Leçon 8 : gestion des GPO

Dans cette leçon, nous allons aborder la **délégation de la gestion** des ordinateurs à d'autres utilisateurs prenant le rôle d'administrateur. Nous aborderons également le déploiement d'un logiciel sur l'ensemble du domaine et, finalement, les options d'audit.

Cette leçon suit le livre de référence suivant :

[70-742] *A. Warren,* Exam Ref 70-742 : Identity with Windows® Server® 2016, 1st edition, Microsoft Press, March 2017

8.1 Déléguer la gestion

Il y a plusieurs manières de déléguer des tâches sur des réseaux Microsoft. Ainsi, on peut *déléguer l'administration de certaines machines* à des utilisateurs particuliers (qui sont alors administrateurs de ces machines). On peut également déléguer *la gestion de tâches d'administration* comme la gestion des utilisateurs, par exemple, à un ou plusieurs utilisateurs.

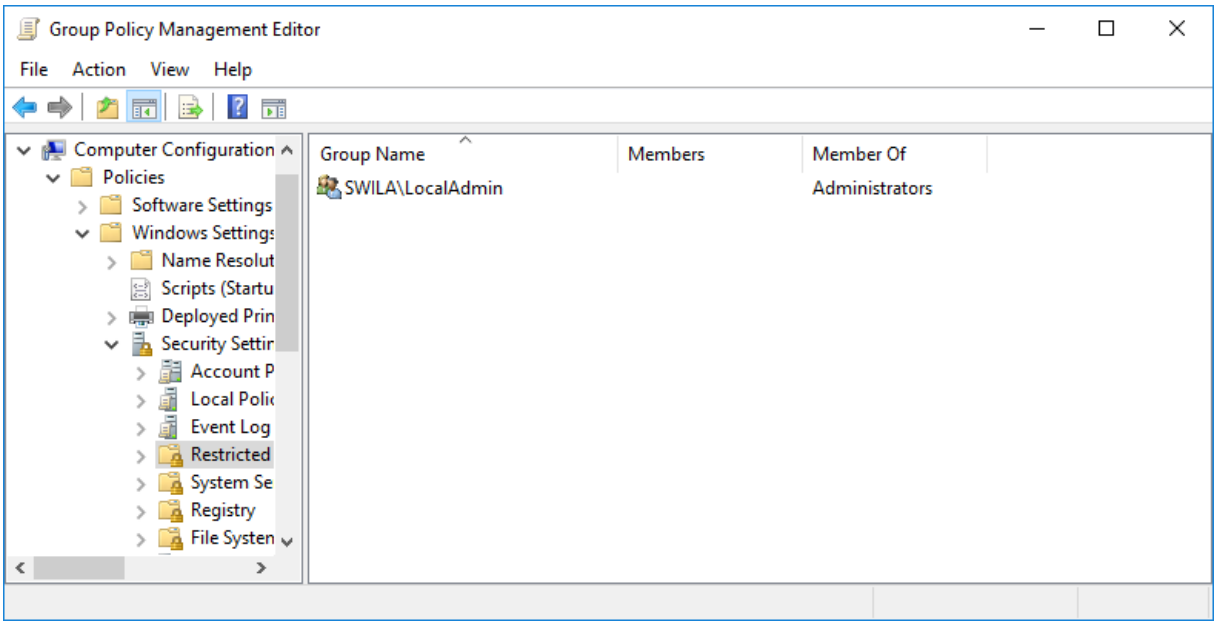
8.1.1 Déléguer l'administration de machines

Il est parfois nécessaire de pouvoir *déléguer* l'administration d'un groupe de machines à des utilisateurs différents de l'administrateur. Pour rappel, sur les machines, il y a un groupe *local* `Administrators`. Les membres de ce groupe sont des administrateurs *locaux* et peuvent réaliser des tâches d'administration telles que : installation de pilotes, ajout et configuration d'imprimantes, configuration réseau …. Ainsi *déléguer* l'administration des machines revient à donner des droits d'administrateur sur ces machines.

Si nous définissons un groupe de sécurité *LocalAdmin* sur le domaine, il est possible d'ajouter ce groupe au groupe local *Administrators* sur *chaque machine*. Cette opération peut vite se révéler très contraignante, dans ce cas, nous pouvons ajouter cette appartenance sur toutes les machines concernées directement au moyen d'une GPO.

