

Attribuer le droit administrateur local à un groupe du domaine en GPP et le magasin central ADMX

Les objectifs du cours sont :

- Mapper un groupe de domaine à un groupe local
- Créer un magasin central ADMX

Monsieur GONSOR vous appelle, car en voulant accéder au site Internet de sa banque, il lui a été de demander d'installer un plug-in sur son poste.

Malheureusement, il n'a pas pu le faire car le logiciel lui a demandé de saisir les identifiants de l'administrateur local ou du domaine.

Il vous demande si vous pouvez lui donner les droits Administrateurs.

Au lieu d'attribuer les droits Administrateur sur le poste de l'utilisateur, vous allez créer une gpp qui va attacher le groupe global de la direction au groupe d'administrateur local.

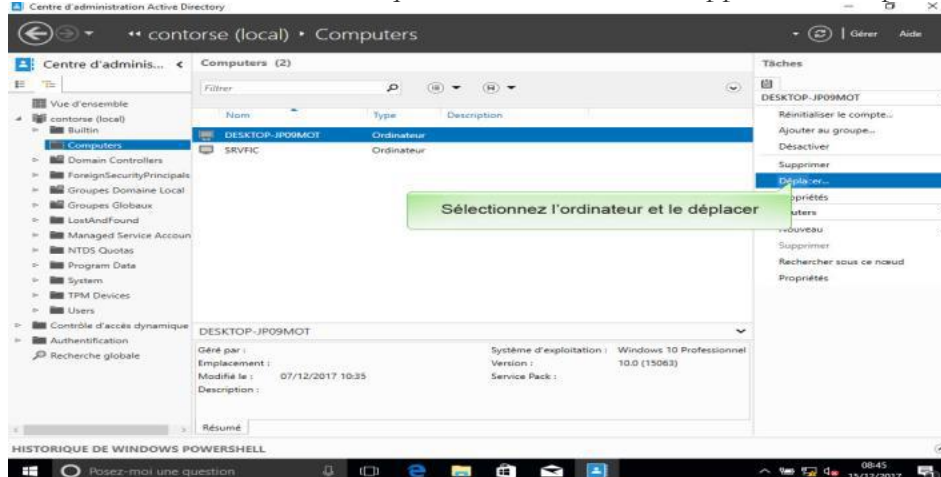
Ainsi, les utilisateurs de ce groupe auront les droits pour installer les logiciels sur leurs postes.

Création d'une GPO Ordinateur

Nous sommes connectés avec le compte de l'administrateur du domaine et avant de créer une nouvelle stratégie de type ordinateurs, nous allons déplacer l'ordinateur dans une OU.

Comme vous le savez, pour qu'une stratégie s'applique il faut que l'objet Utilisateur ou Ordinateur soit placé dans une OU.

Pour ce scénario, nous disons que cet ordinateur client appartient à stéphane Gonsor.



