CCI Nîmes

Tuto : GPO

Windows Server et AD

BOUDECHICHA Redhouane
[Date]

Présentation d’une GPO

Une **GPO** (Group Policy Object, ou Objet de Stratégie de Groupe en français) est un mécanisme utilisé dans **Active Directory** pour gérer et appliquer des configurations centralisées sur des ordinateurs et des utilisateurs d'un réseau. Les GPO permettent aux administrateurs système de définir des paramètres et des règles qui sont automatiquement appliqués aux machines et aux comptes utilisateur dans un domaine Active Directory.

Fonctionnement

- **Portée** : Les GPO peuvent s'appliquer à différents niveaux d'Active Directory :
    1. **Site** : Affecte tous les objets (ordinateurs et utilisateurs) dans un site spécifique.
    2. **Domaine** : Affecte tous les objets dans un domaine.
    3. **Unité Organisationnelle (OU)** : Affecte uniquement les objets dans une OU spécifique.
- **Héritage** : Les GPO appliquées à un niveau supérieur (par exemple, domaine) sont héritées par les niveaux inférieurs (par exemple, OU). Cependant, il est possible de bloquer ou de forcer l'application d'une stratégie.

Types de paramètres configurables

1. **Configuration utilisateur** :
    - Politiques d'accès (par exemple, restreindre l'accès à certains logiciels).
    - Script de connexion/déconnexion.
    - Redirection de dossiers (par exemple, déplacer le dossier Documents vers un serveur).
2. **Configuration ordinateur** :
    - Installation de logiciels.
    - Paramètres réseau (proxy, DNS).
    - Configuration de la sécurité (mots de passe, pare-feu, restrictions d'accès).

Exemples d'utilisation des GPO

1. **Sécurité** :
    - Imposer une longueur minimale pour les mots de passe.
    - Désactiver les périphériques USB.
    - Configurer des restrictions d'accès à distance.
2. **Déploiement de logiciels** :
    - Installer des applications automatiquement sur des postes clients.
3. **Personnalisation des bureaux** :
    - Définir un fond d'écran spécifique.
    - Bloquer l'accès au Panneau de configuration.
4. **Scripts automatisés** :
    - Exécuter des scripts à l’ouverture de session ou à l'arrêt de l'ordinateur.

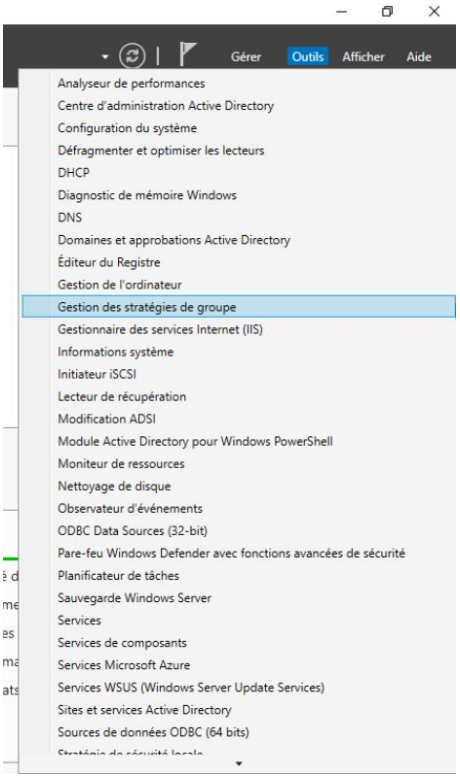
Les GPO sont un puissant outil de gestion centralisée, mais une mauvaise configuration peut entraîner des dysfonctionnements ou des problèmes de sécurité, d'où l'importance de tester les politiques avant de les appliquer à tout le domaine.