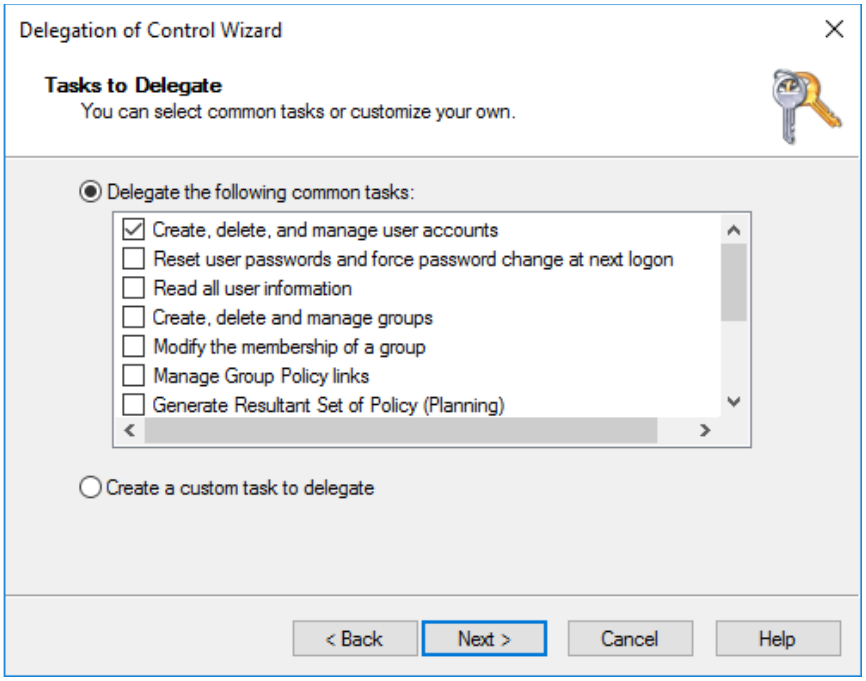
Cet élément de configuration est **une GPO Ordinateur** (ie. *Computer Configuration*). Il faut modifier l'option *Restricted Groups* qui se trouve dans `Computer Configuration\Policies\Windows Settings\Security Settings`. Ensuite, il faut, par un *clic-droit*, choisir **Add Group** et mentionner, par exemple *SWILA\LocalAdmin* et mentionner que **ce groupe est membre de** (option *This group is member of*, en bas) *Administrators*. Une fois cette manipulation terminée, tous les ordinateurs sur lesquels cette GPO s'applique verront leur groupe local Administrators modifié avec *SWILA\LocalAdmin* comme membre.

Tous les membres du groupe de sécurité *LocalAdmin* sont désormais *Administrateurs locaux* des ordinateurs appliquant cette GPO.

