Gestion des stratégies

Théorie : Astuces sur les GPO

Objectifs ICT

☐	Connaitre quelques astuces sur les stratégies de sécurité

Au terme de ce chapitre, je suis capable de …

Thème 1	
☐oui ☐non	Expliquer le principe de quelques astuces sur les stratégies de sécurité.
☐oui ☐non	D'utiliser les quelques astuces sur les stratégies de sécurité.

Table des matières

Informations sur le chapitre

Durée

Durée prévue :

- *5 périodes, avec les exercices*

Références

- *123_07_03_Astuces sur les GPO.docx (CPLN)*

- *http://technots.free.fr/?p=429*
- https://social.technet.microsoft.com/Forums/fr-FR/fdda9447-6ff0-4b80-bec1-c184d423627d/quel-est-lintert-pour-une-gpo-de-loption-appli-quenforced?forum=windowsserver2008fr
- *https://www.techsupportforum.com/forums/f8/domain-security-policy-vs-domain-controller-policy-304404.html*
- *https://www.it-connect.fr/les-gpo-ne-sappliquent-pas-14-pistes-a-etudier/*

1 Les commandes importantes

Voici les deux principales commandes utilisées :

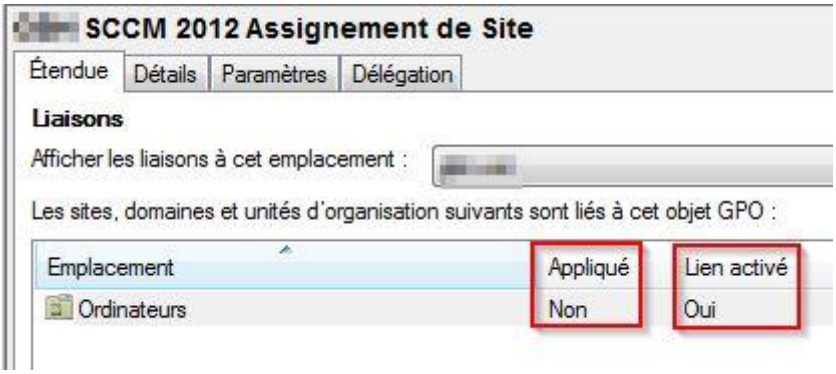
gpupdate / force : cette commande force la mise à jour des stratégies de sécurité

gpresult /r : Affiche un résumé des stratégies effectivement appliquées

> ***Remarque :***
> **Suivant le type de GPO, il peut être nécessaire de reconnecter l'utilisateur ou redémarrer l'ordinateur.**

2 Différence entre les options « Appliqué » et « Activé »

- Enforced (Appliqué). Ne peut jamais être contredis par une GPO appliquée plus bas dans la hiérarchie.
- Enabled (Lien activé). La stratégie fonctionne. Si ce paramètre est sur « non », la stratégie ne fonctionnera pas



http://technots.free.fr/?p=429

Autre explication :

L'option « **lien activé** » (linked dans la version anglo-saxonne) veut dire que la stratégie est attachée (et va donc affecter) son Site (ou son Domaine ou son / « **O.U.** »).

Globalement, cela signifie que la stratégie est appliquée à son conteneur.

L'option « appliqué » (enforced dans la version anglo-saxonne) permet de forcer l'application des paramètres d'une stratégie, même si une stratégie de priorité supérieur vient les contredire.

Car si on ne fait rien, c'est le dernier qui a parlé qui a raison.

Bourbita Thameur

https://social.technet.microsoft.com/Forums/fr-FR/fdda9447-6ff0-4b80-bec1-c184d423627d/quel-est-lintert-pour-une-gpo-de-loption-appliquenforced?forum=windowsserver2008fr

3 Différence entre les stratégies « Default Domain Policy » et «Default Domain Controller Policy»

La stratégie « **Default Domain Policy »** s'applique sur tous les machines et serveurs membre du domaine.