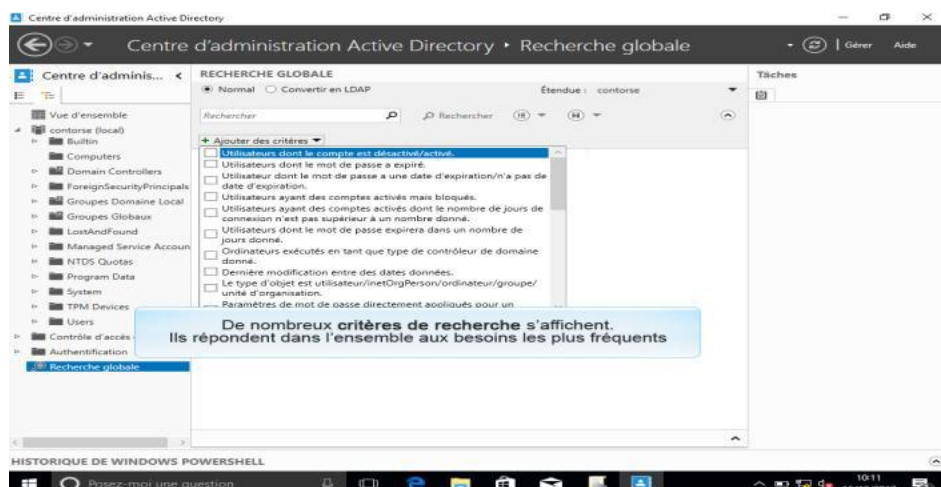
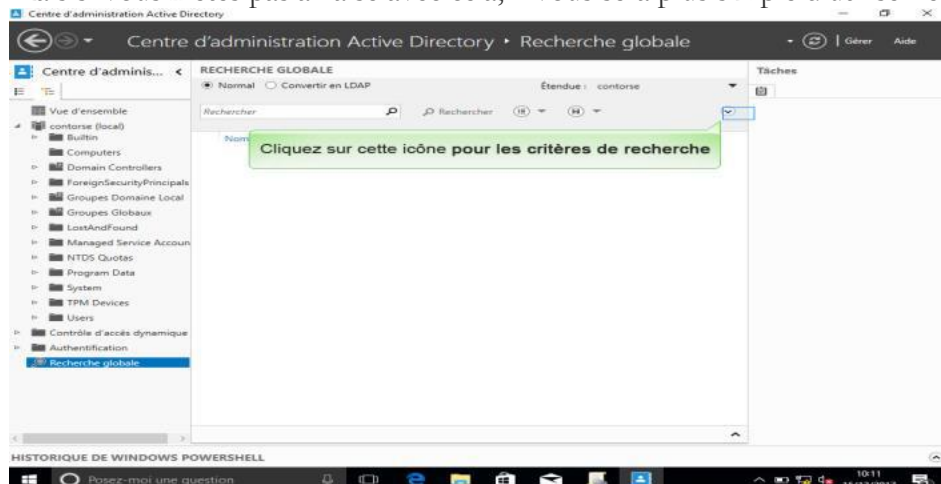
Nous allons le déplacer dans le dossier Ordis de l'UO Service direction.

Avant de quitter cette console pour créer notre nouvelle GPO, nous tenions à vous montrer qu'il existe un certain nombre de critères de recherche qui vous facilitent certaines tâches administratives.

Supposons que l'on vous demande de lister tous les objets utilisateurs du domaine.

Vous pourriez utiliser powershell et faire un script ou en trouver un sur Internet par exemple.

Mais si vous n'êtes pas à l'aise avec cela, il vous sera plus simple d'utiliser les filtres existants.



De nombreux critères de recherche s'affichent.

Ils répondent dans l'ensemble aux besoins les plus fréquents

A un critère il est possible d'en ajouter d'autres ou encore d'en filtrer le résultat par des conditions.

Nous pouvons ici filtrer notre résultat en demandant de rechercher tous les objets utilisateurs dont le nom est deluc par exemple.

Comme vous pouvez le voir, cette console est extrêmement puissante et nous permet d'être beaucoup plus efficace.

Enfin, notez qu'il est possible de sauvegarder vos requêtes.

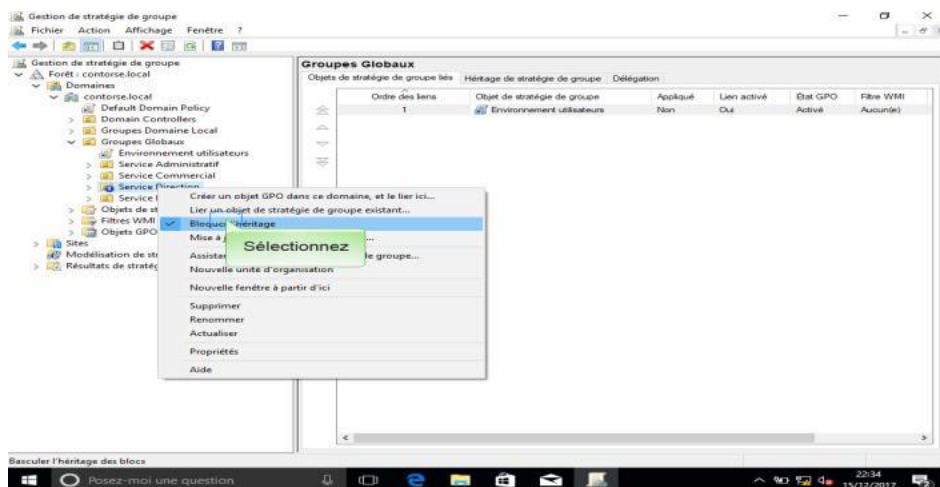
Cela vous fera gagner un temps précieux.