Comment réaliser crée une GPO et la liée a une UE (OU en anglais)

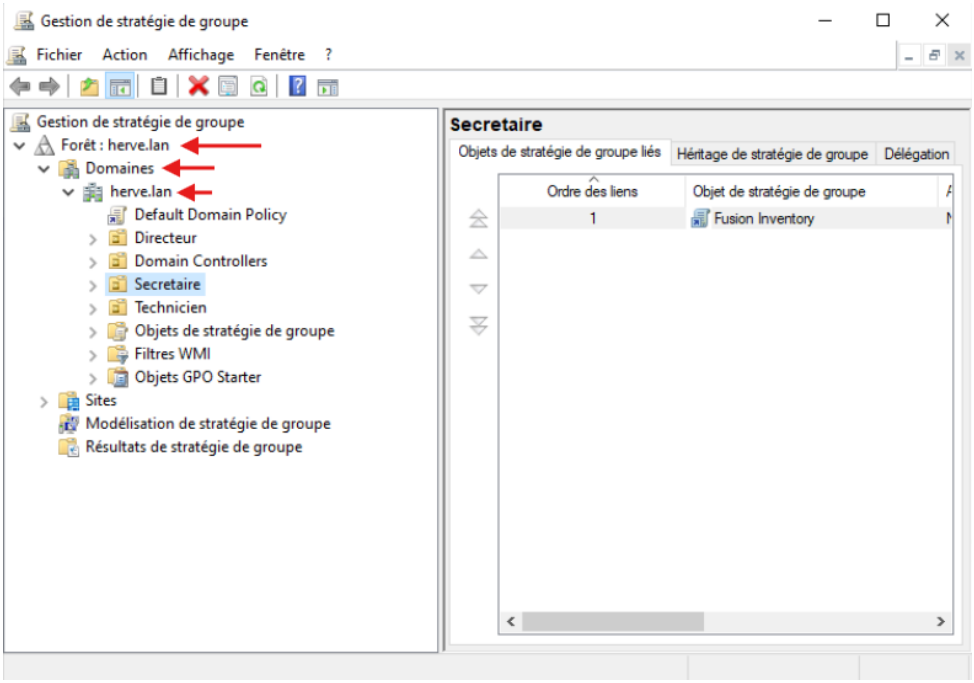
On part du principe que votre AD fonctionne, que des comptes utilisateurs y sont présent et stocké dans des UE et que bien sur vous les avez testés avant.

Crée la GPO

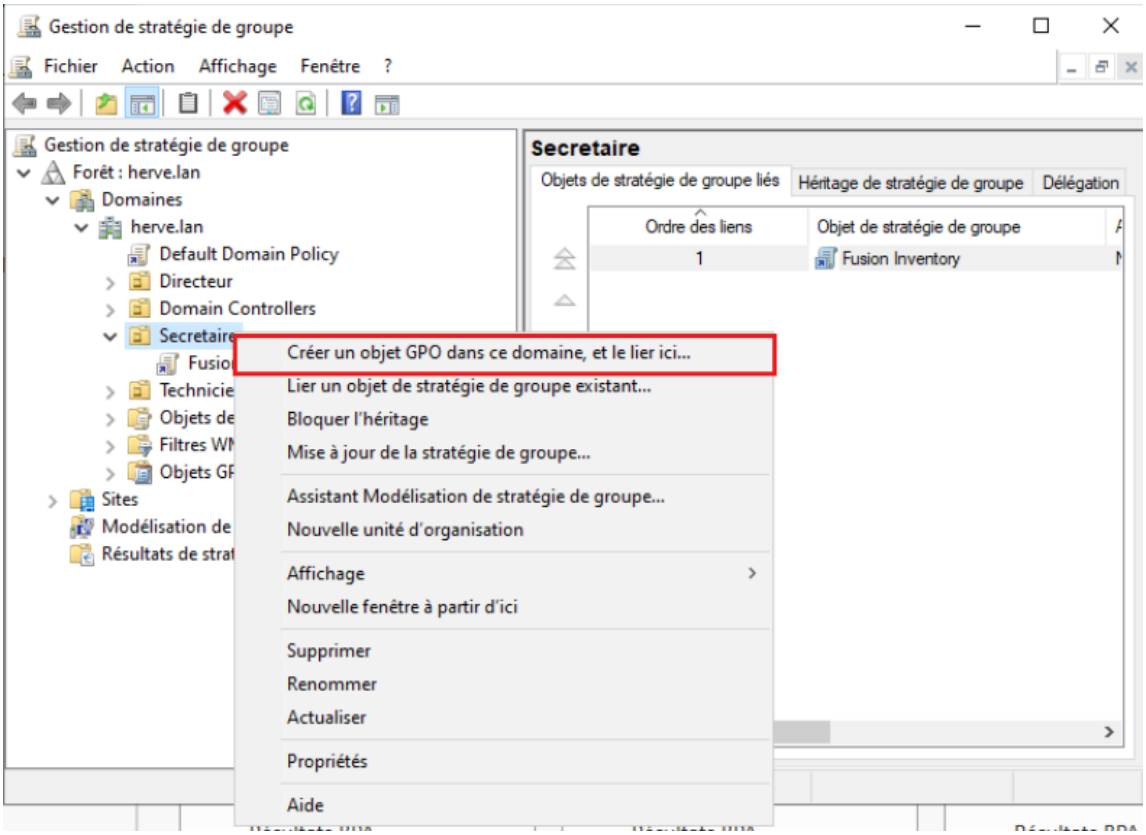
Via l'outil de gestionnaire des serveurs rendez-vous sur l'onglet Outils puis chercher la section « gestion des stratégies de groupe »



