Windows Server 2012 R2 : sécurité

I Présentation

Tout utilisateur qui a accès a un ordinateur du domaine peut essayer de pirater le serveur. L'objectif de cette partie n'est pas de protéger l'accès au domaine de façon parfaite mais de vous donner quelques notions de base sur la sécurité.

Dans un premier temps, vous allez créer un nouveau compte pour l'administration car tout pirate qui a déjà le login a la moitié des informations pour la connexion. Il ne lui reste plus qu'à trouver le mot de passe. Cette protection est importante car l'administrateur a tous les droits sur le système.

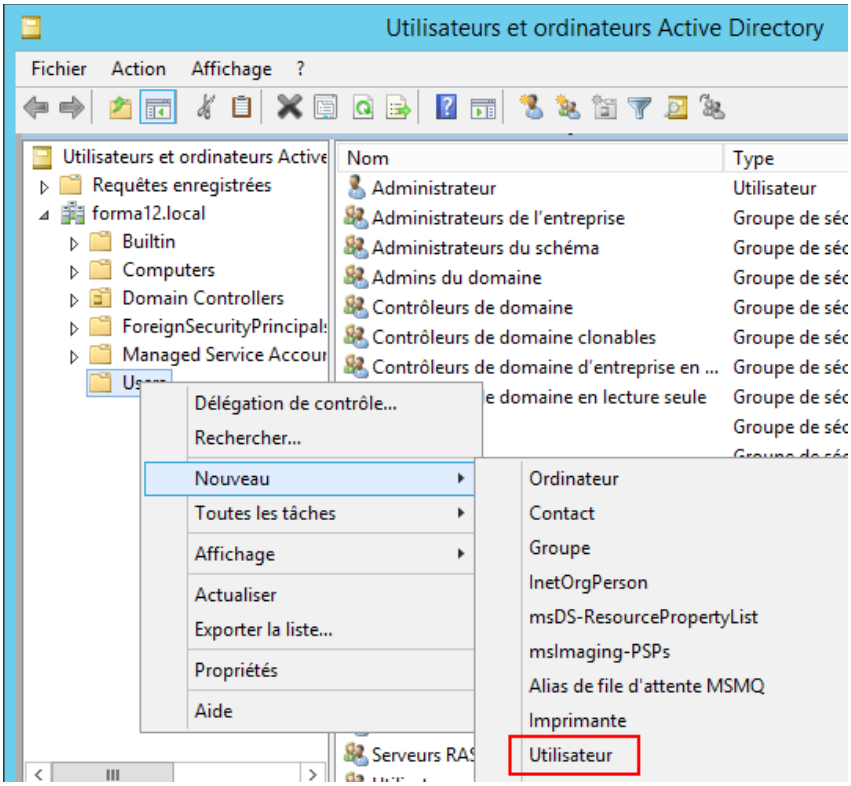
Ensuite pour éviter le piratage des autres comptes, il faut imposer un mot de passe pas trop simple. Typiquement, les gens ont tendance à utiliser le nom de leur femme, fils, chien, … De plus, à force de taper le même mot de passe, il est possible de déterminer le mot de passe de la personne (position des doigts sur le clavier) donc il faut forcer le changement régulier du mot de passe.

Si le pirate a beaucoup de temps, il pourra trouver le mot de passe donc l'administrateur doit être informé de toute tentative éventuelle (entrée incorrecte du mot de passe).

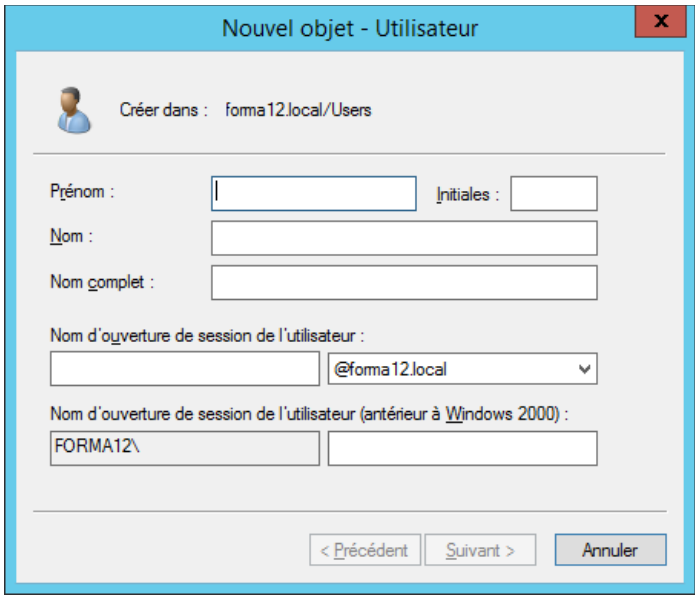
II Création d'un nouveau compte d'administration

Vous allez créer un nouveau compte dont le nom ne doit pas être proche de administrateur et surtout ne pas être le nom de l'administrateur. Prenons par exemple « AD$gest12 ». Il faut créer le compte grâce à un des outils d'administration : « Utilisateurs et ordinateurs Active Directory ».