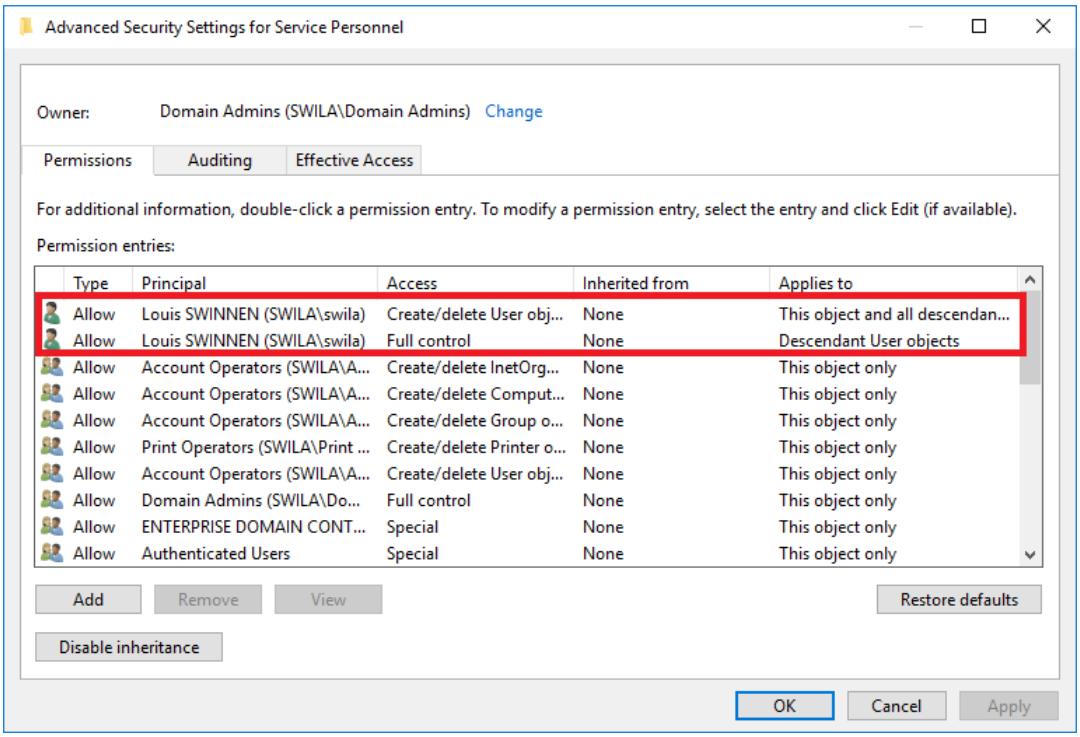


8.1.2 Déléguer des tâches d'administration AD

Il est possible de déléguer la gestion de certaines parties d'Active Directory à des utilisateurs qui ne sont pas des administrateurs. Nous avons déjà vu qu'il est possible de déléguer, à des utilisateurs, la gestion d'une GPO liée à une unité d'organisation.



Nous pouvons également déléguer la possibilité de créer des objets dans une branche d'Active Directory au moyen de la **Délégation de contrôle** (*clic-droit sur l'élément, **Delegate Control***). Il est ainsi possible de préciser les actions qui sont déléguées à l'utilisateur ou au groupe d'utilisateurs renseigné. Une fois la délégation de contrôle effectuée, il est possible de visualiser / modifier / supprimer les autorisations via les *Advanced Security Settings* (clic-droit **Properties** puis **Security** puis **Advanced**).



Une fois la délégation terminée, l'utilisateur peut accéder aux éléments d'Active Directory par les outils d'administration ou via une console MMC spécifique pour gérer sa branche.

8.2 Installation et déploiement de logiciels

Il est possible de procéder à l'installation et au déploiement de logiciels via une GPO. Cette possibilité peut être intéressante si de nombreuses machines sont mises à disposition des utilisateurs et que ces derniers doivent pouvoir utiliser un *pack* de logiciels identiques quel que soit la machine sur laquelle ils se connectent.

Cette possibilité d'installation se base sur le service *Windows Installer*. Il est donc important de savoir que **seuls les logiciels utilisant ce service d'installation peuvent être déployés via une GPO**. Pour être plus précis, il est nécessaire de disposer du logiciel à installer sous la forme d'un fichier `.msi`. Si le logiciel n'est pas disponible sous le format MSI, le déploiement au travers d'une GPO ne sera pas possible.

Il existe bon nombre de systèmes de déploiement de logiciels à travers des réseaux, mais ceux-ci sont des applications supplémentaires et payantes à ajouter aux serveurs et postes clients. Il est important de remarquer que si le nombre de postes de travail de l'entreprise est élevé, ces outils de gestion et maintien de la configuration sont indispensables. Dans des environnements plus réduit, l'outil de déploiement à travers une GPO peut suffire.

8.2.1 Configuration Ordinateur ou Configuration Utilisateur

Le déploiement de logiciel est présent à la fois dans la partie **Computer Configuration** et **User Configuration**. A l'instar de l'option d'exécution des scripts, il y a une différence entre configurer un déploiement au niveau utilisateur et au niveau ordinateur.

En effet, en mode *Computer Configuration*, le déploiement est d'office en mode *Assigned* alors qu'en mode *User Configuration*, les modes de déploiement possibles sont *Assigned* ou *Published*. Nous allons expliquer ces deux modes dans la suite :

- **Pour une configuration utilisateur (*user configuration*),**
  - Le déploiement en mode « *published* » permet d'installer l'application via le *Control Panel* > *Programs and Features* et puis en choisissant *Install a program from the network*. Il faut donc que l'utilisateur **choisisse** d'installer l'application pour que celle-ci soit présente. Cette option d'installation est disponible sur *toutes les machines* sur lesquelles l'utilisateur se connecte.
  - Le déploiement en mode « *assigned* » montre l'application *comme si* elle était déjà installée (icône sur le bureau, groupe dans le menu démarrer). Lorsque l'utilisateur clique sur le programme, il est installé (si ce n'était pas déjà fait) puis est utilisé. L'application est donc ici installée en fonction des besoins.
- **Pour une configuration ordinateur *(computer configuration)***,
  - Le déploiement en mode « *assigned* » permet d'installer le package durant le démarrage de la machine. Cette application est donc installée de manière silencieuse avant de permettre la connexion d'un utilisateur sur le système. Cette option peut être très intéressante pour déployer un nouveau programme rapidement sur l'ensemble d'un parc de machines.

