

Microsoft Windows Server 2008

Installation d'une GPO

Les GPO (Group Policies Object) permettent de la mise en œuvre de stratégies spécifiques liées à des groupes définis dans l'Active Directory.

Les stratégies de groupe sont des fonctions de gestion centralisée de la famille Microsoft Windows. Elles permettent la gestion des éléments inscrits dans un environnement Active Directory.

Bien que les stratégies de groupe soient régulièrement utilisées dans les entreprises, elles sont également utilisées dans les écoles ou dans les petites organisations pour restreindre les actions et les risques potentiels comme par exemple le verrouillage du panneau de configuration, la restriction de l'accès à certains dossiers, la désactivation de l'utilisation de certains exécutables, la gestion des imprimantes, le déploiement d'applications, etc.

Les GPO sont supportées sur les systèmes serveur Windows 2003 Server, Windows Server 2008 et Windows Server 2008 R2, ainsi que sur les systèmes clients Windows 2000, Windows XP Professionnel, Windows Vista et Windows 7.

Sommaire

1 Présentation

2 Les trois phases de l'utilisation des stratégies de groupe

- 2.1 Création et édition des stratégies de groupe
- 2.2 Liaison des stratégies de groupe
- 2.3 Application des stratégies de groupe

3 Les stratégies de groupe locales

4 Quelques commandes

5 Exemples

- 5.1 Stratégie de groupe pour déploiement logiciel
- 5.2 Stratégie de groupe pour gestion de l'impression

1 Présentation

Les stratégies de groupe peuvent contrôler des clés de registre, la sécurité NTFS, la politique de sécurité et d'audit, l'installation de logiciel, les scripts de connexion et de déconnexion, la redirection des dossiers, et les paramètres d'Internet Explorer. Les paramétrages sont stockés dans les stratégies de groupe. Chaque stratégie de groupe possède un identifiant unique appelé GUID (« Globally Unique Identifier »). Chaque stratégie de groupe peut être liée à un ou plusieurs domaine, site ou unité d'organisation Active Directory. Cela permet à plusieurs objets ordinateurs ou utilisateurs d'être contrôlés par une seule stratégie de groupe et donc de diminuer le coût d'administration globale de ces éléments.

Les stratégies de groupe utilisent des fichiers de modèle d'administration avec les extensions .ADM ou .ADMX qui décrivent les clés de registre modifiées par l'application des stratégies de groupe. Sur un ordinateur de travail, les modèles d'administration sont stockés dans le répertoire %WinDir%\Inf, alors que sur un contrôleur de domaine Active Directory, pour chaque domaine et pour chaque stratégie de groupe, ils sont stockés dans un répertoire individuel (Le « group policy template », ou GPT) au sein du répertoire Sysvol. Les fichiers .ADMX sont des fichiers basés sur le format XML et introduits par Windows Vista pour la gestion des stratégies de groupe.

Les stratégies de groupe sont analysées et appliquées au démarrage de l'ordinateur et pendant l'ouverture de session de l'utilisateur. Les ordinateurs rafraîchissent les paramètres transmis par les stratégies de groupe de façon périodique, généralement toutes les 60 ou 120 minutes, ce paramètre étant ajustable par un paramètre de stratégie de groupe.

Les stratégies de groupe sont supportées sur Windows 2000, Windows XP Pro, Windows Vista, Windows 2003, Windows 2008 et Windows 7.

Lorsque l'on utilise un système Windows Serveur avec Active Directory, il existe une stratégie applicable au serveur du domaine appelée Default Domain Controller Policy, et une autre pour les domaine lui-même nommée Default Domain Policy. Ces deux stratégies s'appliquent par défaut sur les machines (serveurs de domaine ou ordinateurs) et les utilisateurs. Déclarés dans le domaine.

L'administrateur dispose ensuite d'un outil de gestion lui permettant de créer et d'administrer d'autres stratégies à appliquer sur les objets de son choix.

2 Les trois phases de l'utilisation des stratégies de groupe

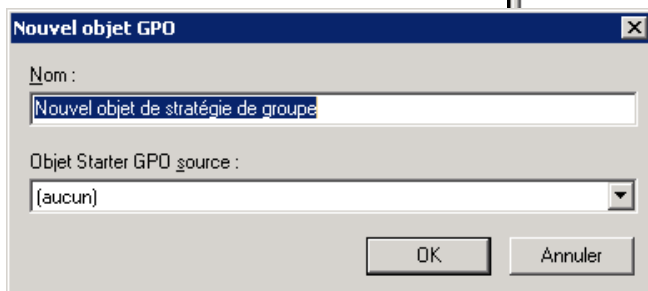
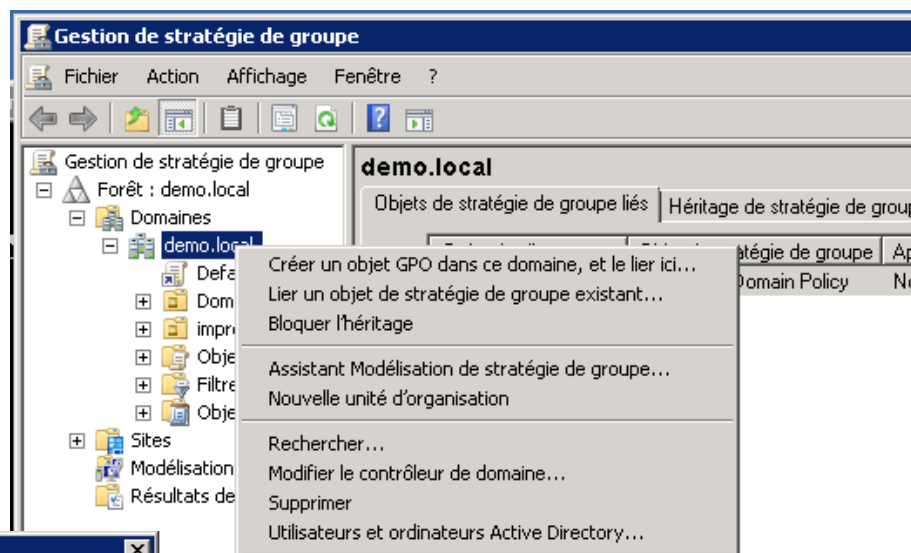
Les stratégies de groupe peuvent être considérées en trois phases distinctes - Création de la stratégie de groupe, Liaison des stratégies de groupe et application des stratégies de groupe.