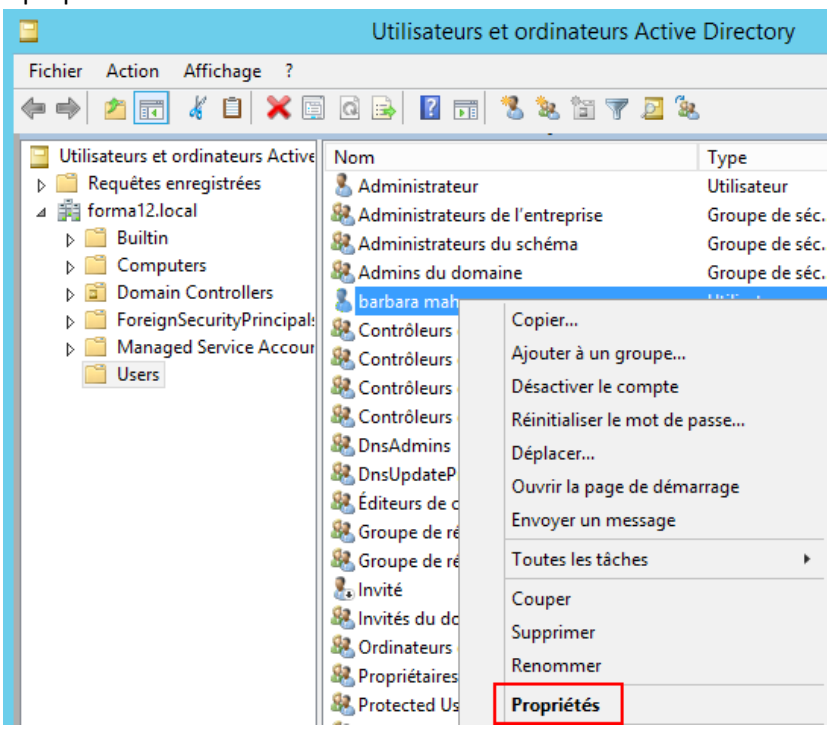
Il faut choisir « Users » dans la partie gauche puis faire un clic droit et choisir « Nouveau » - « Utilisateur » :



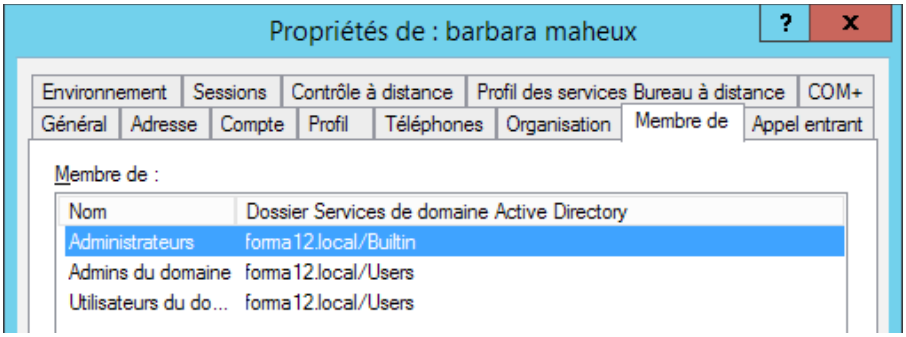
Ensuite il faut entrer les informations. Vous pouvez mettre le nom de l'administrateur mais le plus important est le nom d'ouverture.



L'utilisateur apparaîtra dans la liste sous son nom et non le nom d'ouverture (barbara maheux dans l'exemple ci-dessous). Il faut maintenant lui donner les droits d'administration. Pour cela, vous allez modifier ses propriétés :

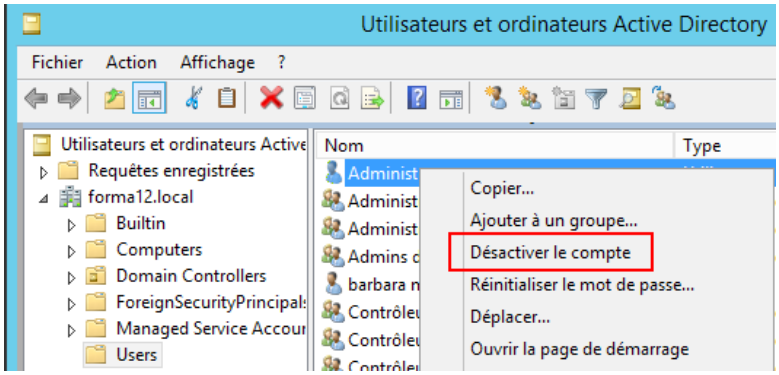


Il faut choisir l'onglet « Membre de » puis cliquer sur « Ajouter » pour le mettre dans les groupes « Admins du domaine » et « Administrateurs ».



Avant de désactiver l'utilisateur « Administrateur », il faut vérifier que vous pouvez vous connecter avec le compte que vous venez de créer et que vous avez bien les droits d'un administrateur.

Ensuite, vous pouvez effectivement désactiver le compte :

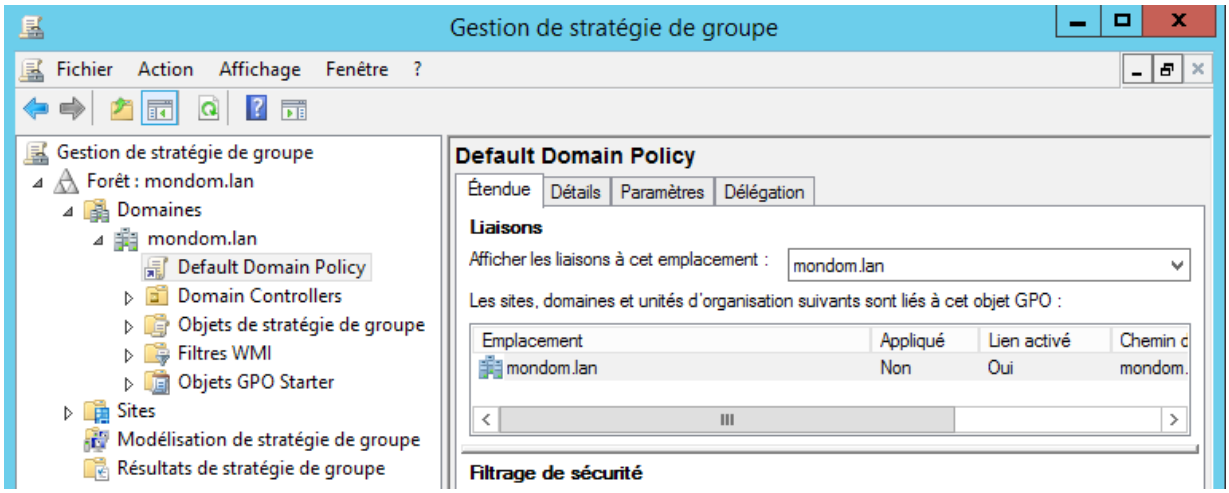


III Configuration des mots de passe

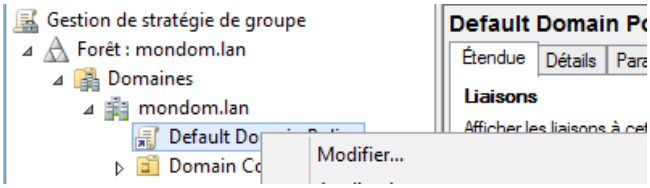
Il est possible de définir le « comportement » des comptes et de paramétrer les options :

