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 ?

Revision #1
Created 2 November 2026 13:51:06 by Hugo
Updated 2 November 2026 13:51:06 by Hugo