CentraleSupélec

Sécurité dans les domaines MS Windows : Les GPO

Thibault LENGAGNE et Valentin JAOUEN

Centrale Supélec - Campus de Rennes

19 janvier 2016

Plan

Windows Server

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

Fonctions principales

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

Stratégie

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

Conséquence dangereuse

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

Plan

Historique

- *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

Objectifs

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

Structure Active Directory

Active Directory

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

Structure Active Directory

Organisation hiérarchisée d'objets classé en trois catégories :

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

Plan

Présentation

- 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

Exemple de stratégie de groupe

- 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

Plan

Présentation

- 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 stockées et répliquées dans le dossier SYSVOL

SYSVOL ?

Dossier partagé 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 donnée
- La configuration des postes n'est plus stockée localement grâce au dossier SYSVOL
  - Il suffit d'appliquer un GPO existant à un nouveau poste et la configuration s'applique
- La suppression d'une GPO restaure les paramètres locaux appliqués avant les GPOs
- Il est théoriquement possible de configurer n'importe quel paramètre par GPO
- Configuration des postes uniforme
- Les GPO sont réappliquées à intervalle régulier

Limites des GPO

- 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

Plan

Merci de votre attention