- ✗ Durée maximale du mot de passe ;
- ✗ Durée minimale du mot de passe ;
- ✗ Longueur minimale du mot de passe ;
- ✗ Unicité du mot de passe : nombre de nouveaux mots de passe devant être utilisés avant qu'un ancien mot de passe puisse être réutilisé ;
- ✗ Verrouillage des comptes : nombre d'essais infructueux de mot de passe , durée entre deux essais et durée de verrouillage après le nombre d'essais maximum atteint ;
- ✗ Déconnecter de force : déconnexion automatique d'un utilisateur en dehors de ses plages horaires ;
- ✗ Les utilisateurs doivent ouvrir une session pour changer de mot de passe.

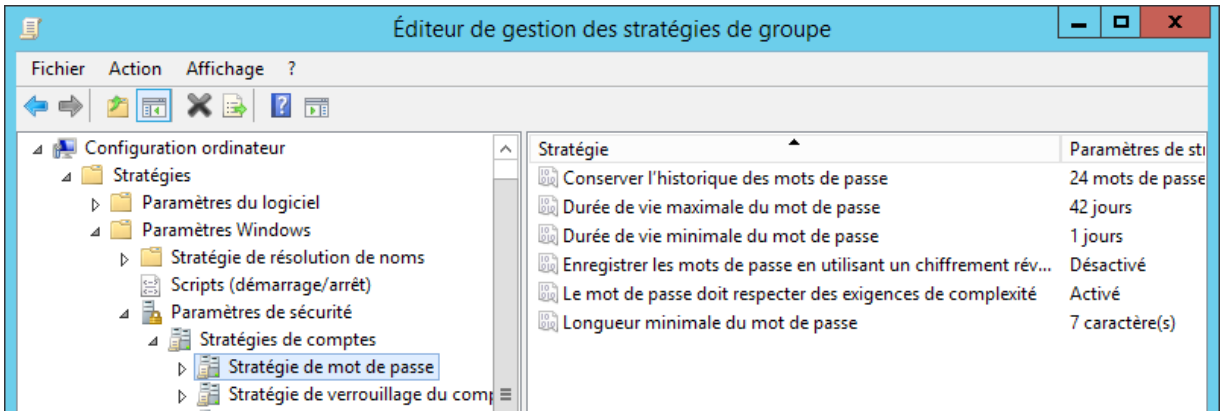
Pour configurer ce comportement, il faut ouvrir les outils d'administration et choisir « Gestion des stratégies de groupe » et déployer la partie droite de l'écran afin de voir le domaine créé :



Puis vous devez faire un clic droit sur « Default Domain Policy » et choisir Modifier :

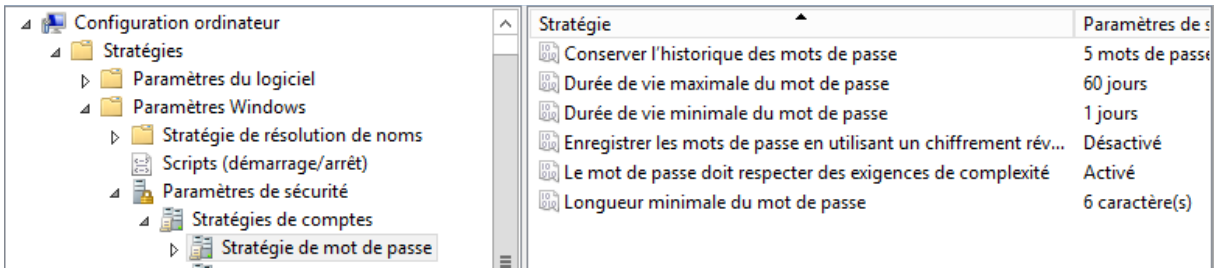


Il faut ensuite sélectionner « Stratégie de mot de passe » comme dans l'image ci-dessous :



Vous pouvez ensuite configurer le format des mots de passe en imposant les exigences de complexité (des caractères spéciaux et des chiffres doivent être mis dans le mot de passe) et le nombre minimum de caractères. Vous pouvez aussi définir la durée maximale d'un mot avant d'être obligé de le modifier et le nombre de mots de passe différents que vous pouvez utiliser avant de pouvoir utiliser à nouveau le même mot de passe.

Exemple de configuration possible :



Pour modifier les paramètres, il faut faire un clic droit dessus puis choisir « Propriétés ».