Lorsqu'on supprime la GPO de déploiement du logiciel, le système vous demande de décider s'il faut laisser l'application installée (pour les utilisateurs et/ou machines sur lesquelles elle est déjà déployée) ou supprimer l'application.

Le mode **Advanced** permet de spécifier des options particulières. Ainsi, il est possible d'ajouter, via l'onglet **Modifications**, des fichiers MST qui sont *des modifications à l'installation de base* ou encore des fichiers MSP *qui sont des correctifs (Patch)*.

8.2.2 Distribution par le réseau

Il est important que les applications mises à disposition soient disponibles depuis le réseau. Il est donc important de **configurer un partage** pour distribuer et gérer le déploiement des applications. L'autorisation de *Lecture* est nécessaire sur le partage alors que l'autorisation NTFS de *lecture et exécution* est nécessaire sur le fichier à déployer.

Ainsi le chemin vers le package d'installation doit toujours être un chemin réseau de la forme `\\SERVER\Partage\Package.msi`.

8.2.3 Configurer la GPO de déploiement

1. Décider le mode de déploiement (User ou Computer – Assigned ou Published).
2. Placer le fichier d'installation MSI dans un dossier partagé accessible.
3. Créer une nouvelle GPO de déploiement. Il faut procéder comme suit,
   a. dans le cas d'une GPO computer :

i. `Computer Configuration \Policies\Software Settings\ Software Installation` puis choisir **New** puis **Package**.
ii. Choisir le MSI d'installation
iii. Sélectionner le type de déploiement (*assigned* ou *advanced*). Le mode *advanced* permet de préciser de nombreuses options.
iv. Appuyer sur **OK**
v. Lier cette stratégie à **une unité d'organisation** contenant des objets **ordinateurs**

b. Dans le cas d'une GPO user :
i. `User Configuration \Policies\Software Settings\Software installation` puis choisir **New** puis **package**
ii. Choisir le MSI d'installation
iii. Sélectionner le type de déploiement (*published, assigned* ou *advanced*). Le mode *advanced* permet de préciser de nombreuses options.
iv. Appuyer sur **OK**
v. Lier cette stratégie à **une unité d'organisation** contenant des objets **utilisateurs**.

Le déploiement par poste de travail (par ordinateur) semble plus naturel. Cependant, en fonction des contrats de licence négociés, l'installation par utilisateur peut être une option intéressante.

8.2.4 Maintenance

Une fois l'installation déployée sur un ordinateur, ce dernier n'essaiera plus d'installer le logiciel, et ce même si le package logiciel change. Ainsi, si une mise à jour est nécessaire, il est nécessaire de modifier la GPO pour que celle-ci provoque une modification de l'installation effectuée.

De plus, lorsqu'un problème survient, il est parfois nécessaire d'effectuer un redéploiement, par l'option « *redeploy application* ». Les options de maintenance sont disponibles dans la GPO.

Pour **mettre à jour** un package logiciel, il faut soit créer une nouvelle GPO et ajouter la nouvelle version du package, soit modifier la GPO déjà créée en ajoutant le nouveau package. Il convient de choisir le mode de déploiement **Advanced** (ou alors de reprendre l'option au moyen d'un clic-droit **Properties**) et, dans l'onglet **Upgrades**, choisir le package logiciel qui est mis à niveau. Lors de la configuration, il est possible de spécifier si l'ancienne version doit être désinstallée au préalable ou non.

Pour provoquer un **redéploiement d'une application**, il faut se rendre dans la GPO contenant le package à déployer et, via un **clic-droit** sur ce package, choisir l'option **All Tasks** puis **Redeploy application**.

Pour **supprimer une application déployée**, il suffit de supprimer le package dans la GPO déployant ce logiciel (**clic-droit** puis **All tasks** puis **Remove**). A ce moment, le système vous demande s'il faut supprimer les packages qui ont été installés sur les machines ou si l'on peut permettre aux utilisateurs de continuer à utiliser le logiciel, tout en empêchant de nouvelles installations.

8.3 Stratégies d'audit

Les audits permettent de consigner dans les journaux systèmes des événements déterminés. Cela permet de *tracer* les actions des utilisateurs sur le réseau. La capacité d'audit est assez importante

puisqu'il est possible de consigner aussi bien les tentatives *réussies* que les tentatives *ratées* (connexion par exemple).

