

# Chapitre 3
# GPO, AD et processus d'application

## 1. Introduction

Gérer les stratégies locales de chaque poste de travail d'une organisation demande beaucoup de travail ainsi qu'une gestion décentralisée des informations. Lorsqu'une modification est faite concernant les politiques de stratégie de groupe, il faut effectuer les mises à jour sur chaque poste de travail concerné. Si le workgroup possède un nombre élevé d'ordinateurs, le travail des administrateurs prend tellement de temps pour effectuer des tâches répétitives qu'il en perd pratiquement son intérêt.

Dans le chapitre Stratégie locale et de domaine nous avons vu l'importance et les avantages qu'Active Directory pouvait nous apporter en termes de centralisation des informations dans un annuaire **LDAP** (*Lightweight Directory Access Protocol*). Nous avons mis en évidence la charge administrative supplémentaire lorsque l'on déploie des stratégies de groupe dans un Workgroup, ainsi que la phase importante de conception et réflexion indispensable lorsque l'on souhaite mettre en place un annuaire Active Directory, puisque la structure de ses différents objets va faciliter ou non la gestion de notre domaine.

Les GPO de domaine fonctionnent à partir d'un seul serveur contrôleur de domaine (Windows 2016, 2019 et 2022) et d'un poste de travail (Windows 10 ou 11).

Remarque

*Nous faisons référence seulement aux systèmes d'exploitation qui sont actuellement en support officiel par Microsoft.*

Dans ce chapitre, il s'agit d'approfondir la compréhension des stratégies de groupe au sein des réseaux professionnels dont l'infrastructure respecte le système pyramidal de forêt et de domaine Active Directory.

## 2. La clé est Active Directory

Les stratégies de groupe fonctionnent en corrélation étroite avec Active Directory. C'est dans l'Active Directory que sont liées les GPO pour qu'elles s'appliquent ensuite sur les postes clients.

La structure de l'Active Directory d'une entreprise, et plus particulièrement la structure des unités d'organisation, définit la façon dont il est possible de gérer les GPO.

La constitution de l'architecture Active Directory détermine la logique de création des stratégies de groupe. Il est intéressant de disposer d'un Active Directory scindé et organisé en concordance avec les différents secteurs d'activités de l'entreprise. Dans cette hypothèse, il sera plus facile de générer des stratégies de groupe orientées vers les besoins des utilisateurs et de les lier aux unités d'organisation correspondantes.

Il est recommandé également de maintenir la simplicité dans l'agencement des unités d'organisation. Une structure simple et compréhensible facilite la gestion des stratégies de groupe.

Pour illustrer ce livre sur les stratégies de groupe, nous allons créer un domaine Active Directory ayant comme nom de domaine **Formation.lok**. Ce domaine aura deux contrôleurs de domaine : **DC** et **SRV1** fonctionnant sous Windows Server 2022 et un poste client nommé **Portable01** fonctionnant sous Windows 11 Entreprise.

## 2.1 Les contrôleurs de domaine

Pour le processus de création d'un contrôleur de domaine Active Directory, il faut dans un premier temps que le futur contrôleur de domaine ait un nom correct. Dans notre cas, ils portent les noms de **DC** et **SRV1**. Ces postes doivent être toujours joignables donc ils doivent avoir une adresse **IPv4 fixe**. Puis nous devons installer les services de domaine Active Directory afin de promouvoir notre **DC** en contrôleur de domaine.

Dans Windows Server 2019 et depuis Windows Server 2008 R2, Microsoft a mis l'accent sur son outil PowerShell qui est désormais en version 5.1 et qui est inclus dans le système d'exploitation, mais il existe la version 7.4.3 qui est à présent open source, disponible sur l'ensemble des plateformes (Windows, Linux, Mac OS). Voici quelques scripts qui vous permettent de configurer rapidement les deux serveurs. Pour exécuter ces scripts, il faut au préalable autoriser l'exécution des scripts avec la commande **`Set-ExecutionPolicy RemoteSigned`**.