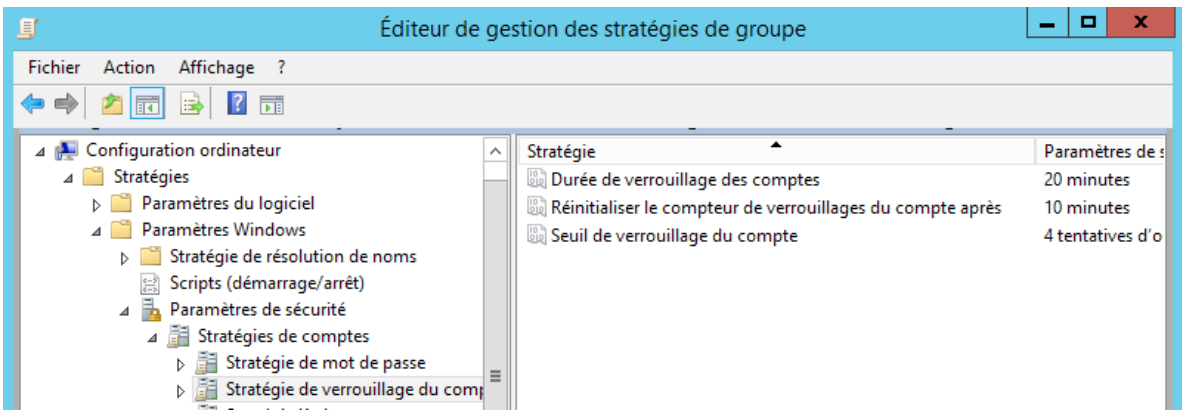
IV Protection des accès au domaine

IV.1 Configuration de comportement en cas d'essais infructueux

En cas d'échecs répétés du mot de passe lors de la connexion, on peut soupçonner l'utilisateur de vouloir pirater le compte. Donc il est judicieux d'être informé de ces erreurs de connexion afin de vérifier qu'aucun piratage n'est en cours.

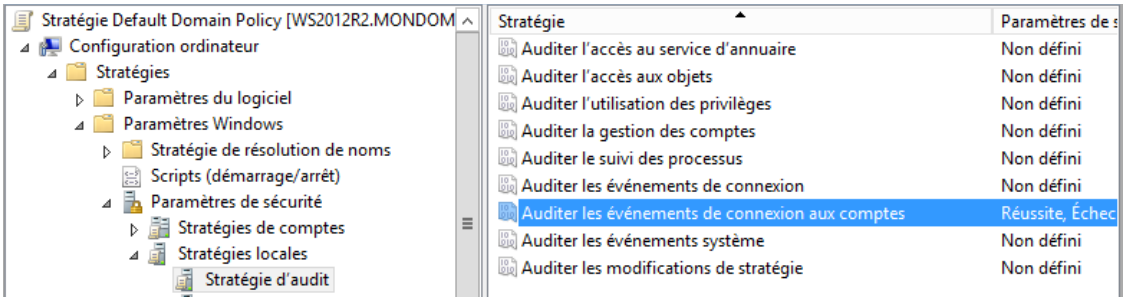
Pour cela, il faut tout d'abord verrouiller l'ordinateur après plusieurs essais infructueux.

Exemple de configuration possible :



IV.2 Surveillance des événements

Il faut maintenant être informé en cas d'essais infructueux. Pour cela, il faut aller dans l'éditeur de Stratégies de groupe (voir image ci-dessous) et activer « Auditer les événements de connexion aux comptes :



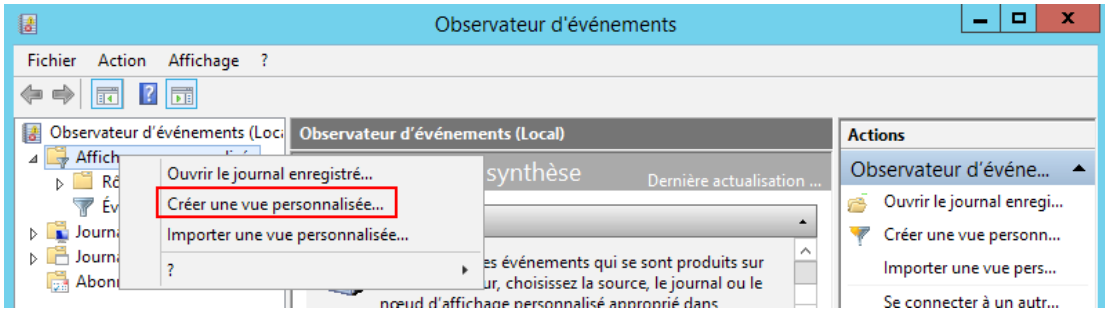
Les réussites permettent de savoir qui s'est connecté sur ce poste et à quelle heure en cas de problème. Si ce poste accède à des données interdites par exemple, il est possible de savoir qui était connecté alors.

Les échecs permettent de connaître les tentatives éventuelles de piratage.

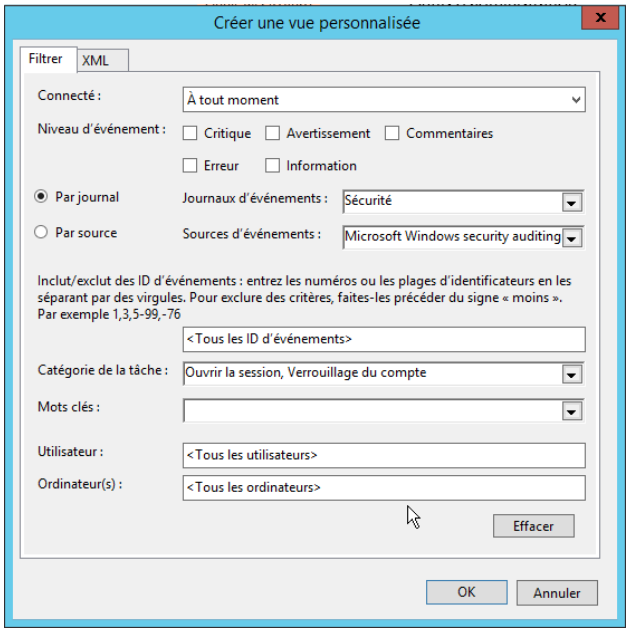
IV.3 Création d'un affichage personnalisé

En cas d'échec ou de réussite de connexion, un événement est créé et il peut être visualisé dans l'observateur d'événements (Outils d'administration). Pour faciliter la recherche des événements de connexion dans l'ensemble des événements, nous allons créer un affichage personnalisé.