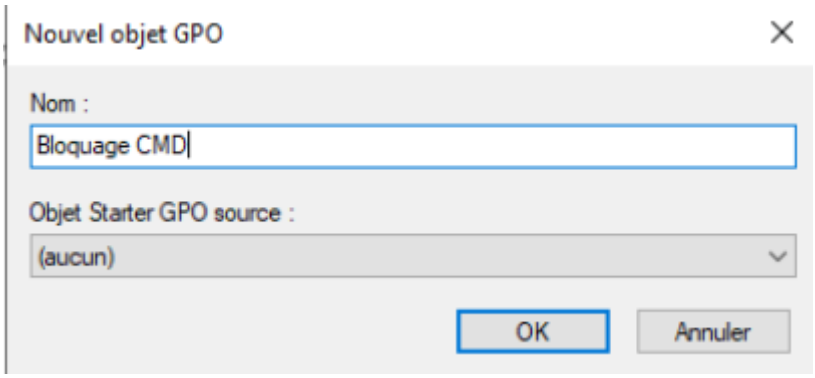
Ensuite il faudra cliquez sur la petite flèche pour dérouler jusqu'à arriver jusqu'à votre domaine qui contient évidemment vos UE (et plein d'autre section) n'oubliez pas de dérouler aussi celle de votre UE, car quand vous aurez créé votre GPO elle apparaitra dedans.



Ensuite Faites clic droit sur votre UE et « crée un objet GPO dans ce domaine, et le lier ici »