La structure Active Directory est le point d'origine de nombreux aspects du réseau. L'application permet à un serveur autonome de devenir contrôleur de domaine, d'héberger les comptes utilisateurs et ordinateurs du réseau ainsi que les groupes de sécurité. De fait, ces éléments offrent la possibilité de définir les niveaux d'accès de chaque utilisateur sur le réseau. Le processus de création d'un annuaire Active Directory implique la mise en place d'un serveur DNS (*Domain Name System*).

Au terme de ces opérations, il est alors possible d'installer ou d'utiliser directement la console de gestion des stratégies de groupe, en fonction de la version du serveur installé.

Ces scripts vont nous permettre de configurer rapidement nos machines et de mettre en place le domaine Active Directory.

Les scripts suivants sont en téléchargement sur le site des Éditions ENI.

### 2.1.1 Promotion du premier contrôleur de domaine

– DC_Script1.ps1

```
#On renomme le serveur
Rename-Computer -NewName DC

# On fixe une adresse IP fixe à la carte réseau
New-NetIPAddress -InterfaceAlias "Ethernet*" -IPAddress 10.0.0.1
- AddressFamily IPv4 -PrefixLength 8
Set-DnsClientServerAddress -InterfaceAlias Ethernet
-ServerAddresses 127.0.0.1

#On installe les services de domaine Active Directory
Install-WindowsFeature -name AD-domain-Services
-IncludeManagementTools

#On redémarre
Restart-Computer
```

– DC_Script2.ps1

```
# On effectue la promotion du contrôleur de domaine

Import-Module ADDSDeployment
Install-ADDSForest `
-DomainName "Formation.lok" `
```

### 2.1.2 Ajout d'un contrôleur de domaine supplémentaire

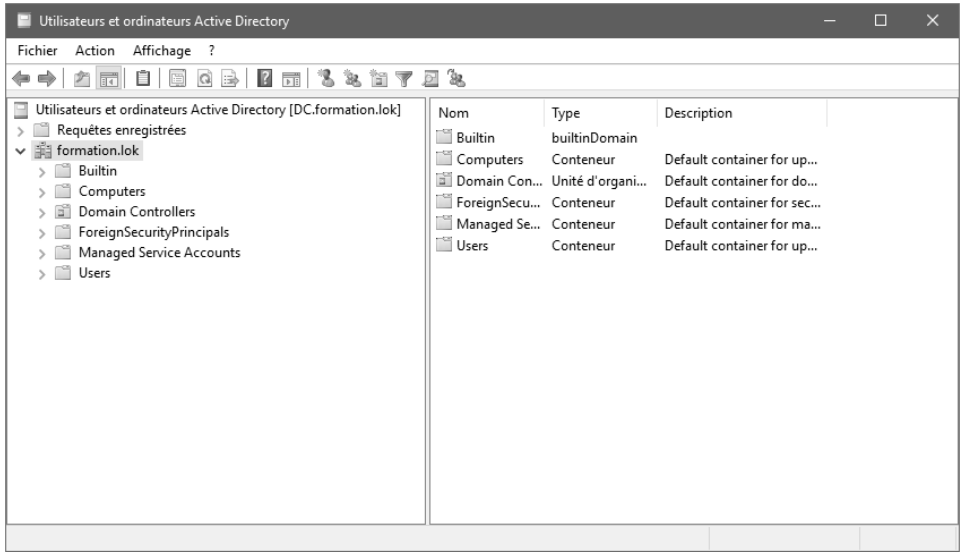
– SRV1_Script1.ps1

```
#On renomme le serveur
Rename-Computer -NewName SRV1

# On fixe une adresse IP fixe à la carte réseau
New-NetIPAddress -InterfaceAlias Ethernet -IPAddress 10.0.0.2
-AddressFamily IPv4 -PrefixLength 8
Set-DnsClientServerAddress -InterfaceAlias Ethernet
-ServerAddresses 10.0.0.1

#On installe les services de domaine Active Directory
Install-WindowsFeature -name AD-domain-Services
-IncludeManagementTools

#On redémarre
Restart-Computer
```