Par contre la stratégie « **Default Domain controllers Policy »** s'applique uniquement aux serveurs qui jouent le rôle du contrôleur de domaine.

https://social.technet.microsoft.com/Forums/fr-FR/070cd06e-6b5e-47d0-b1e3-ba7301a26eb5/diffrence-entre-stratgie-default-domain-policy-et-default-controller-policy?forum=windowsserver2008fr

https://www.techsupportforum.com/forums/f8/domain-security-policy-vs-domain-controller-policy-304404.html

4 Si une stratégie de sécurité ne s'applique pas

Lien : https://www.it-connect.fr/les-gpo-ne-sappliquent-pas-14-pistes-a-etudier/

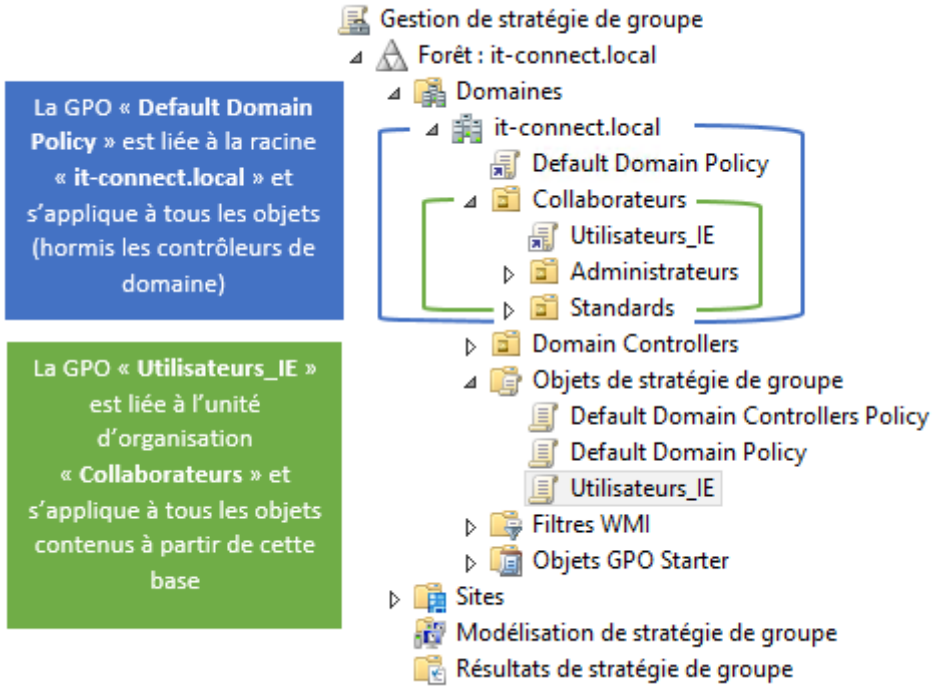
4.1 Un paramètre non appliqué ? vérifiez l'étendue

Si un paramètre ne s'applique pas, vérifiez l'unité d'organisation sur laquelle s'applique la stratégie. S'il s'agit d'un paramètre **Ordinateur**, la stratégie doit s'appliquer sur l'« **O.U.** » qui contient l'**objet ordinateur ciblé**.

Sur le même principe s'il s'agit d'un paramètre **Utilisateur**, la stratégie doit s'appliquer sur l'« **O.U.** » qui contient **cet utilisateur**.

En fait, il faut surtout que l'objet cible soit dans l'étendue de la GPO (l'étendue est aussi appelée scope), c'est-à-dire qu'il soit dans la sous-arborescence sur laquelle s'applique la GPO.

