés.

# Conteneurs par défaut vs OU

| Élément | Type | Remarque |
|---|---|---|
| `Builtin` | Conteneur | Groupes locaux intégrés (Administrateurs, Utilisateurs…) |
| `Computers` | Conteneur | Destination par défaut des PC qui rejoignent le domaine |
| `Users` | Conteneur | Comptes et groupes par défaut (Admins du domaine, etc.) |
| `Domain Controllers` | **OU** | Contient les DC |
| Vos OU | **OU** |  On peut y **lier des GPO** et **déléguer** l'administration, ce qui est impossible sur un conteneur |

Exemple de structure :

```
hp.lan
 └─ HP (OU)
     ├─ Utilisateurs
     │   ├─ Direction
     │   ├─ Compta
     │   └─ IT
     ├─ Ordinateurs
     │   ├─ Postes
     │   └─ Serveurs
```

```
    └─ Groupes
```

On peut rediriger les nouveaux PC vers une OU plutôt que vers `Computers` :

```
redircmp "OU=Postes,OU=Ordinateurs,OU=HP,DC=hp,DC=lan"
```

# Comptes utilisateur

| Attribut | Exemple | Remarque |
|---|---|---|
| Nom d'ouverture de session (pré-Windows 2000) / **sAMAccountName** | `HP\hpierret` | 20 caractères max |
| **UPN** (*User Principal Name*) | `hpierret@hp.lan` | Ressemble à une adresse mail |
| **DN** (*Distinguished Name*) | `CN=Hugo Pierret,OU=IT,OU=Utilisateurs,OU=HP,DC=hp,DC=lan` | Chemin complet dans l'annuaire |

Options courantes : *L'utilisateur doit changer le mot de passe à la prochaine ouverture de session*, *Le compte est désactivé*, date d'expiration, horaires d'accès (onglet Compte).

# Groupes

## Type

- **Sécurité** : sert à donner des **permissions** (et peut aussi servir de liste de distribution).
- **Distribution** : uniquement pour les listes de mail (Exchange), sans permissions.

## Étendue (*scope*)

| Étendue | Peut contenir | Utilisable pour des permissions |
|---|---|---|
| **Domaine local** (DL) | Utilisateurs et groupes de **n'importe quel domaine** de la forêt | Seulement dans **son** domaine |
| **Globale** (G) | Utilisateurs et groupes globaux de **son** domaine | Partout dans la forêt |
| **Universelle** (U) | Utilisateurs et groupes de toute la forêt | Partout dans la forêt (stockée dans le catalogue global) |

## Stratégie AGDLP (bonne pratique)

> **A**ccounts → **G**lobal → **D**omain **L**ocal → **P**ermissions

1. Les **comptes** (A) vont dans des groupes **globaux** organisés **par métier** : `GG_Compta`.
2. Les groupes globaux vont dans des groupes **domaine local** organisés **par ressource et par droit** : `DL_Partage-Compta_RW`.
3. On donne les **permissions** au groupe domaine local, **jamais** directement à un utilisateur.

➡ Un nouvel employé à la compta ? On l'ajoute à `GG_Compta` et il obtient tous les accès d'un coup.

# PowerShell (module ActiveDirectory)

```
# OU
New-ADOrganizationalUnit -Name "HP" -Path "DC=hp,DC=lan"
New-ADOrganizationalUnit -Name "Utilisateurs" -Path "OU=HP,DC=hp,DC=lan"
New-ADOrganizationalUnit -Name "Compta" -Path "OU=Utilisateurs,OU=HP,DC=hp,DC=lan"

# Utilisateur
New-ADUser -Name "Alice Dupont" -GivenName Alice -Surname Dupont `
    -SamAccountName adupont -UserPrincipalName adupont@hp.lan `
    -Path "OU=Compta,OU=Utilisateurs,OU=HP,DC=hp,DC=lan" `
    -AccountPassword (Read-Host -AsSecureString "MDP") `
    -ChangePasswordAtLogon $true -Enabled $true

# Groupes
New-ADGroup -Name "GG_Compta" -GroupScope Global -GroupCategory Security -Path
"OU=Groupes,OU=HP,DC=hp,DC=lan"
New-ADGroup -Name "DL_Partage-Compta_RW" -GroupScope DomainLocal -GroupCategory Security -Path
"OU=Groupes,OU=HP,DC=hp,DC=lan"
Add-ADGroupMember -Identity "GG_Compta" -Members adupont
Add-ADGroupMember -Identity "DL_Partage-Compta_RW" -Members "GG_Compta"

# Consulter
Get-ADUser adupont -Properties *
Get-ADGroupMember GG_Compta
Get-ADUser -Filter * -SearchBase "OU=HP,DC=hp,DC=lan" | Select Name, SamAccountName

# Gestion courante
Set-ADAccountPassword adupont -Reset -NewPassword (Read-Host -AsSecureString)
```

```
Unlock-ADAccount adupont
Disable-ADAccount adupont
Move-ADObject -Identity "CN=Alice Dupont,OU=Compta,..." -TargetPath "OU=IT,..."
Search-ADAccount -LockedOut
```