– SVR1_Script2.ps1

```
#
# Script Windows PowerShell pour le déploiement d'AD DS
#
Import-Module ADDSDeployment
Install-ADDSDomainController `
-NoGlobalCatalog:$false `
-CreateDnsDelegation:$false `
-Credential (Get-Credential) `
-CriticalReplicationOnly:$false `
-DatabasePath "C:\Windows\NTDS" `
-DomainName "Formation.lok" `
-InstallDns:$true `
-LogPath "C:\Windows\NTDS" `
-NoRebootOnCompletion:$false `
-ReplicationSourceDC "DC.formation.lok" `
-SiteName "Default-First-Site-Name" `
-SysvolPath "C:\Windows\SYSVOL" `
-Force:$true
```

L'implémentation d'Active Directory fait naître la structure par défaut de l'annuaire, mais il appartient aux administrateurs de créer leur propre structure en correspondance avec les besoins de l'entreprise.



La mise en place d'une telle organisation requiert la mise au point d'une méthodologie solide lorsque les objectifs visés sont orientés vers la densité, la cohérence et la pérennité d'Active Directory.

S'il est prévu d'implémenter une politique de stratégie de groupe dès la création du domaine, il est impératif de garder à l'esprit que les GPO s'appuient sur Active Directory pour fonctionner. Plus la structure Active Directory est pensée et organisée en fonction des besoins de l'entreprise, plus elle sera accueillante et facilitera la mise en place de stratégies de groupe pertinentes. La façon d'organiser Active Directory dépend de la taille de l'entreprise et de son organisation.

Il est fortement recommandé de planifier un tel projet avant sa mise en route, cela évite de nombreuses complications futures.

Afin d'illustrer les propos contenus dans cette section du chapitre, voici une proposition d'exemple de structure Active Directory flexible pour l'intégration de stratégies de groupe.

## 2.2 Modèle de structure des unités d'organisation

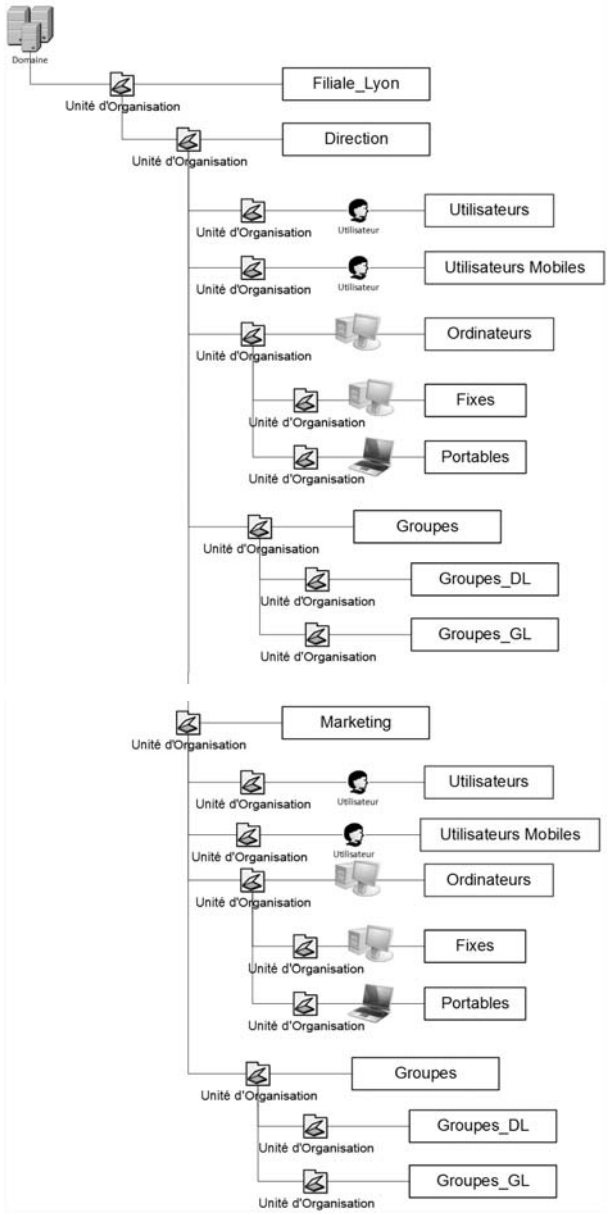
Les structures Active Directory varient d'une organisation à une autre. Voici un exemple illustré par un schéma qui propose un modèle de structure permettant le déploiement des stratégies de groupe.