Création et édition des stratégies de groupe

Les stratégies de groupe peuvent être éditées au travers de un outil accessible soit par l'outil d'administration "Gestion des stratégies de groupe" ou par un appel direct en ligne de commande de la Group Policy Management Console ("gpmc.msc").

La console GPMC simplifie grandement la gestion des stratégies de groupe en fournissant un outil de gestion centralisée et collective des objets. La GPMC inclut de nombreuses fonctionnalités telles que la gestion des paramètres, un panneau pour la gestion du filtrage par groupe de sécurité, des outils de sauvegarde et de restauration et d'autres outils graphiques intégrés à la MMC.

Pour créer une nouvelle GPO, dans la console de gestion de stratégie de groupe faire un clic droit sur le domaine ou l'OU recevant la nouvelle GPO, puis créer un objet dans ce domaine et le lier ici.



Ceci ouvre une fenêtre pour nommer la nouvelle GPO. Saisir le nom retenu et valider par OK

La nouvelle GPO apparaît dans l'arborescence

Liaison des stratégies de groupe

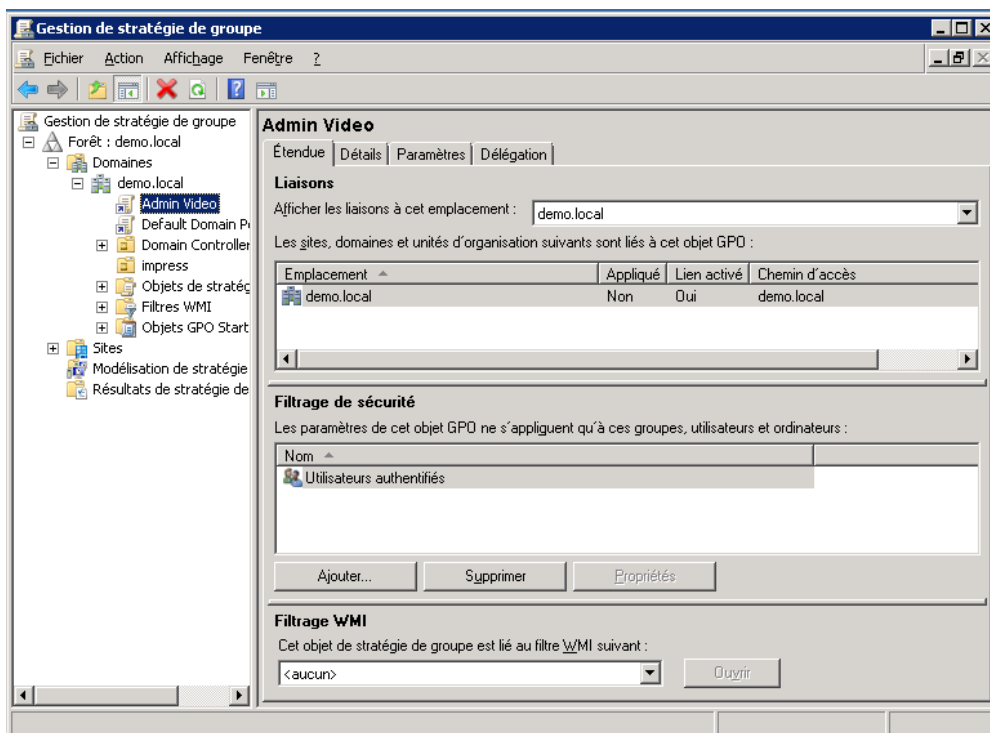
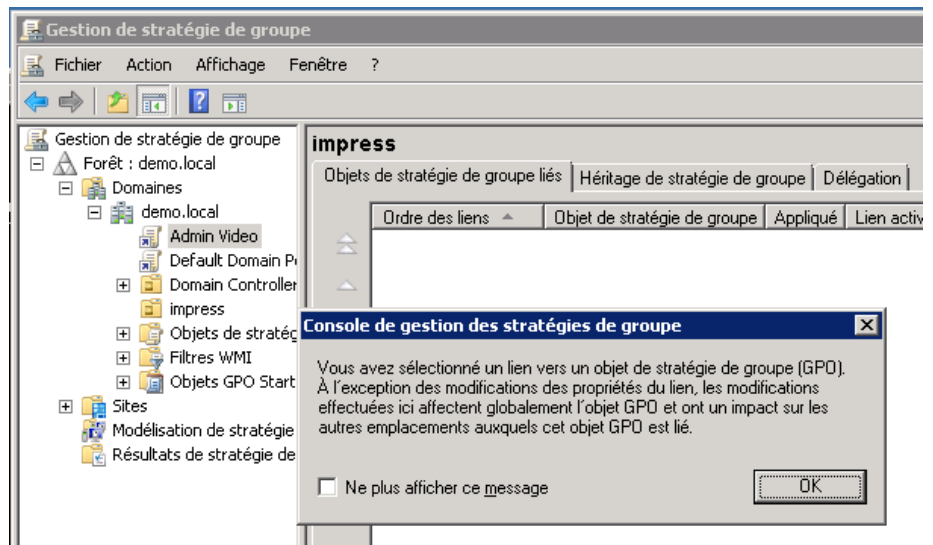
Après avoir créé une stratégie de groupe, elle peut être liée à un site Active Directory, à un domaine ou à une unité d'organisation (OU).

Pour cela, nous allons modifier les paramètres de cette GPO.

Cliquer sur la GPO :

La fenêtre vous demande si vous voulez vraiment modifier les liens de la GPO.