Il est également possible de consigner l'accès aux différentes ressources (accès à un partage par exemple) dans les journaux d'audit.

Il faut être vigilant : il est possible d'activer les audits sur beaucoup d'éléments du système. **Vouloir tout auditer ne mène à rien** étant donné la masse considérable d'information que cela représente. Ainsi vouloir auditer trop d'élément conduit à remplir les journaux d'audit et les rendre illisible car l'information vraiment intéressante est perdue parmi l'ensemble.

De plus, organiser la surveillance des différents éléments par le système et écrire dans les fichiers journaux est une **opération qui a un coût** (négligeable si cette opération n'est faite qu'aux moments intéressant mais élevé si cette opération survient fréquemment).

Il convient donc de garder une bonne gestion en auditant les éléments qui semblent important, en limitant un audit élevé dans le temps (pour trouver une anomalie par exemple), …

Il faut tenir compte que les contrôleurs de domaine sont configurés pour auditer un certain nombre d'éléments : *la création réussie d'un utilisateur, la réinitialisation réussie d'un mot de passe, la connexion réussie au domaine, la récupération réussie du script d'ouverture de session*. Il est souvent intéressant d'ajouter des audits *d'échec* permettant de consigner les événements (i.e. tentatives) qui n'ont pas aboutis.

8.3.1 Modifier la stratégie d'audit

Il est possible de créer une stratégie d'audit en ajoutant une GPO et en activant un paramètre dans `Computer Configuration \Policies\Windows Settings\Security Settings\Lacal Policy\Audit Policy`. Depuis Windows Server 2008 R2, il y a également la possibilité d'utiliser une stratégie d'audit avancée dont les paramètres sont disponibles ici : `Computer Configuration \Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration`.

8.3.2 Accès aux objets et audit

Il est également possible d'auditer l'accès aux objets (dans Active Directory ou sur le système de fichiers comme un dossier ou à un fichier). Cette option d'audit se trouve dans les paramètres de sécurité associés à l'objet (*advanced security settings* de l'unité d'organisation, d'un fichier ou d'un dossier). Pour y accéder, il faut faire un **clic-droit** sur l'objet concerné **Properties**, choisir l'onglet **Security** puis **Advanced** et enfin aller dans l'onglet **Auditing**. Il est possible d'auditer *la réussite* (***Success***) ou l'*échec* (***fail***) à un certain nombre d'accès. L'audit peut être restreint à un utilisateur ou groupe donné.

Dès qu'un audit sur un objet est réalisé, il faut également **activer des stratégies** particulières nommées : *Audit object access* (fichiers ou dossiers) et *Audit directory service access* (éléments dans Active Directory) dans la GPO. Sans cette activation, les modifications réalisées au niveau de l'audit de l'objet seront sans effet.

8.3.3 Visualiser les audits

Une fois la stratégie d'audit installée, il est possible d'en observer les résultats en consultant les journaux systèmes. En effet, dans l'outil **event viewer**, on trouve, dans les journaux *Windows Logs*, le journal *Security* reprenant tous les audits configurés.