**Remarque**

*Attention, l'arborescence Active directory proposée dans le livre représente seulement une structure Active Directory qui n'est plus valable aujourd'hui dans les entreprises, mais qui facilite la compréhension et le fonctionnement des stratégies de groupes. Nous traiterons dans le chapitre Étude de cas, le cas d'une entreprise moderne et nous verrons comment créer nos Unité d'Organisations (OU).*

Scénario

La société Formation de France souhaite mettre en place un annuaire Active Directory. Elle possède trois filiales situées à Lyon, Marseille et Nantes, afin de mettre en place une infrastructure centralisée et des stratégies de groupe.




*Exemple d'une structure d'OU dans Active Directory*

### Le modèle en détail

La structure Active Directory du modèle présente les caractéristiques d'un annuaire contenant un grand nombre d'objets.

Le domaine **Formation.lok** contient les unités d'organisation des filiales de **Lyon**, **Marseille** et **Nantes** qui s'appellent respectivement **Filiale_Lyon**, **Filiale_Marseille** et **Filiale_Nantes**.

L'organisation déployée au sein de l'unité d'organisation Filiale_Lyon suit une logique de classement des comptes objets d'Active Directory par service et par activité.

Chaque service de l'entreprise possède une unité d'organisation contenant des sous-catégories destinées à héberger les comptes utilisateurs et ordinateurs appartenant à ce service.

Une unité d'organisation spécifique aux groupes existe au même niveau hiérarchique que les unités d'organisation des filiales.

### À l'échelle des filiales

Étudions à présent la structure des unités d'organisation qui composent les filiales.

Chaque filiale comporte plusieurs conteneurs. Les OU de service hébergent les comptes utilisateurs et les comptes ordinateurs.

L'unité d'organisation des comptes ordinateurs est divisée en deux sous-catégories afin de séparer les ordinateurs portables des ordinateurs de bureau.

Dans ce cas, il est possible de lier des stratégies de groupe aux utilisateurs du service et de lier des stratégies aux utilisateurs mobiles connectés avec des liaisons lentes.

Il est également possible d'appliquer des stratégies à tous les ordinateurs du service ou uniquement aux ordinateurs portables ou encore aux seuls ordinateurs de bureau.

Le découpage de la structure Active Directory prend une dimension importante dans la mesure où il définit en partie la façon dont il est possible d'implémenter les stratégies de groupe.

Pour mettre en œuvre cette arborescence, voici un extrait du script PowerShell disponible en téléchargement sur le site des Éditions ENI.

– Arborescence Active Directory.ps1

```
Write-host{
################################################
# Jérôme Bezet-Torres
# GPO Sous server
# Création de l'arborescence Active Directory
################################################
}
# Déclaration des variables
$domain="Formation"
$Ext="lok"
$Villes= @("Filiale_Marseille","Filiale_Lyon","Filiale_Paris")
$Services= @("Marketing","Informatique","Direction","Comptabilité")
$Groupes= @("Groupes_DL","Groupes_GL","Ordinateurs","Utilisateurs",
"Utilisateurs Mobiles")
$Type= @("Fixe","Portable")
$ordi=$Groupes[2]

#Création des OU filiales
Foreach($v in $Villes )  {New-ADOrganizationalUnit -Name $v
-ProtectedFromAccidentalDeletion $false}

#Création des OU de services
Foreach($s in $Services){
Foreach($v in $Villes ){
New-ADOrganizationalUnit -Name $s -Path "ou=$v,dc=$domain,dc=$Ext"
-ProtectedFromAccidentalDeletion $false}}
```

**Remarque**

*Le script a été coupé volontairement par l'auteur.*