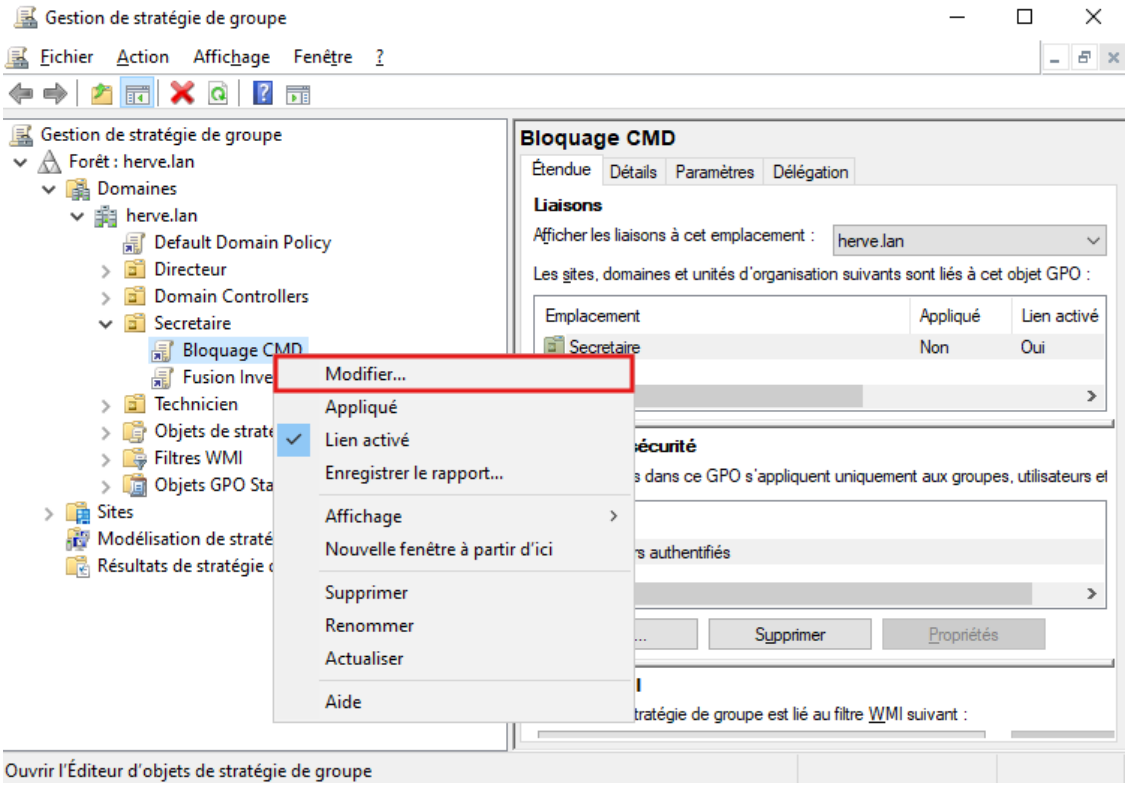
Donnez lui un nom et c’est terminer vous avez créé une GPO liée à votre UE directement



Attribuer un rôle à votre GPO

Maintenant l’objectif est de donné un rôle à cette GPO car pour le moment elle ne sert quasiment à rien. Donc comme exemple on va retirez l’utilisation du CMD, sachez néanmoins que vous pouvez quasiment tout bloquer que ce soit au niveau machine ou Windows.

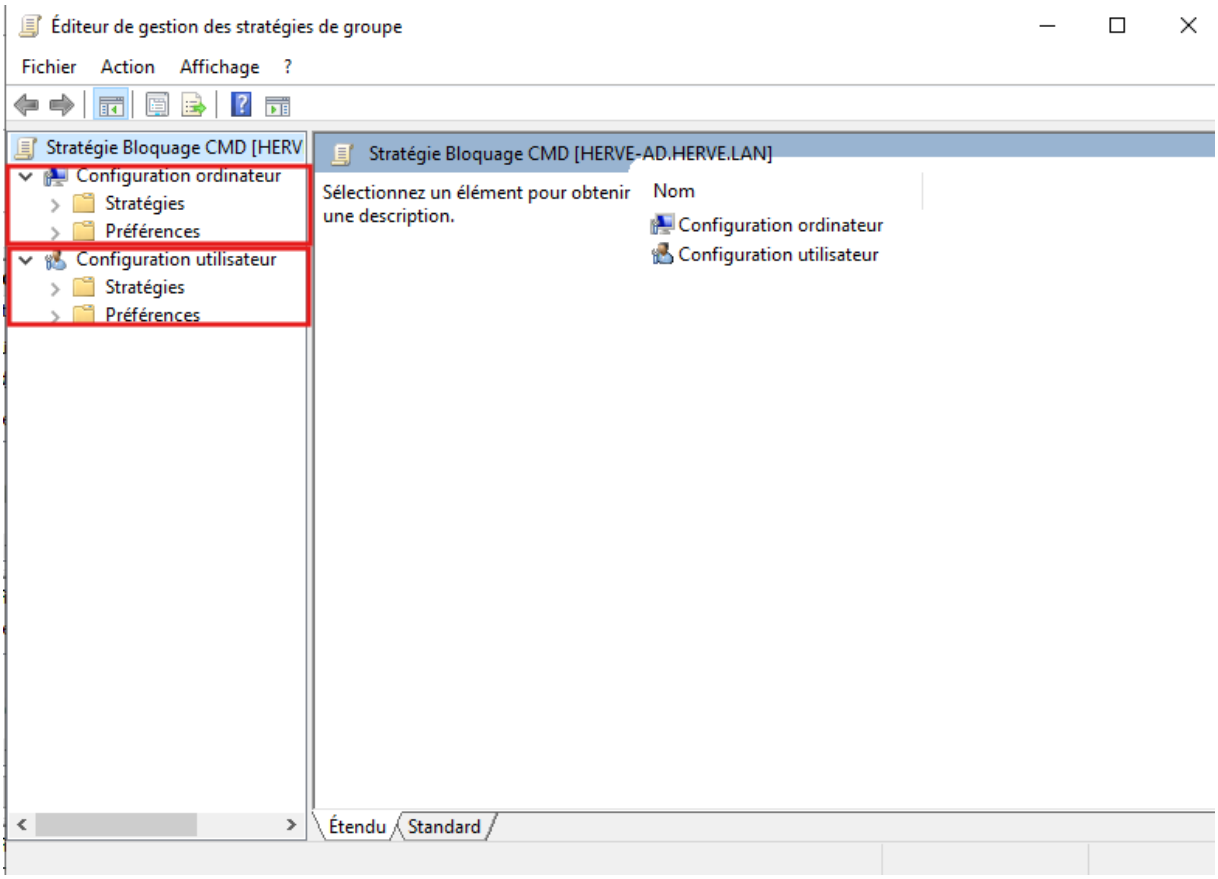
Pour ce faire faite clic droit sur votre GPO et non pas votre UE, puis sélectionner modifier cela vous ouvrira une pages avec un large choix d’option applicable.