Cliquer sur OK pour ouvrir la fenêtre de configuration



La partie droite de la fenêtre permet alors de modifier les liens et les paramètres.

Cliquer sur les différents onglets pour définir :

- l'étendue
- les paramètres
- les délégations
- Par les détails, il est possible d'activer et désactiver la GPO.

Application des stratégies de groupe

Le client de stratégie de groupe du poste récupère la configuration (de base dans un intervalle aléatoire compris entre 60 et 120 minutes, mais cela est configurable via les stratégies de groupe) qui est applicable à l'ordinateur et à l'utilisateur connecté et l'applique en tenant compte des différents critères de filtre, de sécurité et d'héritage.

Il est possible de forcer la mise à jour de la GPO par la commande *gpupdate /force*.

3 Les stratégies de groupe locales

Les stratégies de groupe locales sont une version plus basique des stratégies de groupe utilisées avec Active Directory. Dans les versions antérieures à Windows Vista, les stratégies de groupe locales peuvent être utilisées sur un ordinateur local, mais ne peuvent pas être utilisées pour des comptes utilisateur ou des groupes. La limitation liée aux utilisateurs peut être contournée en utilisant l'éditeur de base de registre pour modifier les clés sous HKCU ou HKU. Les stratégies de groupe locales réalisent des modifications sous la clé HKLM, ce qui affecte tous les utilisateurs ; les mêmes changements peuvent être effectués sous HKCU ou HKU pour affecter uniquement certains utilisateurs. Microsoft fournit des informations complémentaires sur le site Technet1.

Windows Vista supporte les stratégies de groupe locales multiples, qui permettent de positionner les paramètres pour les utilisateurs individuels.

4 Quelques commandes

Il est possible de vérifier l'application des GPO manuellement avec les commandes

- **gpresult** : cette commande permet d'afficher les GPO actives
- **gpupdate /force** : il est possible de forcer l'application des GPO manuellement avec cette commande

5 Exemples

Nous allons traiter ici quelques exemples de stratégies de groupe courantes.

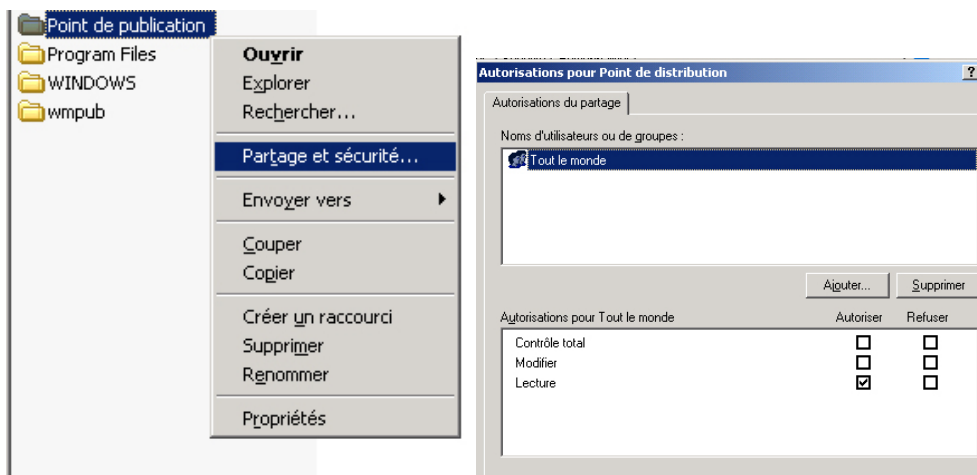
Stratégie de groupe pour déploiement logiciel

1. Introduction

Il s'agit d'une fonctionnalité très utile de Microsoft Active Directory. Elle permet à l'administrateur d'un réseau de pouvoir déployer sur l'ensemble des machines, grâce à une stratégie de groupe, les applications nécessaires aux utilisateurs ou de pouvoir procéder à des mises à jour automatisées et uniformes sur une portion ou l'ensemble d'un parc machines.

2. Création du point de distribution

La première étape, quelque soit le type de logiciels que vous souhaitez voir installer, est de placer dans un répertoire partagé sur le serveur de fichiers, le logiciel que vous souhaitez distribuer. Afin que tout les utilisateurs puisse installer le logiciel il faut mettre les droits en lecture au groupe Tout le Monde. On appelle ce partage point de distribution.



3. Déploiement du logiciel

Création de la GPO de déploiement

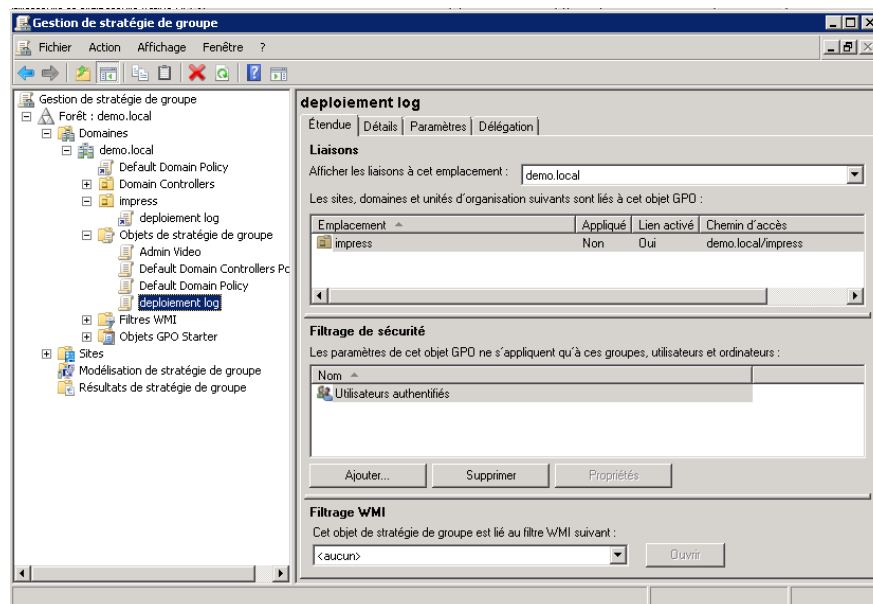
Une fois le point de distribution partagé, vous pouvez copier le ou les logiciels qui vous souhaitez distribuer à l'intérieur (dans notre exemple nous installerons la suite Microsoft Office). (N'oubliez pas que l'application doit être au format Windows Installer).

