

# Sécurité dans les domaines MS Windows : Les GPO

**Thibault LENGAGNE et Valentin JAOUEN**

Centrale Supélec - Campus de Rennes

January 21, 2016

- 1 Introduction
- 2 Active Directory
- 3 Stratégie de groupe
- 4 Mise en oeuvre des stratégies de groupe : les GPOs
- 5 Conclusion

*Windows Server* est la dénomination regroupant les systèmes d'exploitation orientés serveur de Microsoft :

- Windows NT
- Windows 2000 Server
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Depuis *Windows 2000 Server* sont apparut les fonctionnalités suivantes :

- Active Directory, un annuaire d'organisation et de gestion des objets réseaux
- Un serveur web *Internet Information Services* (IIS) intégré
- Terminal Server, un service permettant d'ouvrir une session à distance
- La prise en charge d'une grande quantité de RAM et de processeurs multiples
- La prise en charge de nombreux protocoles
- La gestion centralisée de clients multiples
- Une interface de gestion réseau

- Désigne la configuration logicielle du système par rapport aux utilisateurs
- Par défaut suite à une installation de *Windows* : aucune stratégie n'est configurée

## Conséquence dangereuse

Tout est permis en fonction des droits des groupes d'utilisateurs prédéfinis (administrateurs, utilisateurs, utilisateurs avec pouvoir, ...).

- 1 Introduction
- 2 Active Directory**
- 3 Stratégie de groupe
- 4 Mise en oeuvre des stratégies de groupe : les GPOs
- 5 Conclusion

- *Network Directory Services* (NTDS) à l'origine
- Présenté en 1996 pour la première fois
- Première utilisation en 1999 dans *Windows 2000 Server*
- Amélioré constamment depuis
- Résulte d'une évolution de la BDD de comptes de domaine *Security Account Manager* (SAM) et une mise en oeuvre de LDAP
- *Active Directory* est donc un annuaire LDAP

## Objectif principal

Fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows.

## Objectifs secondaires

- Attribution et application de stratégies
- Distribution de logiciels
- Installation de mises à jour critiques par les administrateurs



## Active Directory

Service d'annuaire utilisé pour stocker des informations relatives aux ressources réseau sur un domaine.

## Structure Active Directory

Organisation hiérarchisée d'objets classés en trois catégories :

- les ressources : imprimantes, ordinateurs ...
- les services : courrier électronique, intranet, ...
- les utilisateurs : comptes utilisateurs et groupes

Ces objets peuvent être regroupés en :

- unités d'organisation permettant l'application des GPO
- groupes universels, globaux ou locaux
- arbres et forêts

- 1 Introduction
- 2 Active Directory
- 3 Stratégie de groupe**
- 4 Mise en oeuvre des stratégies de groupe : les GPOs
- 5 Conclusion

- Permet de configurer des restrictions d'utilisation de *Windows*
- Permet de configurer des paramètres à appliquer soit sur un ordinateur donné, soit sur un compte utilisateur donné

D'où la possibilité d'agir sur :

- La définition d'un environnement
- Le déploiement de logiciels
- L'application des paramètres de sécurité

- Menu démarrer et Barre des tâches
  - ① Suppression du menu Documents dans le menu Démarrer
  - ② Suppression des Connexions réseau et accès distant du menu Démarrer
  - ③ Suppression du menu Exécuter dans le menu Démarrer
  - ④ Désactivation de la fermeture de session dans le menu Démarrer
  - ⑤ Désactivation de la commande Arrêter
- Panneau de configuration
  - ① Désactivation du Panneau de configuration
  - ② Masque de certaines applications du Panneau de configuration
- Système
  - ① Activation des quotas de disque
  - ② Désactivation des outils de modifications du Registre
  - ③ Désactivation de l'invite de commandes
- Internet Explorer
  - ① Désactivation de la modification des paramètres de la page de démarrage

- 1 Introduction
- 2 Active Directory
- 3 Stratégie de groupe
- 4 Mise en oeuvre des stratégies de groupe : les GPOs**
- 5 Conclusion

- GPO signifie *Group Policy Object*
- Apparus avec *Windows 2000 Server* avec l'*Active Directory*
- Un GPO est un objet *Active Directory*
- Il contient un ensemble de paramètres applicables à un utilisateur ou à un ordinateur
- Les GPOs sont accessibles dans tous le domaine, dans le dossier SYSVOL

## SYSVOL ?

Dossier partagé sur un volume NTFS entre les contrôleurs de domaine et avec les clients du domaine.

# Avantages des GPO

- Configurent de manière automatisée et centralisée les postes de travail et les serveurs *Windows* d'un environnement donné
- La configuration des postes n'est pas stockée localement. Il suffit d'ajouter un poste à un GPO existant et la configuration s'applique
- La suppression d'un GPO restaure les paramètres locaux
- Il est presque possible de configurer n'importe quel paramètre par GPO
- Configuration des postes uniforme
- Les GPO sont réappliquées à intervalle régulier

- La gestion des GPOs n'est pas chose aisée
  - Il faut être sûr d'appliquer le ou les bons GPOs aux bons ordinateurs et/ou utilisateurs
  - Beaucoup d'administrateurs sont confrontés à ce problème lorsqu'ils mettent en oeuvre les GPOs
- Si chaque poste ou chaque utilisateur du réseau nécessite une configuration particulière, les GPOs ne sont plus vraiment efficaces



- 1 Introduction
- 2 Active Directory
- 3 Stratégie de groupe
- 4 Mise en oeuvre des stratégies de groupe : les GPOs
- 5 Conclusion**



Merci de votre attention