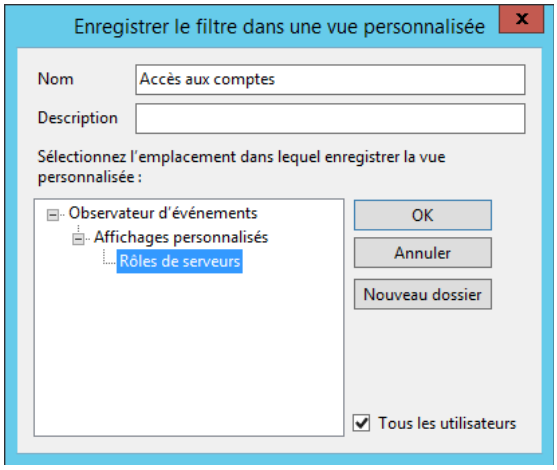
Pour cela, vous devez ouvrir « Observateur d'événements » (outils d'administration) puis sélectionner « Affichages personnalisés » et faire un clic droit pour **créer une vue personnalisée** :



Vous devez configurer la vue comme ci-dessous :

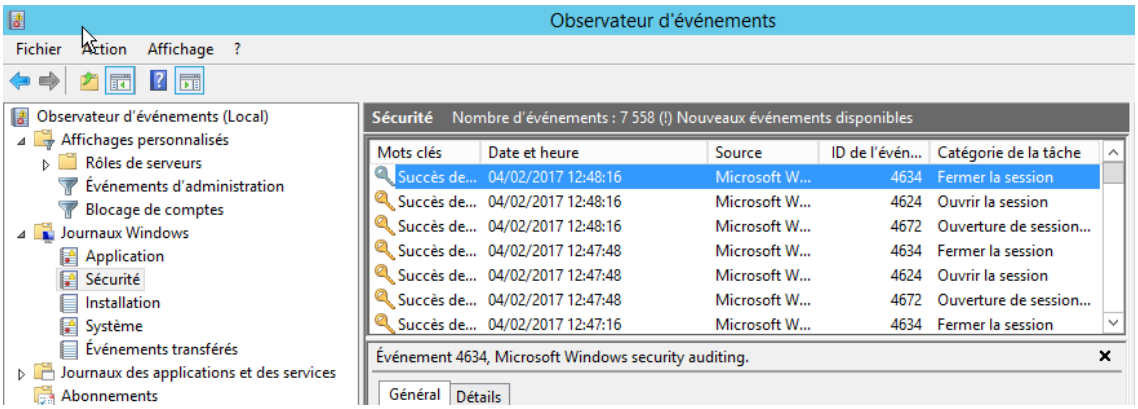


Si vous entrez comme ID d'événement 4740, seuls les événements générés suite à un verrouillage de compte seront pris en compte. Puis il faut enregistrer le filtre avec un nom :



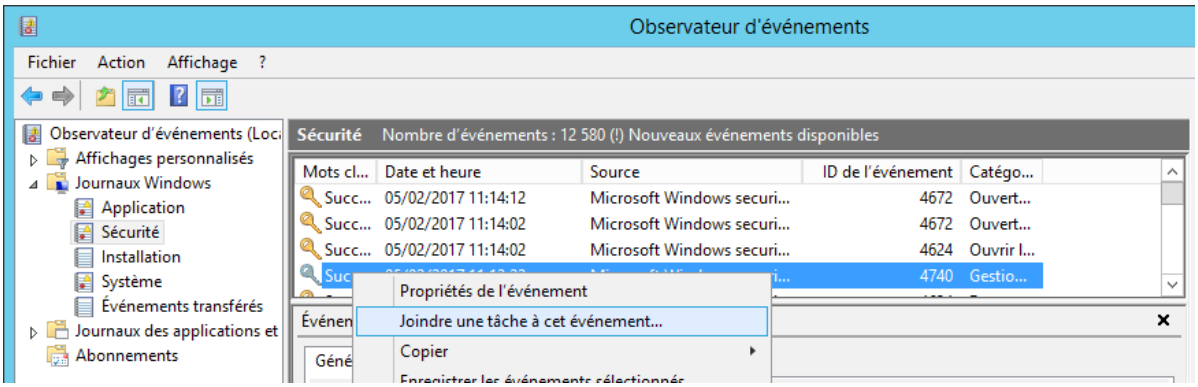
IV.4 Supervision des événements

Pour connaître les événements survenus, il suffit de les visualiser dans la fenêtre « Observateur d'événements » :

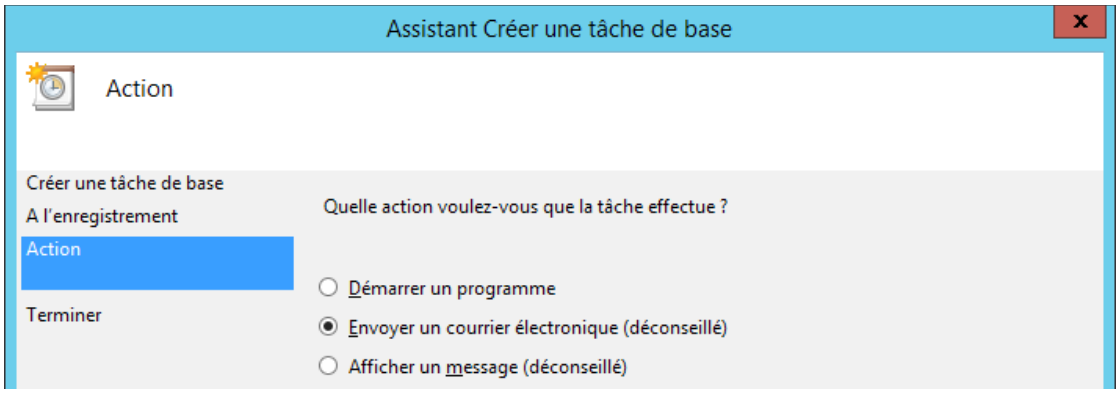


Vous devez choisir le type d'événements dans la partie gauche de la fenêtre pour avoir la liste des événements. Si vous sélectionnez un des affichages personnalisés créés, vous n'aurez que les événements que vous avez choisi.