Ensuite allez dans **Outils d'administration** puis **Gestion des stratégies de groupe** ou tapez dans Exécuter : gpmc.msc Dans **Gestion des stratégies de groupe**, développez votre forêt puis votre domaine, et aller dans la gestion des stratégies de groupe.

Créer votre GPO par un clic droit puis **Nouveau**, nommer votre GPO et valider.

Une fois votre GPO créée, il peut être nécessaire de compléter le champ de filtrage de la GPO afin de limiter l'application de celle-ci. Ainsi, on peut limiter l'action à un utilisateur ou un groupe d'utilisateurs, ou à une machine ou un groupe de machines.

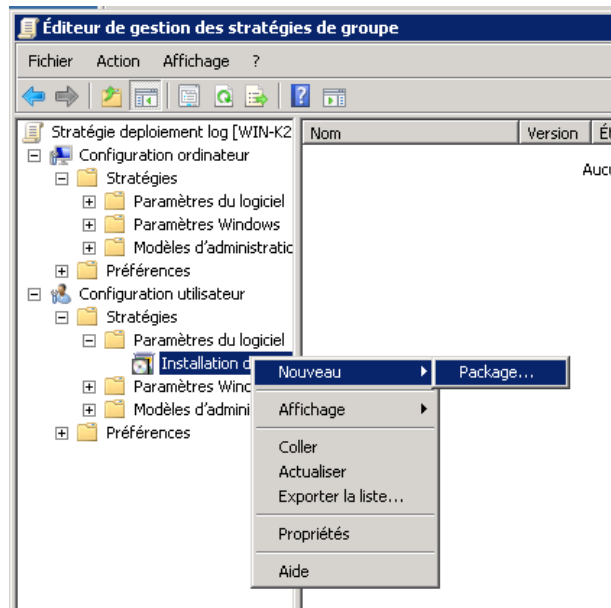
Vérifier dans les détails que la GPO est bien active.



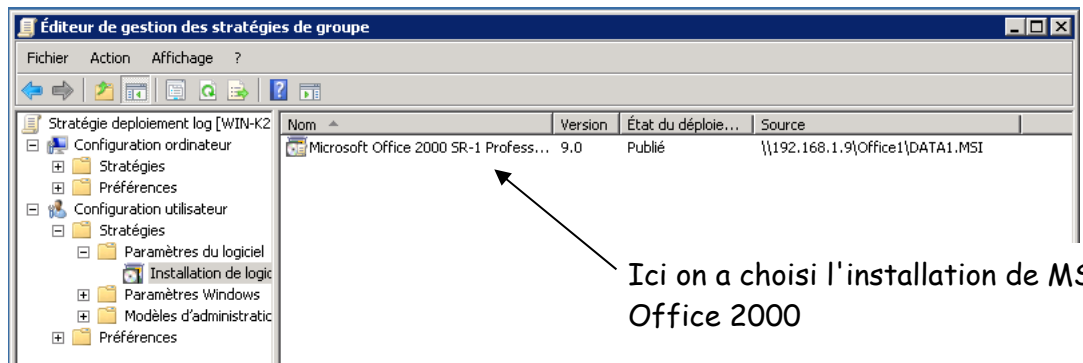
Lier la GPO au logiciel

Afin de pouvoir publier le logiciel vers tous les utilisateurs, nous devons lier la GPO créée précédemment au logiciel. Pour ce faire vous devez faire un clic droit sur la GPO et cliquez sur l'onglet **Modifier**.

Une nouvelle fenêtre s'ouvrira alors donnant accès à l'éditeur des stratégies de groupe. Sous l'onglet **Configuration utilisateur** développez **Paramètres du logiciel** puis cliquez sur **Installation de logiciel**. Faites un clic droit et faites **Nouveau** puis **Package**.

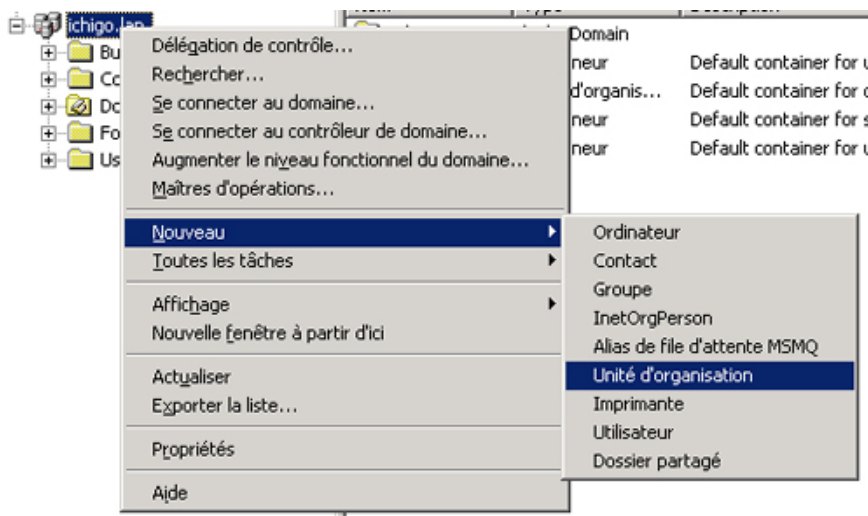


Vous aurez alors à rentrer le chemin menant au répertoire partagé *point de publication*, dans la fenêtre **Déploiement du logiciel**, qui s'affichera, choisir l'application cible et cliquez sur OK pour valider. Dans la fenêtre suivant valider l'attribution du déploiement (pour le rendre automatique à la prochaine ouverture de fichier).