Création en masse depuis un CSV :

```
Import-Csv .\users.csv -Delimiter ";" | ForEach-Object {
    New-ADUser -Name "$($_.Prenom) $($_.Nom)" -SamAccountName $_.Login `
        -UserPrincipalName "$($_.Login)@hp.lan" -Path $_.OU `
        -AccountPassword (ConvertTo-SecureString $_.MDP -AsPlainText -Force) -Enabled $true
}
```

# Protection contre la suppression accidentelle

Les OU créées via la GUI sont **protégées** par défaut : on ne peut pas les supprimer directement. Pour en supprimer une :

- GUI : *Fonctionnalités avancées* → propriétés de l'OU → onglet **Objet** → décocher la protection.
- PowerShell : `Set-ADOrganizationalUnit "OU=Test,DC=hp,DC=lan" -ProtectedFromAccidentalDeletion $false`

# Questions de révision

1. Quelle est la différence entre une OU et un conteneur comme `Users` ?
2. Explique AGDLP avec un exemple.
3. Quelle est la différence entre un groupe global et un groupe domaine local ?
4. Quelle est la différence entre sAMAccountName, UPN et DN ?
5. Pourquoi n'arrives-tu pas à supprimer une OU, et comment faire ?
6. Groupe de sécurité ou de distribution : lequel pour donner accès à un partage ?

# Joindre un poste au domaine

## Prérequis côté client

1. **DNS = le contrôleur de domaine** (`10.19.1.254`), par DHCP (option 006) ou en manuel. ⚠ C'est **la cause n°1 des échecs**. Avec 8.8.8.8 en DNS, le client ne trouve jamais `hp.lan` .
2. Connectivité : `ping srv01.hp.lan`.
3. SID unique : machine clonée → **sysprep** obligatoire.
4. Heure synchronisée : Kerberos tolère **5 minutes** d'écart maximum.
5. Édition **Pro / Entreprise / Éducation** de Windows : **Windows Famille ne peut pas rejoindre un domaine**.
6. Un compte du domaine autorisé : tout utilisateur du domaine peut joindre **jusqu'à 10 machines** par défaut, un admin du domaine sans limite.

Test rapide avant de joindre :

```
nslookup -type=SRV _ldap._tcp.dc._msdcs.hp.lan
```

Si le DC apparaît, le DNS est bon.

## En GUI

`sysdm.cpl` → onglet **Nom de l'ordinateur** → **Modifier** → **Membre d'un domaine** : `hp.lan` → identifiants `HP\Administrateur` → « Bienvenue dans le domaine hp.lan » → **redémarrer**.

## En PowerShell

```
# Renommer et joindre en une seule fois
Add-Computer -DomainName "hp.lan" -NewName "CLI01" -Credential HP\Administrateur `
    -OUPath "OU=Postes,OU=Ordinateurs,OU=HP,DC=hp,DC=lan" -Restart

# Quitter le domaine
Remove-Computer -UnjoinDomainCredential HP\Administrateur -WorkgroupName WORKGROUP -Restart
```

**Pré-créer** le compte ordinateur dans AD (par exemple pour le placer directement dans la bonne OU) :

```
New-ADComputer -Name "CLI01" -Path "OU=Postes,OU=Ordinateurs,OU=HP,DC=hp,DC=lan"
```

# Ouvrir une session de domaine

Sur l'écran de connexion → **Autre utilisateur** → `HP\adupont` ou `adupont@hp.lan`. Pour une session **locale** : `.\Administrateur` (le `.` désigne la machine locale).

Vérifier :

```
whoami                :: hp\adupont
whoami /upn           :: adupont@hp.lan
echo %logonserver%    :: \\SRV01
systeminfo | findstr /i "domaine"
```

# Dépannage

| Erreur ou symptôme | Cause / solution |
|---|---|
| « Un contrôleur de domaine AD pour le domaine hp.lan n'a pas pu être contacté » | **DNS** du client ≠ IP du DC, ou zone/enregistrements SRV absents |
| « The SID of the domain ... was identical to the SID of this machine » | VM clonée sans sysprep : faire un sysprep et réessayer |
| Erreur liée à l'heure / Kerberos | Corriger l'heure ou le fuseau horaire (`w32tm /resync`) |
| « La relation d'approbation entre cette station de travail et le domaine principal a échoué » | Mot de passe du compte ordinateur désynchronisé (souvent après restauration d'un **snapshot** du client). `Test-ComputerSecureChannel -Repair -Credential HP\Administrateur`, ou retirer puis rejoindre le domaine |
| Joindre fonctionne mais la session est lente ou les GPO ne s'appliquent pas | DNS secondaire public (8.8.8.8) sur le client : ne mettre **que** les DC en DNS |

Vérifier le canal sécurisé : `Test-ComputerSecureChannel -Verbose` ou `nltest /sc_verify:hp.lan`.

# Questions de révision

1. Quel paramètre réseau du client est indispensable pour joindre le domaine ?
2. Quelle édition de Windows 10/11 ne peut pas rejoindre un domaine ?
3. Où arrivent par défaut les comptes ordinateurs ? Comment les placer ailleurs ?
4. Comment se connecter avec un compte **local** sur un PC membre du domaine ?
5. Après restauration d'un snapshot du client, la connexion échoue avec une erreur de relation d'approbation. Pourquoi ?