Tout cela signifie que vous devez lire les événements pour être informé d'une tentative de piratage. Il est plus efficace d'être informé par mail par exemple. Il faut sélectionner l'événement concerné dans l'observateur d'événements et faire un clic droit puis choisir « Joindre une tâche à cet événement... » :



Après avoir appuyé deux fois sur « Suivant », vous pouvez choisir l'action à faire quand l'événement survient :



Il ne reste plus qu'à configurer la tâche.

V Gestion des stratégies

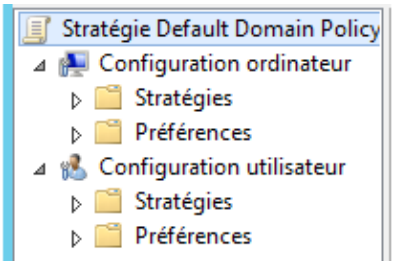
V.1 Principes des stratégies

L'application de stratégies sur un réseau permet de définir de façon centralisée la configuration des ordinateurs ainsi que l'environnement de travail des utilisateurs qui se connectent au réseau. Les stratégies peuvent être liées à des Unités d'organisation et s'appliquent aux utilisateurs et ordinateurs présents dans cette OU ou dans une OU de niveau inférieur.

V.2 Constitution d'une GPO

Une GPO (Group Policy Object ou stratégie de groupe) est constituée de deux parties :

- Partie pour le réglages de l'ordinateur
- Partie pour le réglages de l'interface de l'utilisateur



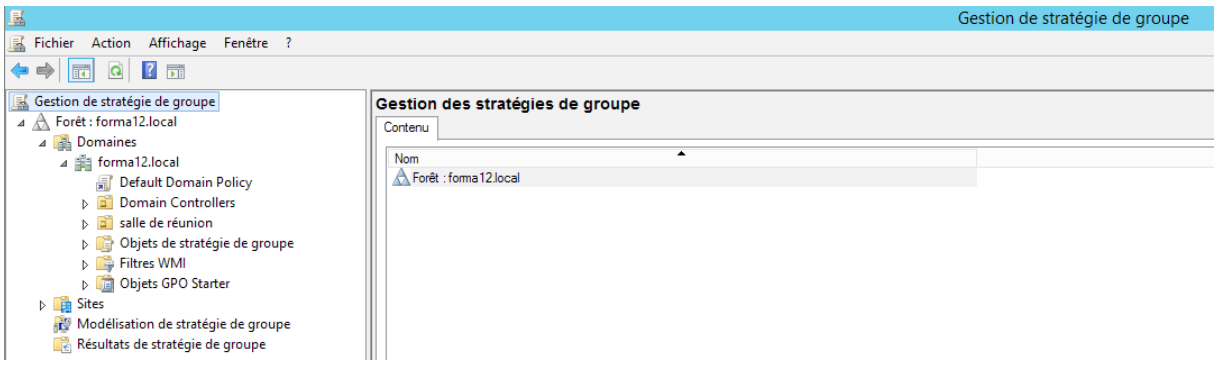
Chaque partie est constituée de deux rubriques :

- La rubrique **stratégies** pour les réglages figés
- La rubrique **préférences** pour les préréglages.

V.3 La console de gestion des GPO

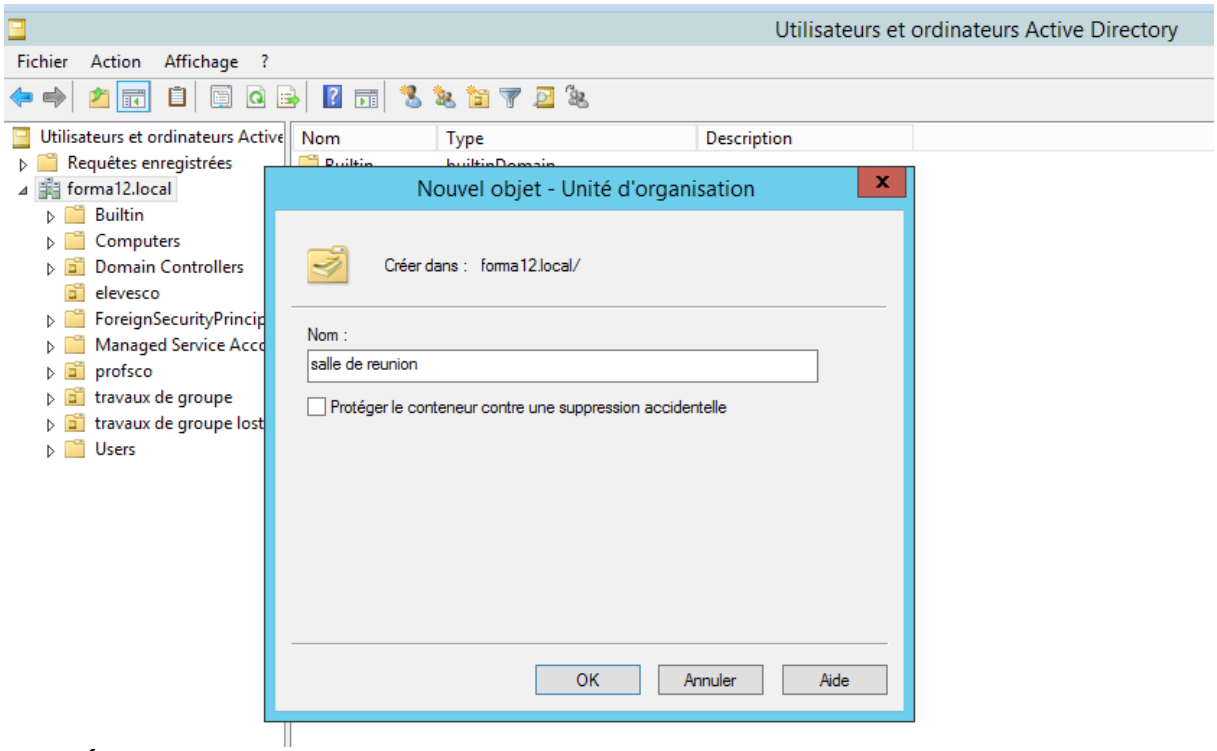
La gestion se fait à partir de l'outil **Gestion des stratégies de groupes (GPMC)**.