Création de l'unité d'organisation

Allez dans l'outil d'administration **Utilisateurs et ordinateurs Active Directory**. Faites un clic droit sur le nom de votre domaine, puis sélectionnez **Nouveau** puis **Unité d'organisation**.



Donnez un nom à cette nouvelle unité organisationnelle (par exemple déploiement logiciel) et fermez la fenêtre.

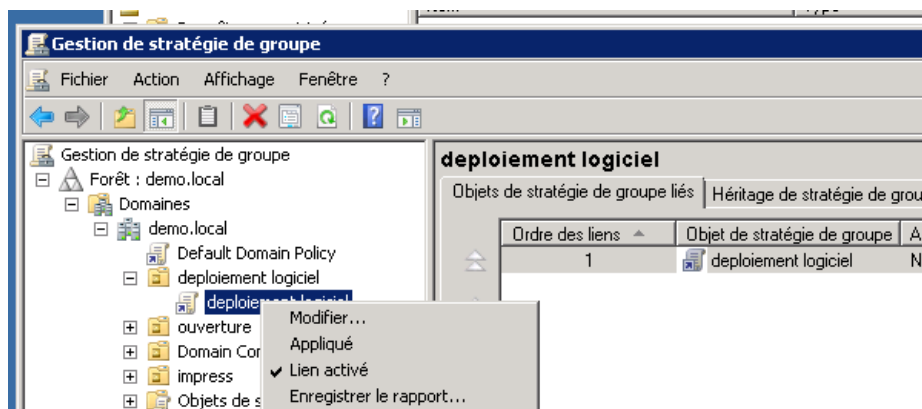
Lier la GPO à l'unité organisationnelle

Allez dans **Gestion des Stratégies de Groupe**, faites un clic droit sur l'UO que vous venez de créer et cliquez sur **Lier un objet de stratégie de groupe existant**, puis dans la fenêtre choisir le domaine puis la GPO que nous venons de créer.



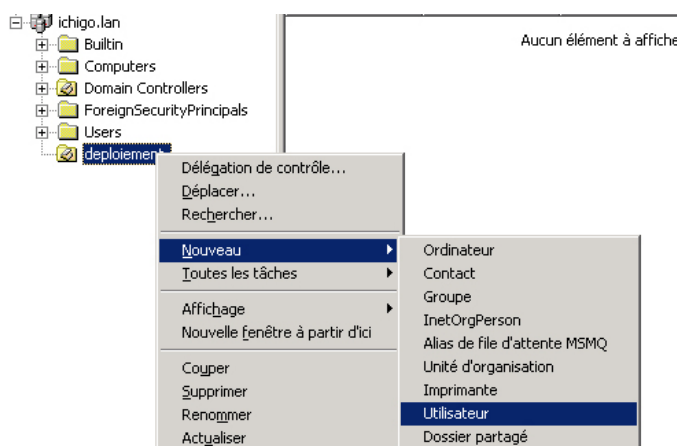
Une fois la GPO associée à l'UO, elle apparaît dans l'arborescence du gestionnaire de stratégie de groupe.

Vérifier par un clic droit que la stratégie est toujours active.



Création d'un utilisateur type

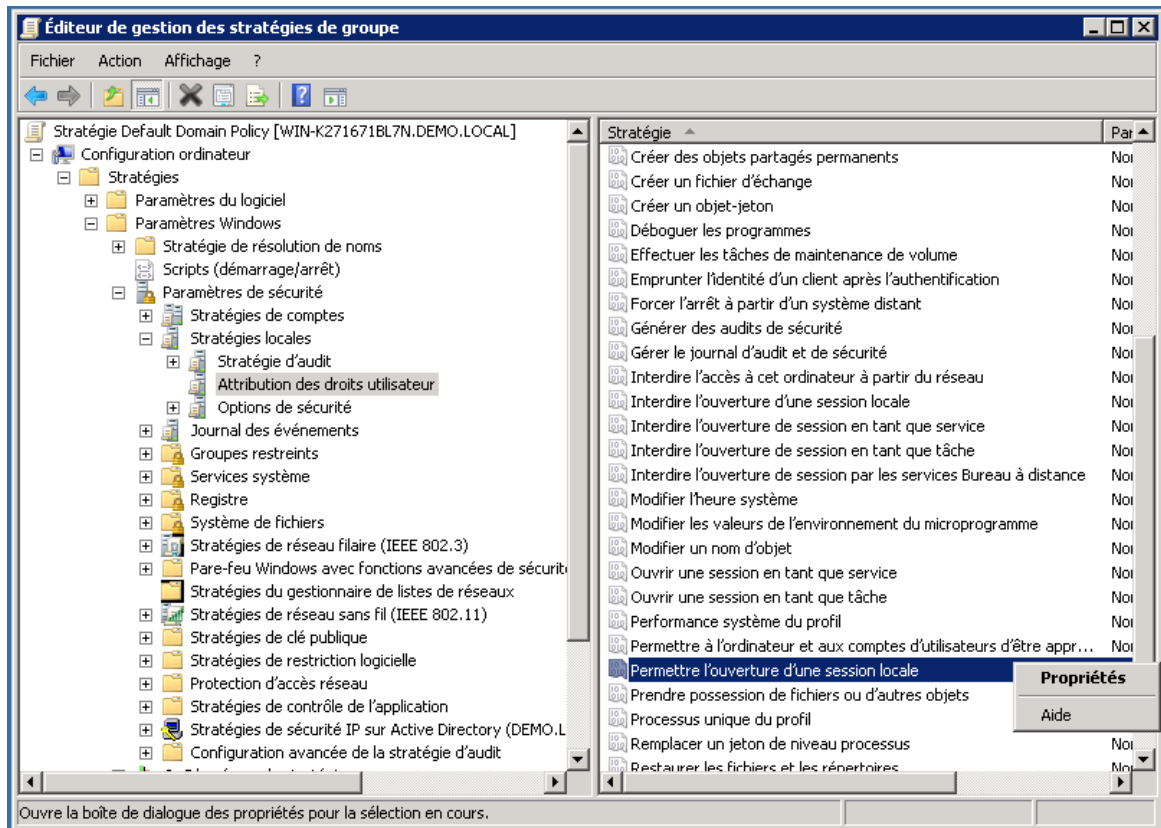
Allez dans **Utilisateurs et Ordinateurs Active Directory**. Cliquez avec le bouton droit sur le domaine puis sur votre unité d'organisation puis **Nouveau** et **Utilisateur**.