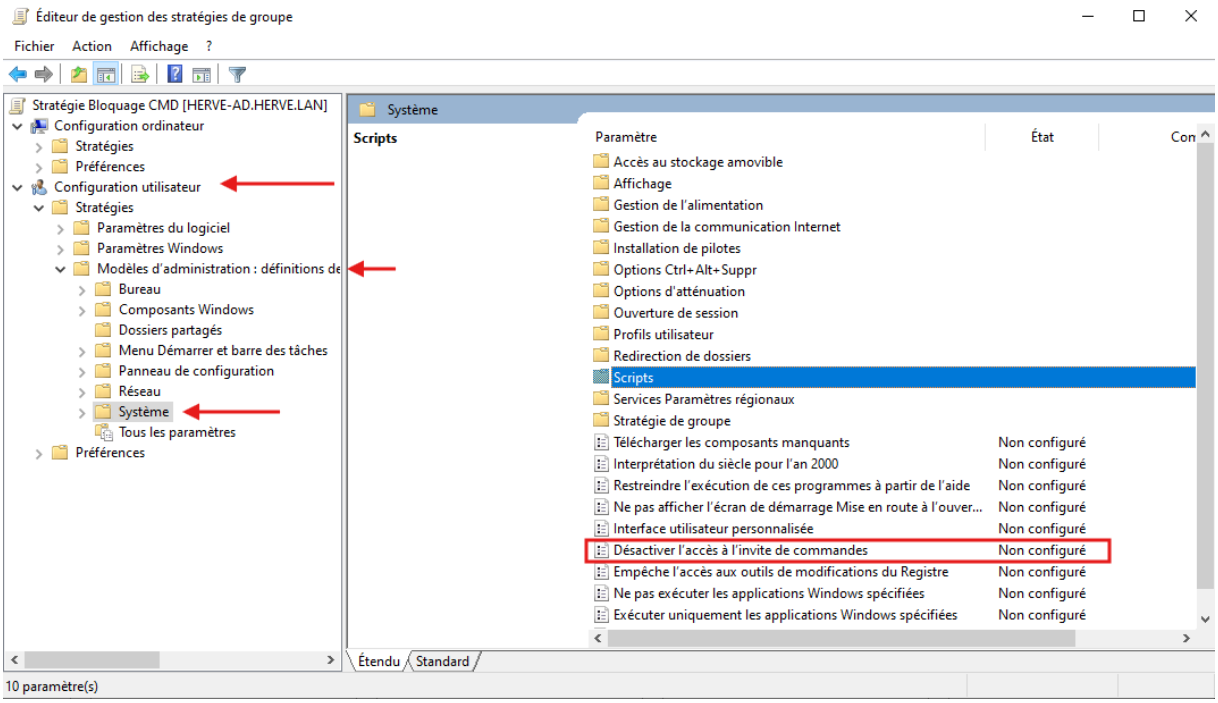
Voici les deux sections rencontrées, La configuration ordinateur dont les paramètres configurés affectent le système dans son ensemble, indépendamment de l'utilisateur qui se connecte.