Nous allons créer un groupe Admins_locaux à la racine de l'OU groupe globaux.
Ajoutez le groupe GG_Direction comme membre de ce groupe.
Vous allez comprendre l'intérêt de groupe par la suite.

L'avantage de créer un groupe Admin local est que si plus tard nous devons élever les droits d'un utilisateur du domaine, il suffira alors de l'ajouter à ce groupe.

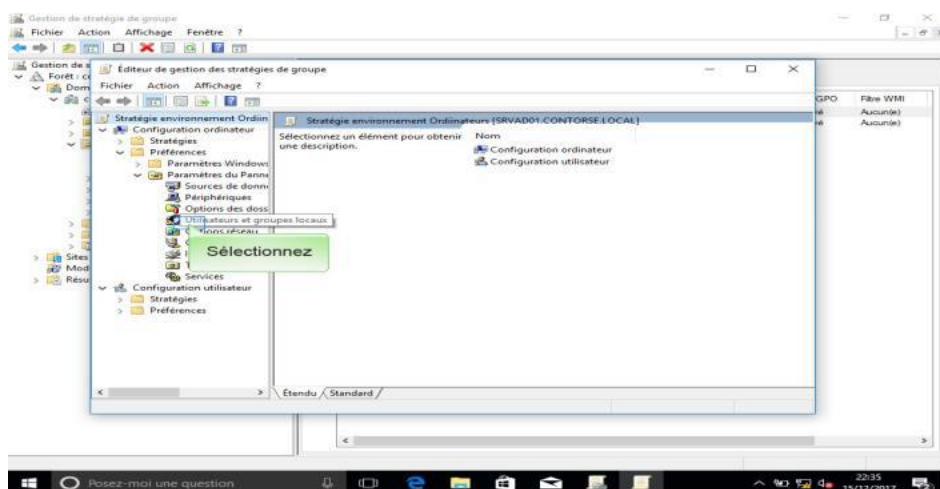
Nous allons maintenant créer une GPP Ordinateur et mapper les utilisateurs du groupe Admin_locaux au groupe administrateurs locaux de la machine.

Nous allons désactiver le blocage d'héritage pour l'OU Service Direction.



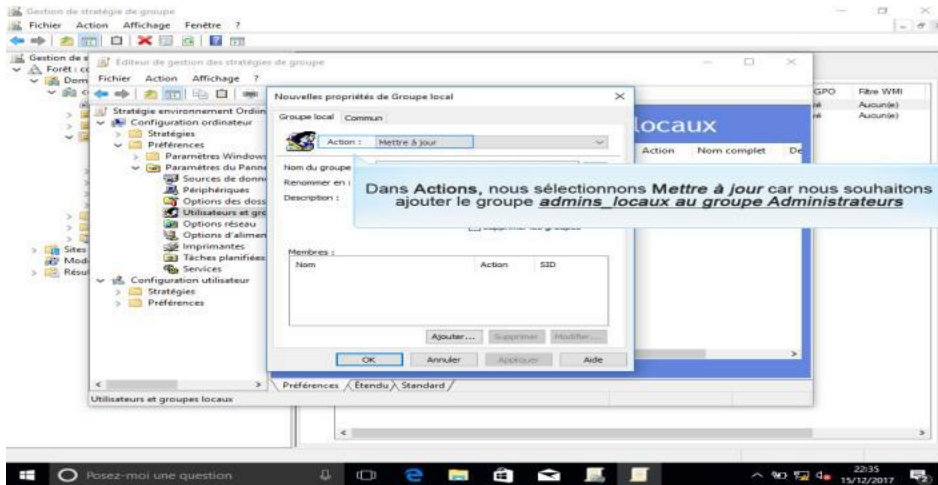
Puis nous créons un objet stratégie de groupe nommé « environnement ordinateur » sur l'OU « Groupes globaux ».

Cette stratégie est volontairement placée à la racine de Groupes Globaux mais seuls les utilisateurs appartenant au groupe Admins_locaux seront concernés par la GPP que nous allons configurer.