Entrez les coordonnées de votre utilisateur ainsi que les paramètres de son mot de passe puis validez.

Il faut maintenant lui donner les droits en fonction de ses droits, en particulier pour faire l'installation et l'inscription locale sur le client de l'application. Aller dans **Gestion des Stratégie de Groupe**. Puis naviguez dans **Forêt** puis **Domaines**. Choisir votre domaine puis **Objets de stratégie de groupe**, et faire un clic droit sur **default Domain policy** et **Modifier**.

Une nouvelle fenêtre de gestion s'ouvre. Aller dans **Configuration ordinateur**, **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité**, **Stratégies locales**, **Attribution des droits utilisateur**. Vous verrez alors dans la fenêtre de droite l'option **Permettre l'ouverture d'une session locale**, modifiez la pour rajouter l'utilisateur que vous venez de créer.



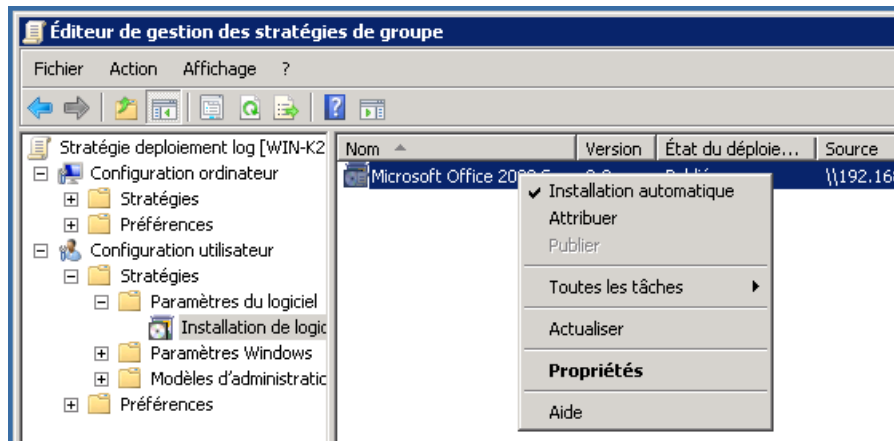
Fermez ensuite toute les fenêtres et allez dans Exécuter et tapez **gpupdate /force** pour mettre à jour le système.

4. Mise service

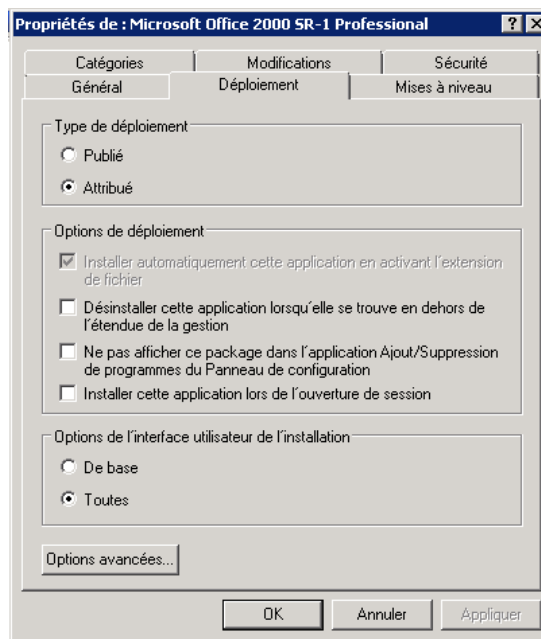
Maintenant, lors d'une ouverture de session sur un poste en utilisant l'utilisateur déclaré, la GPO va installer les lancements d'installation d'Office dan le **menu démarrer**.

Le paramétrage permet d'installer uniquement les lanceurs d'installation. Aussi, l'installation de Word ou Excel ne sera effective que si l'utilisateur cherche à exécuter ces applications, ou s'il cherche à ouvrir un fichier doc, xls, ou compatible.

Il est possible d'effectuer l'installation complète à l'ouverture de session. Pour cela, retourner dans le gestionnaire de stratégies de groupe. Modifier la stratégie pour ouvrir la fenêtre de paramétrage. Aller sur le fichier de déploiement et modifier ses propriétés.



Il est possible d'effectuer l'installation complète à l'ouverture de session. Pour cela, retourner dans le gestionnaire de stratégies de groupe. Modifier la stratégie pour ouvrir la fenêtre de paramétrage. Aller sur le fichier de déploiement et modifier ses propriétés.



Dans l'onglet de déploiement, le type doit être à attribué, ce qui permet de cocher la case d'installation à l'ouverture de session. Attention, un tel déploiement est long, donc réservé à un administrateur du domaine, ou un utilisateur prévenu et compétent.