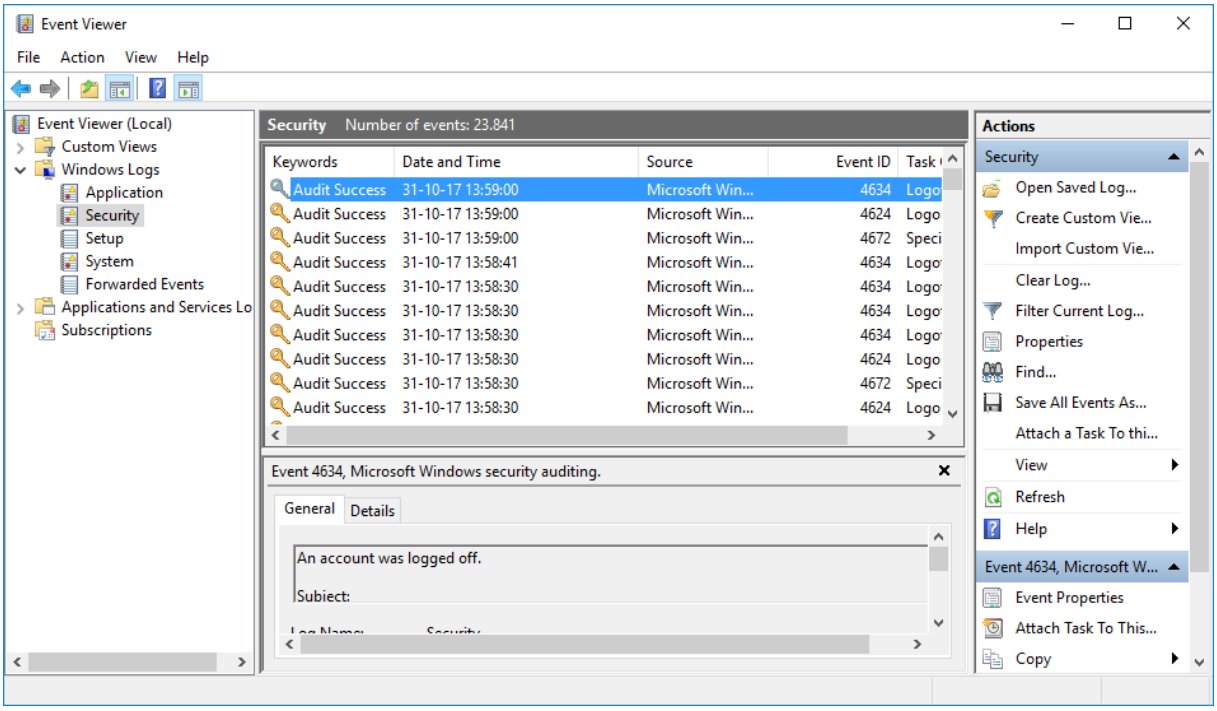


Figure 8.1 : Visualiser les audits

8.4 La boucle de rappel

Lors de la leçon précédente, nous avons abordé le concept de boucle de rappel. Cependant, il me semble important de revenir sur ce point étant donné la spécificité de celle-ci et l'importance de son utilisation dans le monde professionnel.

Pour rappel, une GPO contenant une *user configuration* doit être liée à des objets utilisateurs dans Active Directory alors qu'une GPO contenant une *computer configuration* doit être liée à des objets ordinateurs (une unité d'organisation par exemple). C'est assez logique puisque les stratégies s'appliquent à des objets différents et il est souvent bon de séparer, dans la structure d'Active Directory, les objets ordinateurs et utilisateurs.

8.4.1 L'exception boucle de rappel

L'activation de la boucle de rappel se fait sur des objets *ordinateurs*. Lorsque celle-ci est active et qu'un utilisateur se connecte, la GPO qui devrait être appliquée n'est plus celle dont il a hérité.