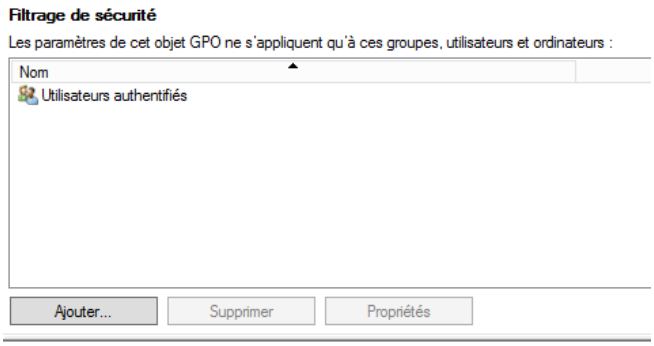
Exemple de cette notion d'étendue :



> ***Remarque :***
> **En fait, vérifiez que l'objet ciblé n'est pas « hors de portée » de la GPO..**

4.2 Le filtre de sécurité

Par défaut, le groupe « **Utilisateurs authentifiés** » dispose des autorisations nécessaires sur un objet de stratégie nouvellement créé. Pour rappel, ce groupe inclut tous les utilisateurs et tous les ordinateurs du domaine !



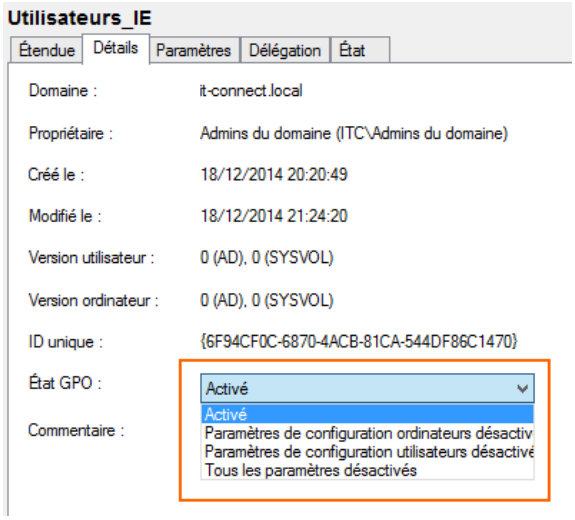
De ce fait et si vous avez décidé de modifier ce filtre de sécurité, assurez-vous que l'objet cible de la stratégie dispose des autorisations nécessaires. Dans les autorisations NTFS de la stratégie, vous retrouverez « **Utilisateurs authentifiés** » avec le droit « **Appliquer la stratégie de groupe** » sur « **Accepte**r », ce type d'autorisation est ajouté automatiquement lorsque vous ajoutez un utilisateur ou un groupe dans la zone « **Filtrage de sécurité** ».

Normalement, on ne modifie pas manuellement ces autorisations, sauf cas particulier.

Par exemple, si l'on souhaite empêcher qu'une stratégie s'applique sur un utilisateur, un ordinateur, ou un groupe, on modifiera manuellement les droits en passant par « **Appliquer la stratégie de groupe** » sur l'état « **Refuser** ». Ainsi, la stratégie ne s'appliquera pas, d'ailleurs vous pourriez contrôler au sein de votre infrastructure que n'ayez pas ce genre de problème qui pourrait se manifester par des messages du type « **Accès refusé** ».

4.3 Vérifier l'état de la stratégie

En sélectionnant une stratégie et en cliquant sur l'objet « **Détails** », il est possible de donner différents états à la stratégie (notamment des états de désactivation). Vérifiez que l'état est bien sur « **Activé** » pour activer l'ensemble des paramètres (ordinateurs et utilisateurs) définis dans cette stratégie.