Et la configuration Utilisateur ou les paramètres configurés affectent uniquement les sessions utilisateur, peu importe l'ordinateur utilisé.

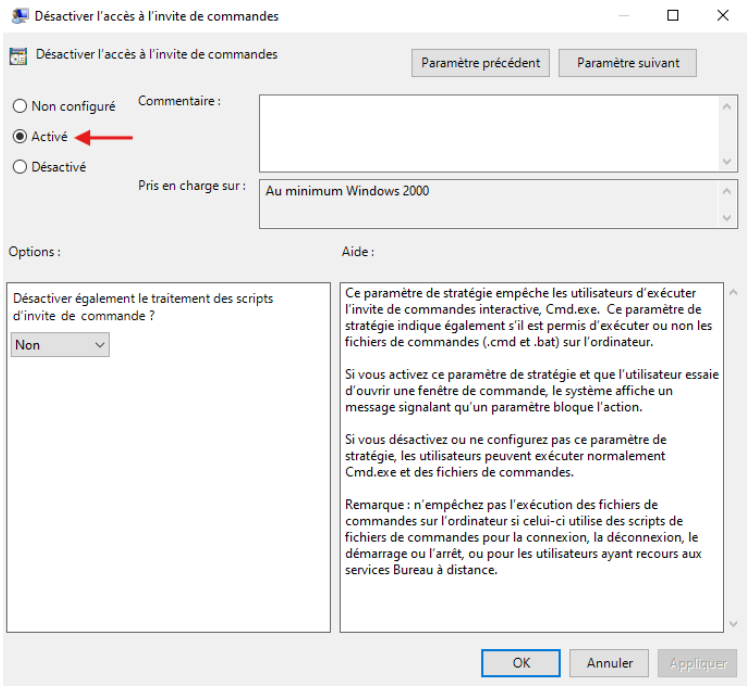
Dans notre cas nous allons nous rendre dans la configuration utilisateur (sachez que même si c'est une configuration utilisateurs elle ne s'appliquera pas uniquement à l'utilisateur mais aux unités d'organisation)



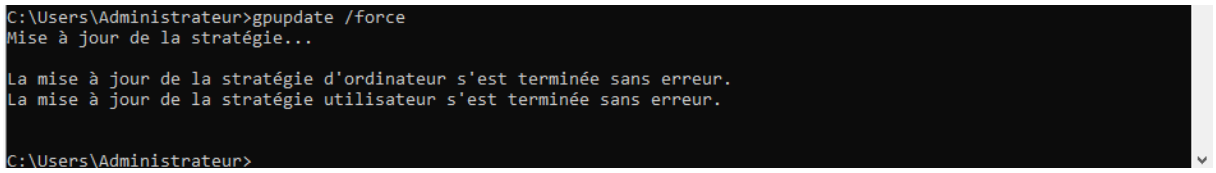
Donc rendez vous dans la configuration utilisateur, dérouler les stratégies, le modèles d'administration puis cliquez directement sur le dossier Système et repérer « Désactiver l'accès à l'invite de commande.



Doublez clic sur celle-ci et cocher bien Activé puis Appliquer et OK.



Et au final rendez vous dans votre CMD du serveur AD, et tapez la commande gpupdate /force pour forcez la mise a jours immédiats des paramètre (Au cas ou des utilisateurs serait déjà connecté et pour faciliter le déploiement)



Maintenant plus qu'a se rendre sur une machine cliente et se connecter a un qui fais partie de l'Unité d'Organisation viser et normalement le tour est jouer.

Vous aurez se magnifique message 😊 s