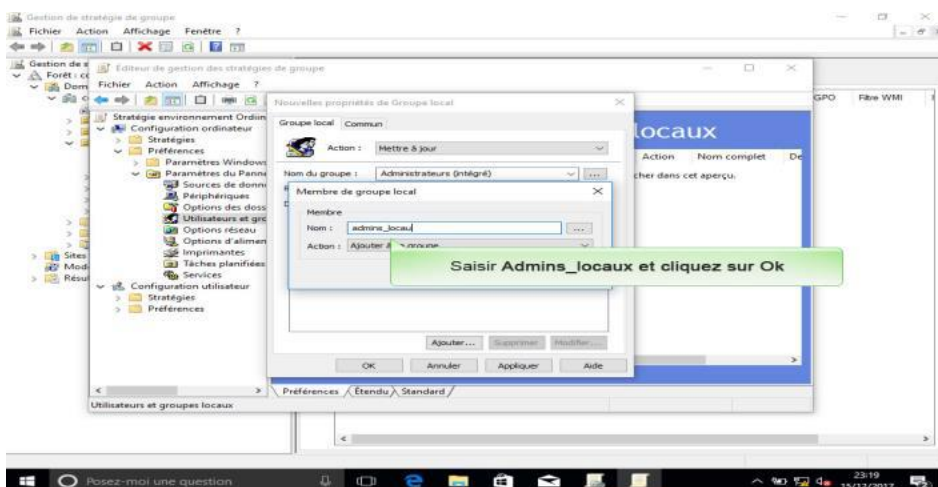
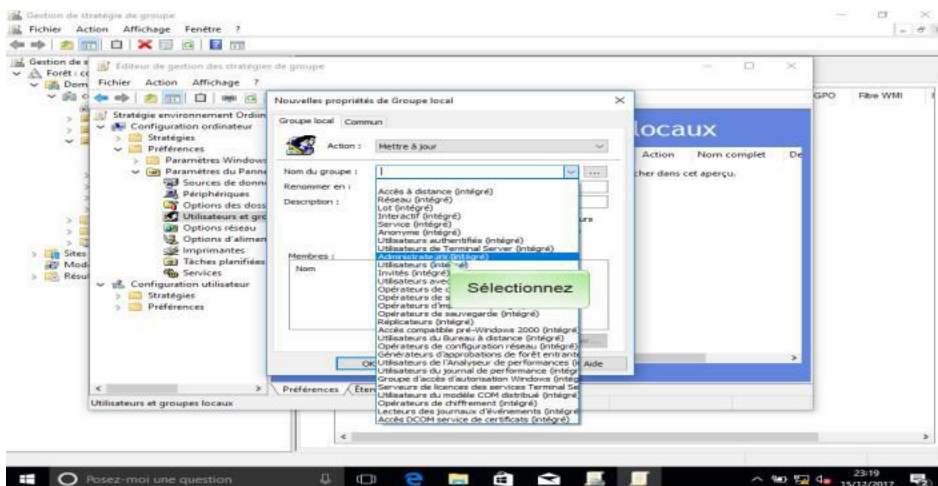


Cette GPP nous permet de créer des admin locaux sur des postes du domaine mais aussi d'ajouter un utilisateur ou un groupe du domaine dans un groupe local.

En clair, le groupe du domaine Admins_locaux va être ajouté au groupe Administrateurs sur chacun des postes du domaine, puisque la stratégie est placée à la racine de Groupe Globaux.