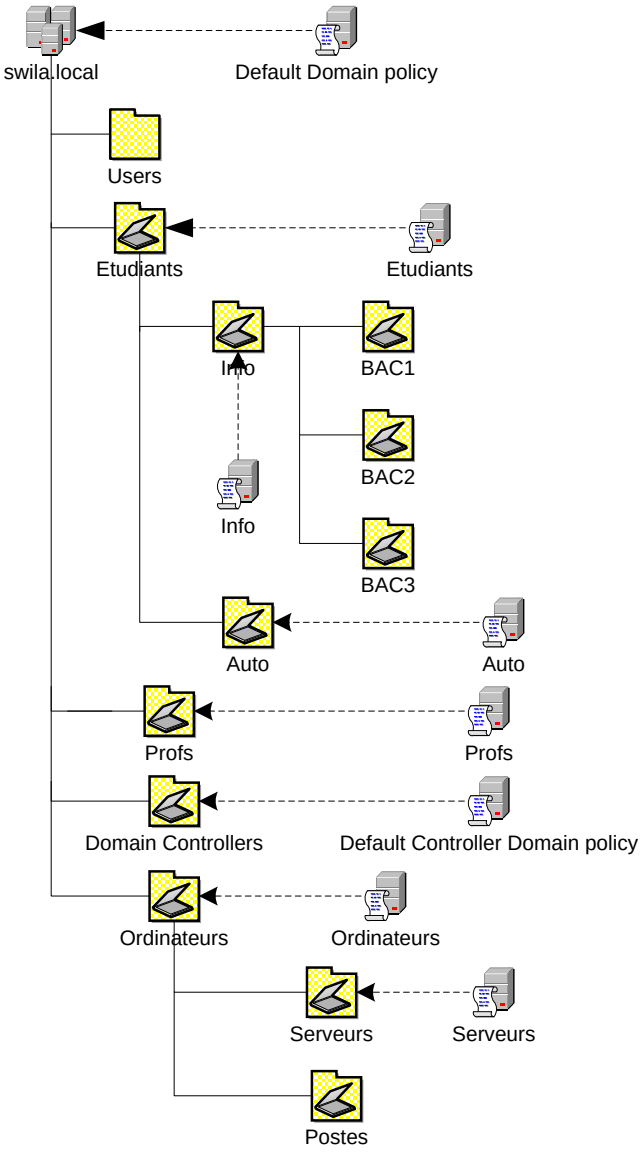


Figure 8.2 : Structure possible d'Active Directory

Sur la figure 8.2, si nous activons la boucle de rappel au niveau de stratégie *Serveurs* liée à l'unité d'organisation *Serveurs*, et qu'un utilisateur membre du groupe *Profs* par exemple se connecte sur une machine de cette unité, la stratégie qui lui sera appliquée sera modifiée.

En effet, la boucle de rappel supporte 2 modes de fonctionnement :

- Mode **merge** : la stratégie utilisateur va être modifiée en ajoutant les éléments contenus dans la configuration utilisateur de la boucle de rappel
- Mode **remplace** : la stratégie utilisateur va être supprimée et remplacée par les éléments contenus dans la configuration utilisateur de la boucle de rappel.

Ainsi, dans notre exemple, si nous activons, dans la GPO Serveurs la boucle de rappel et qu'un membre de l'unité d'organisation *Profs* se connecte, la stratégie utilisateur qui lui sera appliquée sera : GPO Profs + GPO Serveurs (mode *merge*) ou GPO Serveurs (mode *replace*).

Nous voyons donc ici apparaître une contradiction par rapport à ce que nous avions dit précédemment. En effet, la GPO définissant la boucle de rappel contient *à la fois* des éléments de configuration ordinateur et utilisateur bien que, *seuls des objets ordinateurs* soient présents dans l'unité d'organisation.

Ce mode de fonctionnement est particulièrement intéressant lorsqu'on dispose de *serveurs partagés* entre plusieurs utilisateurs : la stratégie appliquée sur celui-ci peut donc être complètement différente de celle appliquée à l'utilisateur lorsqu'il se connecte ailleurs, sur une autre machine.

8.4.2 Mise en place

Il faut commencer par activer la stratégie *Configure user Group Policy loopback processing mode* qui se trouve dans `Computer Configuration\Policies\Administrative Templates\System \Group Policy`. Il faut ensuite décider s'il faut *ajouter des nouvelles stratégies à l'utilisateur* (mode **merge**) ou s'il faut *supprimer toutes les stratégies utilisateurs existantes pour n'avoir que celles définies dans la boucle de rappel* (mode **remplace**).

Ensuite, il faut définir les stratégies utilisateurs à ajouter ou remplacer. Nous allons donc, dans cette stratégie, ajouter des éléments *User Configuration* bien que celle-ci s'applique sur des ordinateurs.

Une fois ces paramètres définis, notre GPO est terminée.

8.5 Exercices

1. Modifier la structure de votre Active Directory en créant les OU suivantes dans `CGComputers` : `Clients` et `Servers`. Déplacer l'objet ordinateur correspondant à la VM Windows 10 dans l'OU `Clients`.
2. Installer un nouveau serveur Windows Server 2016 (en suivant la procédure de la leçon 1). Spécifier les informations suivantes :
    a. Nom : `Srv2016-2`
    b. IP : `192.168.190.40`
    c. Ajouter cette machine à votre domaine, dans l'OU `Servers` (cf. étape 1).
3. Créer un groupe de sécurité `AdminMachines` et ajoutez-y le groupe `administratif`
4. Déléguer le contrôle de l'OU `personnel` aux membres du groupe `informatique`.
5. Créer les GPO suivantes nommées comme `indiqué` :
    a. `auditObjet` - GPO d'audit sur la création / suppression d'utilisateurs dans l'OU `personnel` (voir exercice 4)
    b. `outilsInstall` - GPO d'installation sur les ordinateurs contenus dans l'OU clients. On vous demande de déployer les programmes *firefox 32.0* et *putty 0.69*. Vérifiez que l'installation s'est déroulée correctement sur votre VM Windows 10.
    c. `auditEchecConnexion` - GPO d'audit sur tous les ordinateurs (`clients` et `servers`) du domaine consignant les échecs de connexion.
    d. `boucleRappel` - GPO appliquée sur l'OU Servers, activation du mode boucle de rappel (en mode *merge*), mais ne pas appliquer aux administrateurs. Imposer les restrictions suivantes :
        i. Start Menu : Supprimer l'entrée « Tous les programme », Supprimer l'horloge et supprimer l'option « Se Déconnecter »
        ii. Desktop : supprimer l'icône de la corbeille, ne pas enregistrer les modifications. Supprimer l'icône Ordinateur du bureau.
        iii. System : Désactiver le verrouillage de l'ordinateur, la modification du mot de passe et supprimer le gestionnaire des tâches
    e. `outilsInstall` - Modifier la GPO, pour faire la mise à jour du programme *firefox* vers la *version 52.4.1*. Vérifiez que la mise à jour s'est propagée correctement sur la VM Windows 10.
    f. `clientAdmin` - GPO pour déléguer l'administration des machines dans l'OU clients aux membres du groupe AdminMachines (créé à l'exercice 3)
6. Etablir un audit sur le partage `SharedSocial` créé précédemment (cf. leçon 7, exercice 3) pour consigner les ajouts et suppressions de fichiers ou dossiers par un membre du groupe social. Au besoin, vous modifierez la GPO `auditObject` créée à l'exercice 5.