Cet outil permet d'avoir une vue d'ensemble des GPOs :



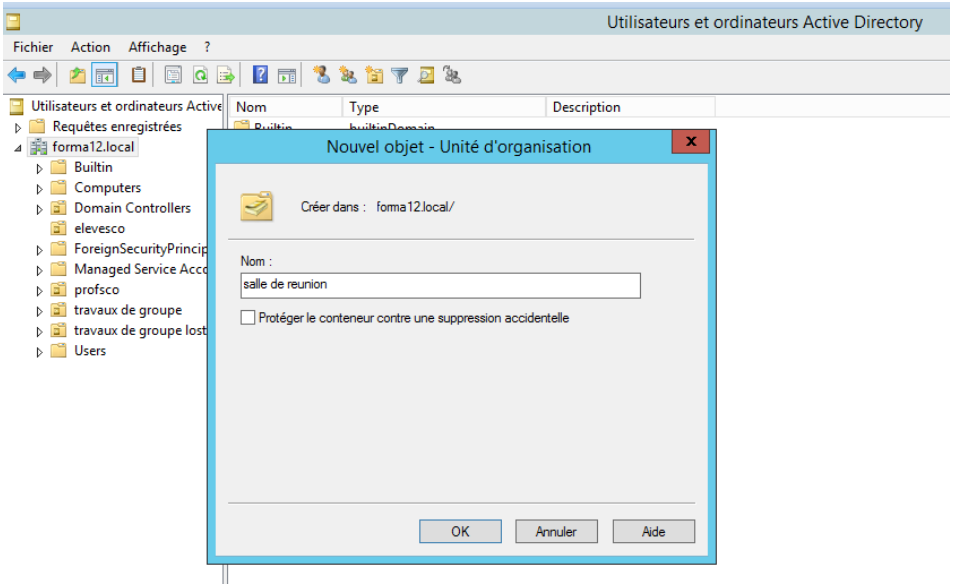
V.4 Édition des paramètres d'une GPO

Il faut d'abord créer une OU (unité d'organisation) dans l'AD. L'OU représentant par exemple une salle dans laquelle vous disposerez vos ordinateurs. Cliquez-droit sur le domaine puis nouveau puis unité d'organisation.

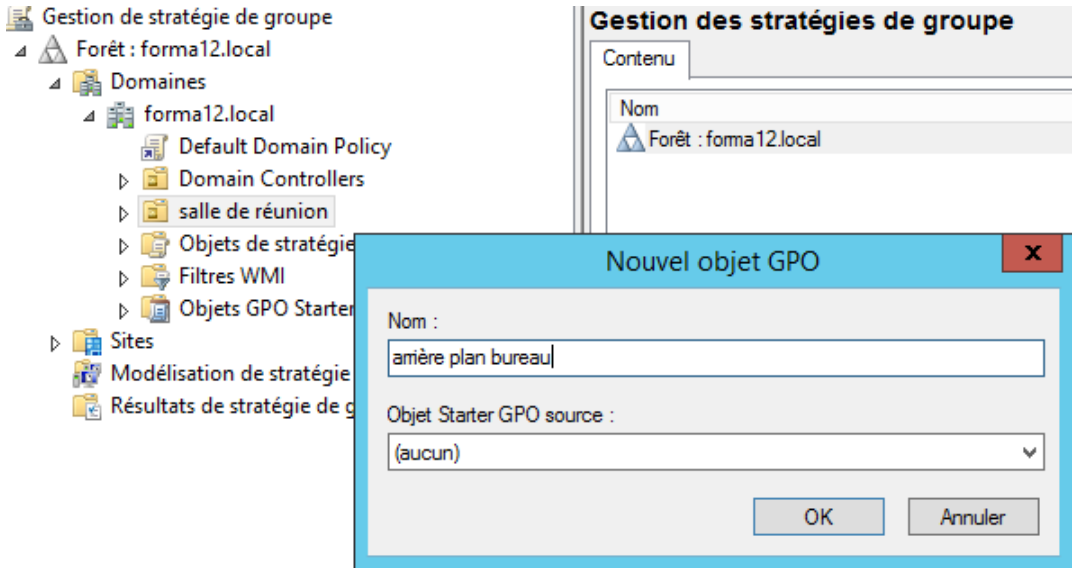


V.5 Édition des paramètres d'une GPO

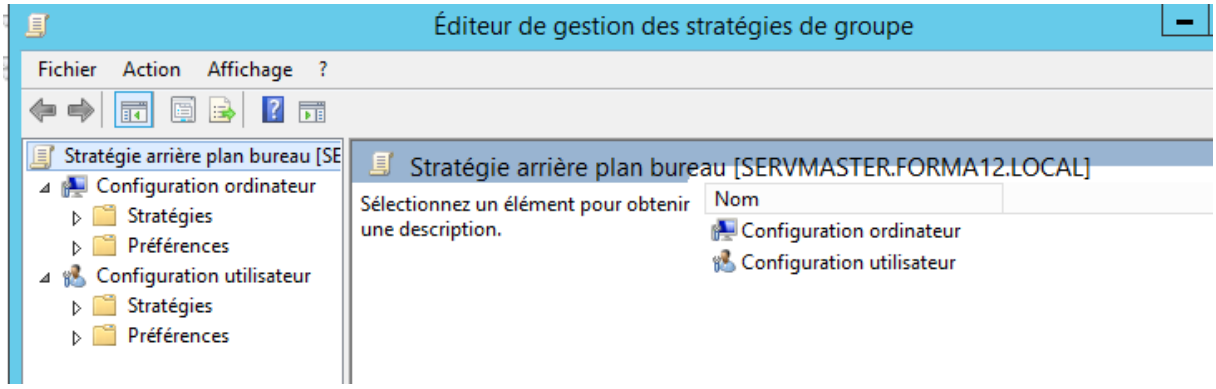
Il faut d'abord créer une OU (unité d'organisation) dans l'AD. L'OU représentant par exemple une salle dans laquelle vous disposerez vos ordinateurs. Cliquez-droit sur le domaine puis nouveau puis unité d'organisation.