4.4 Le lien est-il actif ?

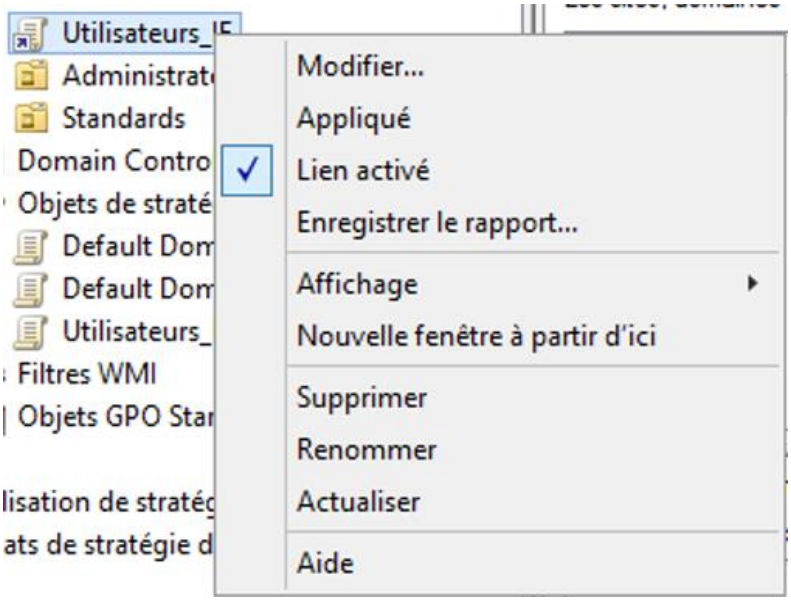
Dans la console de gestion des stratégies de groupe, les différentes stratégies sont stockées dans un container nommé « Objets de stratégie de groupe ». Ensuite, chaque stratégie est liée sur une « **O.U.** » plusieurs « **O.U.** », ce qui crée des liens.

Un lien représente un raccourci entre la GPO dans le container et l'« **O.U.** » sur laquelle s'applique cette GPO.

Ces liens peuvent être activés ou désactivés, cela signifie que l'on peut temporairement désactiver un lien pour désactiver l'application de la stratégie sur une « **O.U.** ». Ceci est pratique puisque ça évite de devoir supprimer le raccourci et le recréer ultérieurement.

Vous devez vérifier que les liens sont corrects, notamment actifs pour la stratégie qui doit s'appliquer.

En faisant un clic droit sur un raccourci, il sera possible de savoir si le lien est activé ou non :

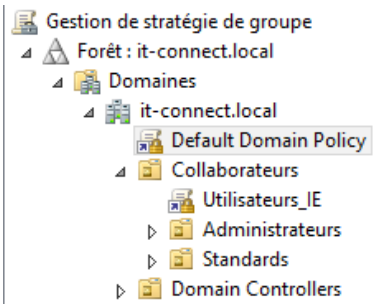


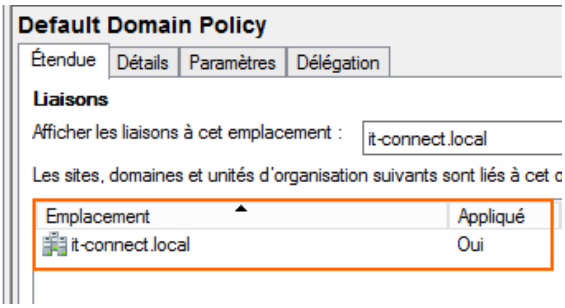
4.5 Les stratégies « Enforced » - « Appliqué »

Que la traduction de cette option est mauvaise ! En fait, dans la version française de Windows « **Enforced »** est traduit par « Appliqué », ce qui peut laisser penser que si on n'active pas ce paramètre la GPO ne sera pas appliquée. Ceci est totalement faux.

Il serait plus judicieux de traduire « **Enforced** » par « **Forcé »**, de ce fait comprenez « **Appliqué »** par « **Forcé »** (« **forcer l'application »**) et là ça change la donne.

Si on active ce paramètre pour une stratégie, on force son application et on la rend prioritaire par rapport à une autre. De plus, si deux stratégies sont forcées ce sera celle de plus haut niveau qui sera prioritaire ! Par exemple, si je force la GPO « **Default Domain Policy** » et la GPO « **Utilisateurs_IE** », ce sera la première qui gagnera sur la deuxième, car elle est placée « **plus haut** ».





On reconnaît facilement une stratégie sur laquelle le paramètre « **Appliqué** » est définit à « **Oui** », car l'icône contient un verrou.