GPO Exercice réel

Modification de l'exercice 5, section d.

Dans le but de protéger le 2ème serveur Windows 2016 déployé et qui sera, dans le futur, accessible en RDP, on vous demande de mettre en place les restrictions suivantes :

d) `boucleRappel` – GPO appliquée sur l'OU Servers, activation du mode blod de rappel (en mode *merge*), mais ne pas appliquer aux administrateurs. Imposer les restrictions suivantes :
   a. Bureau :
      i. Cacher l'icône Emplacements réseau sur le bureau
      ii. Cacher l'icône Internet Explorer sur le Bureau
      iii. Empêcher l'ajout, le glisser-deplacer et la fermeture des barres d'outils de la Barre des tâches
      iv. Empêcher l'utilisateur de rediriger manuellement des dossiers de profils
      v. Empêcher le redimensionnement des barres d'outils du Bureau
      vi. Ne pas enregistrer les paramètres en quittant
      vii. Supprimer le poste de travail du bureau
   b. Composants Windows / Console de gestion Microsoft / Composants logiciels enfichables restreints/autorisés
      i. Désactiver le gestionnaire de serveur
   c. Menu démarrer et barre des tâches
      i. Désactiver le nettoyage de la zone de notification
      ii. Effacer l'historique des documents récemment ouverts en quittant
      iii. Ne pas utiliser la méthode basée sur la recherche pour déterminer les raccourcis du bureau
      iv. Ne pas utiliser la méthode basée sur la recherche pour déterminer les raccourcis de l'environnement
      v. Supprimer et empêcher l'accès aux commandes Arrêter, Redémarrer, Mettre en veille et Mettre en veille prolongée
      vi. Supprimer l'icône de mise en réseau
      vii. Supprimer l'icône Sécurité et maintenance
      viii. Supprimer la liste « Récemment ajoutées » du menu Démarrer
      ix. Supprimer les liens et l'accès à Windows Update
      x. Supprimer les notifications et le centre de maintenance
      xi. Verrouiller la barre des tâches
   d. Panneau de configuration / Imprimantes
      i. Interdire la suppression des imprimantes
   e. Panneau de configuration / Personnalisation
      i. Empêcher de modifier l'arrière-plan du bureau
   f. Système
      i. Désactiver l'accès à l'invite de commandes
      ii. Empêcher l'accès aux outils de modifications du registre
      iii. Empêcher l'exécution d'applications spécifiques : powershell.exe et powershell_ise.exe

Ajout de l'exercice 7

7. En respect du RGPD, on vous demande d'ajouter une GPO `Disclaimer` affichant le texte ci-dessous lors de l'ouverture de session :
   a. Titre du message : « *Politique de confidentialité – Rappel* »
   b. Message : « *En tant qu'utilisateur/trice disposant des accès aux serveurs de l'entreprise dans le cadre de votre fonction au sein de l'organisation, vous êtes tenu.e à observer la plus grande confidentialité à l'égard des informations que vous êtes amené.e à traiter au nom de l'organisation et ne pas en faire un usage à d'autres fins. En cliquant sur "OK" et en poursuivant la connexion, vous reconnaissez avoir pris connaissance de cette information.* »