Ensuite il faut aller dans Gestion des stratégies de groupes puis faire un clique-droit sur l'OU sur laquelle vous voulez appliquer la GPO puis cliquez sur **Créer un objet Gpo dans ce domaine, et le lier ici.**

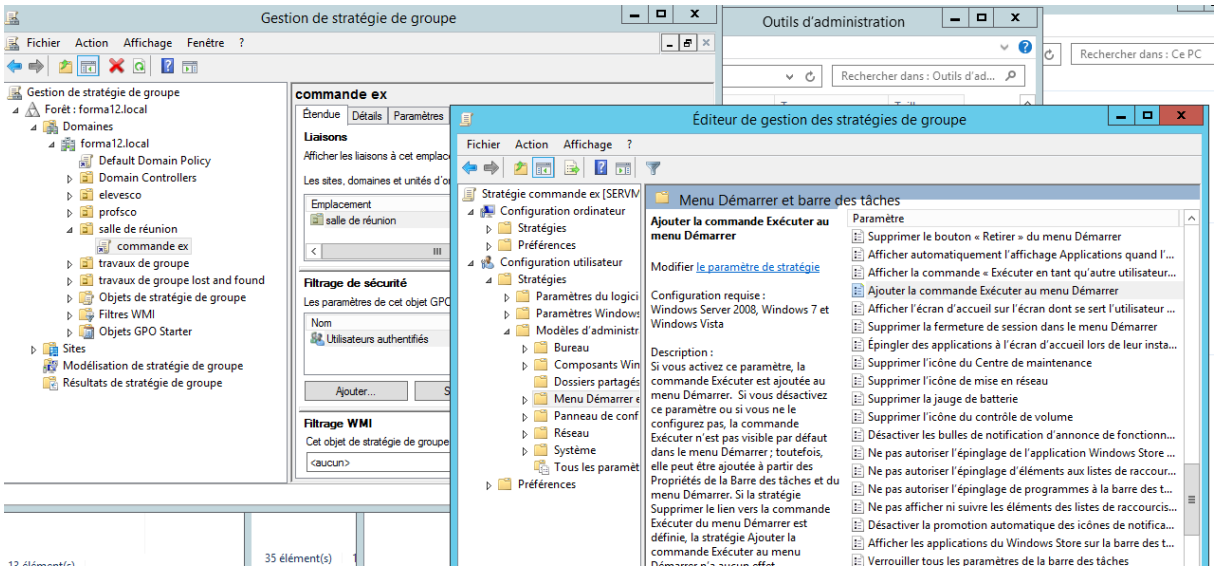


Dans l'OU, sélectionnez la GPO , cliquez-droit puis cliquez sur **modifier.**

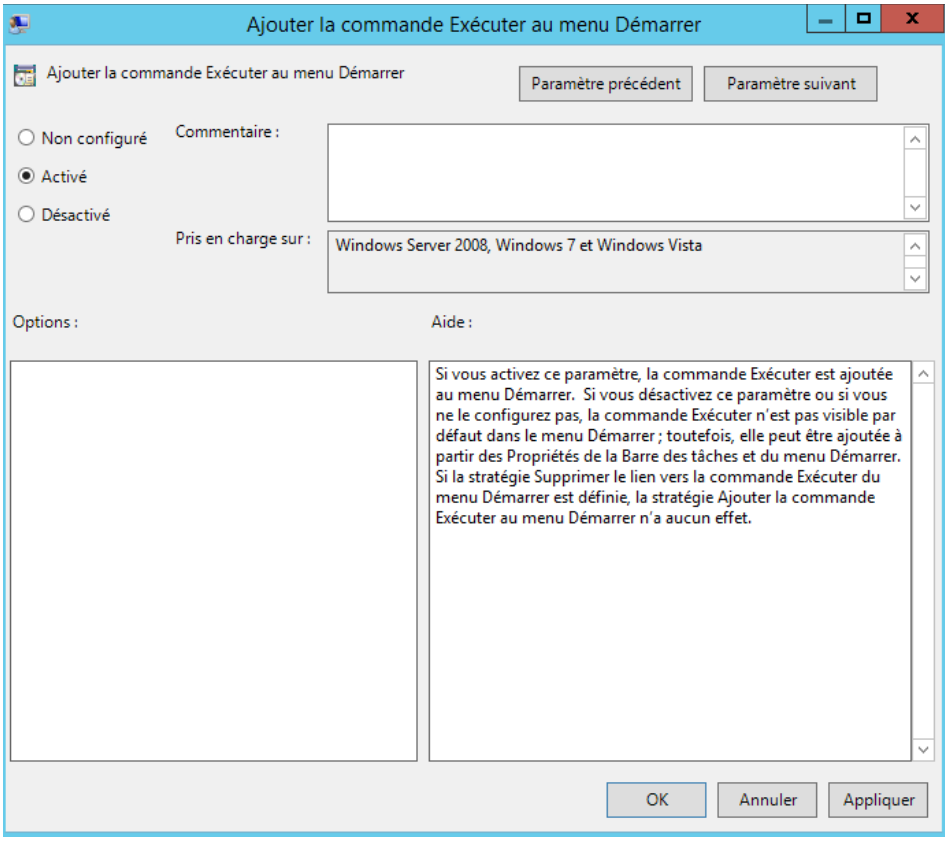


Il ne reste plus qu'a effectuer les réglages souhaités.

Exemple : Création d'un GPO « commande ex » qui affichera la commande exécuter au menu démarrer.



Sur l'action à effectuer, cliquez-droit puis modifier :



En cliquant sur OK vous appliquerez la GPO aux PC situés dans l'OU.

Remarque :

1. Pour placer les PC dans une OU : il faut aller dans l'AD et sélectionner les PC placés dans computers puis les déplacer dans l'OU.
2. La GPO s'applique au démarrage du PC.