Stratégie de groupe pour gestion d'impression

1. Introduction

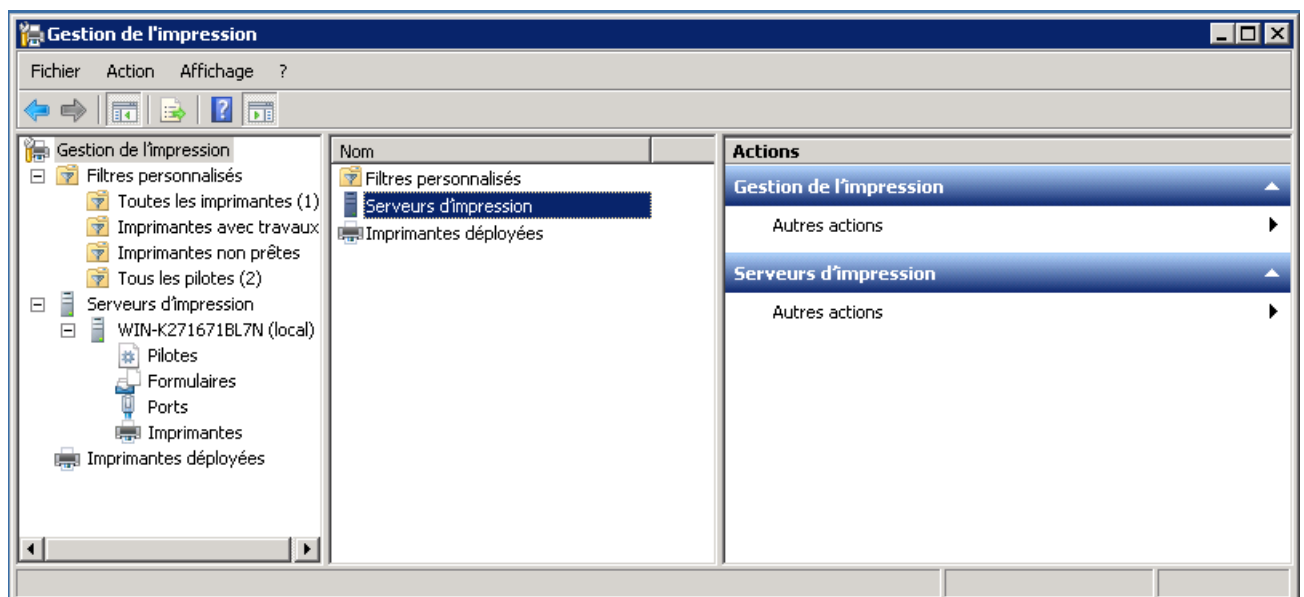
Il s'agit d'une fonctionnalité très utile de Microsoft Active Directory. La gestion de l'impression permet à l'administrateur d'impression d'économiser une quantité de temps significative à installer des imprimantes sur les ordinateurs clients et à gérer et surveiller les imprimantes. Les tâches qui peuvent requérir jusqu'à 10 étapes sur des ordinateurs individuels peuvent, grâce à une stratégie de groupe, être accomplies en 2 ou 3 étapes sur plusieurs ordinateurs simultanément et à distance.

Avant toute chose, il n'est pas nécessaire que le serveur recevant l'Active Directory soit serveur d'impression pour effectuer la gestion de l'impression. Il y a bien séparation du rôle **serveur d'impression**, de la fonctionnalité **Outils de service d'impression**.

2. Installation de l'outil

La première étape, consiste à installer l'outil de gestion. Cet outil s'installe en même temps que le rôle. Lancer le gestionnaire de serveur, et ajouter un rôle **Service de documents et d'impression**.

Une fois l'installation terminée, lancer l'outils : **Démarrer, Outils d'administration, Gestion de l'impression**.



3. Utilisation de l'outil

Pour ajouter des serveurs d'impression à la gestion de l'impression

1. Ouvrez le dossier Outils d'administration, puis double-cliquez sur **Gestion de l'impression**.
2. Dans l'arborescence Gestion de l'impression, cliquez avec le bouton droit sur **Gestion de l'impression**, puis cliquez sur **Ajouter/Supprimer des serveurs**.
3. Dans la boîte de dialogue **Ajouter/Supprimer des serveurs**, sous Spécifier le **serveur d'impression**, dans **Ajouter un serveur**, effectuez l'une des actions suivantes :
 - Tapez le nom.
 - Cliquez sur **Parcourir** pour localiser et sélectionner le serveur d'impression.
4. Cliquez sur **Ajouter à la liste**.
5. Ajoutez autant de serveurs d'impression que vous le souhaitez, puis cliquez sur **OK**.

Pour supprimer des serveurs d'impression dans le composant Gestion de l'impression

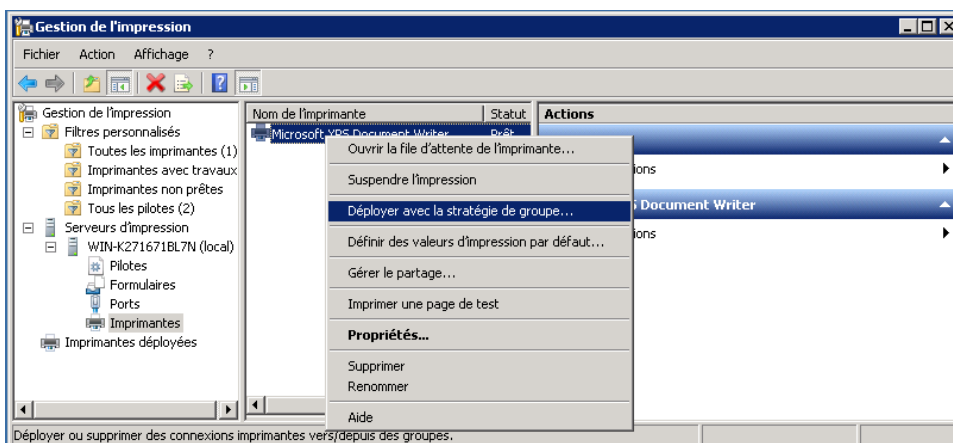
1. Ouvrez le dossier Outils d'administration, puis double-cliquez sur **Gestion de l'impression**.
2. Dans l'arborescence Gestion de l'impression, cliquez avec le bouton droit sur **Gestion de l'impression**, puis cliquez sur **Ajouter/Supprimer des serveurs**.
3. Dans la boîte de dialogue **Ajouter/Supprimer des serveurs**, sous **Serveurs d'impression**, sélectionnez un ou plusieurs serveurs, puis cliquez sur **Supprimer**.

Pour ajouter automatiquement des imprimantes réseau à un serveur d'impression

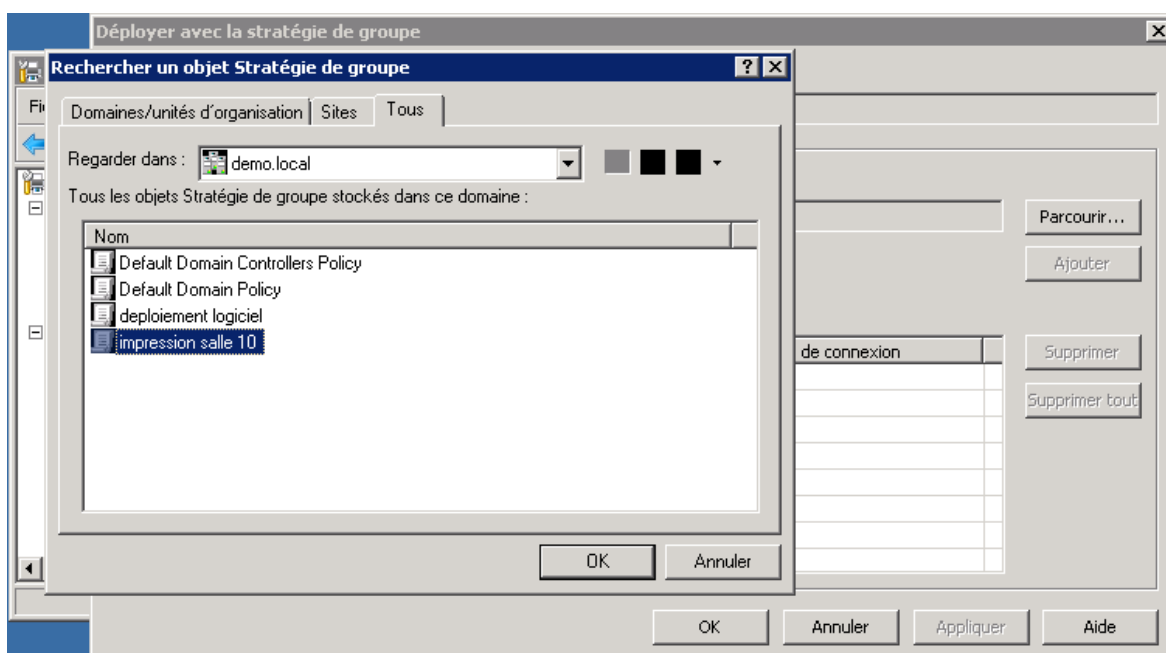
1. Ouvrez le dossier Outils d'administration, puis double-cliquez sur **Gestion de l'impression**.
2. Dans l'arborescence Gestion de l'impression, cliquez avec le bouton droit sur le serveur approprié, puis cliquez sur **Ajouter une imprimante**.
3. Dans la page Installation de l'imprimante de l'**Assistant Installation d'imprimante réseau**, cliquez sur **Rechercher les imprimantes du réseau**, puis sur **Suivant**. Si vous y êtes invité, spécifiez le pilote à installer pour l'imprimante.

Pour déployer des imprimantes pour des utilisateurs ou des ordinateurs à l'aide d'une stratégie de groupe

1. Ouvrez le dossier Outils d'administration, puis double-cliquez sur **Gestion de l'impression**.
2. Dans le volet gauche, cliquez sur **Serveurs d'impression**, puis sur le serveur d'impression applicable et sur **Imprimantes**.
3. Dans le volet central, cliquez avec le bouton droit sur l'imprimante applicable, puis cliquez sur **Déployer avec la stratégie de groupe**.

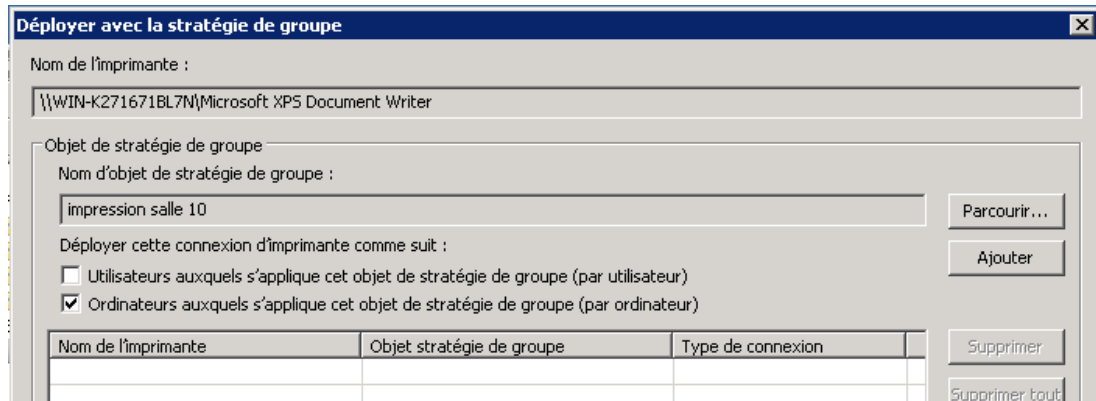


4. Dans la boîte de dialogue **Déployer avec la stratégie de groupe**, cliquez sur **Parcourir**, puis sélectionnez ou créez un nouvel objet GPO pour stocker les connexions aux imprimantes. Cliquez sur **OK**.



5. Spécifiez s'il convient de déployer les connexions aux imprimantes pour des utilisateurs ou des ordinateurs :
 - Pour un déploiement auprès de groupes d'ordinateurs, afin que tous les utilisateurs des ordinateurs puissent accéder aux imprimantes, activez la case à cocher **Ordinateurs auxquels s'applique cet objet de stratégie de groupe (par ordinateur)**.
 - Pour un déploiement pour des groupes d'utilisateurs, afin que les utilisateurs puissent accéder aux imprimantes à partir de tout ordinateur sur lequel ils ouvrent

une session, activez la case à cocher **Utilisateurs auxquels s'applique cet objet de stratégie de groupe (par utilisateur)**.



Cliquez sur **Ajouter**.



- Répétez les étapes 3 à 6 pour ajouter le paramètre de connexion d'imprimante à un autre objet de stratégie de groupe, si nécessaire. Puis cliquez sur **OK** pour valider l'ensemble.