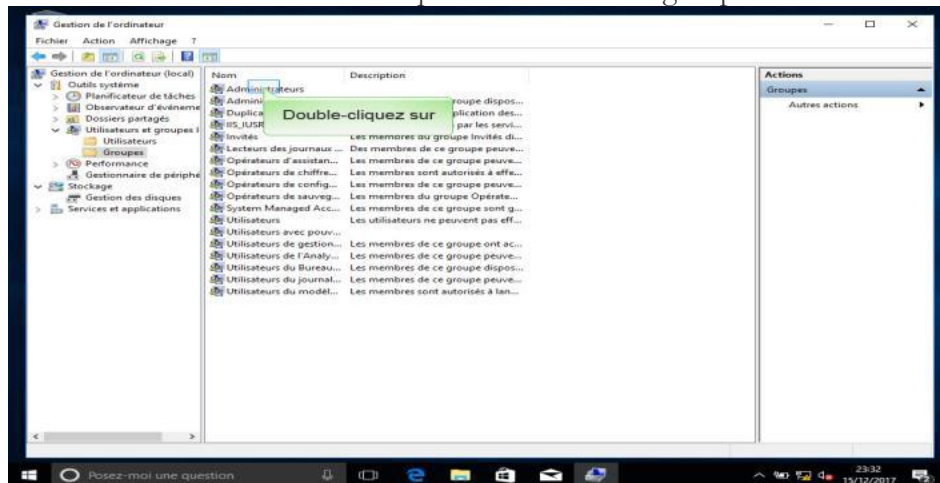


Dans Actions, nous sélectionnons Mettre à jour car nous souhaitons ajouter le groupe admins_locaux au groupe Administrateurs.



Le groupe Admins_locaux va être ajouté au groupe Administrateurs de la machine.

Comme il s'agit d'une stratégie ordinateurs, nous allons redémarrer le pc puis nous connecter avec l'utilisateur stephane gonsor car il est membre du groupe Admins_locaux. Nous allons maintenant vérifier qu'il est membre du groupe Administrateur local



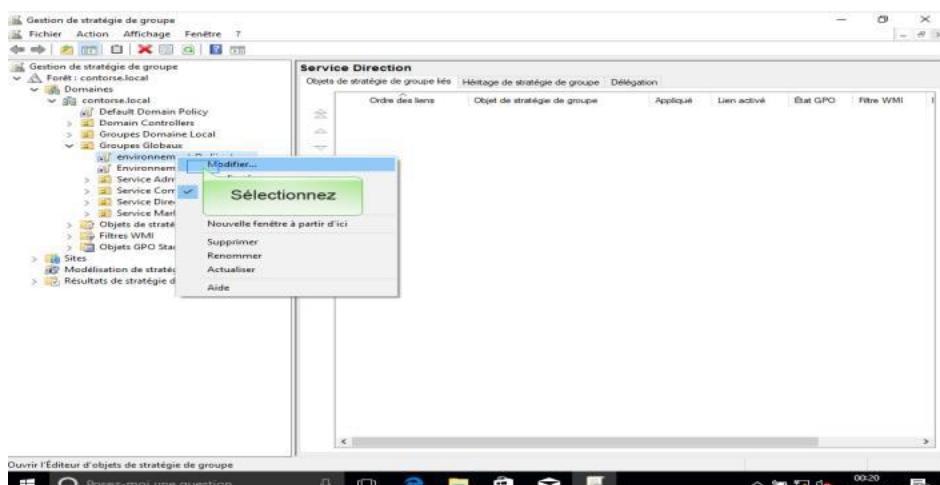
On peut voir que le groupe Admins_locaux a bien été ajouté. Le groupe Admins du domaine est automatiquement ajouté dès que le poste est intégré au domaine.

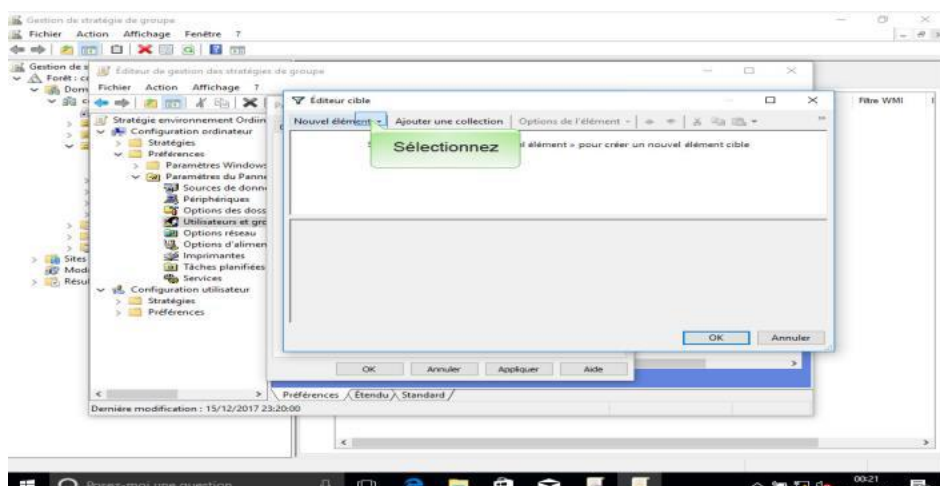
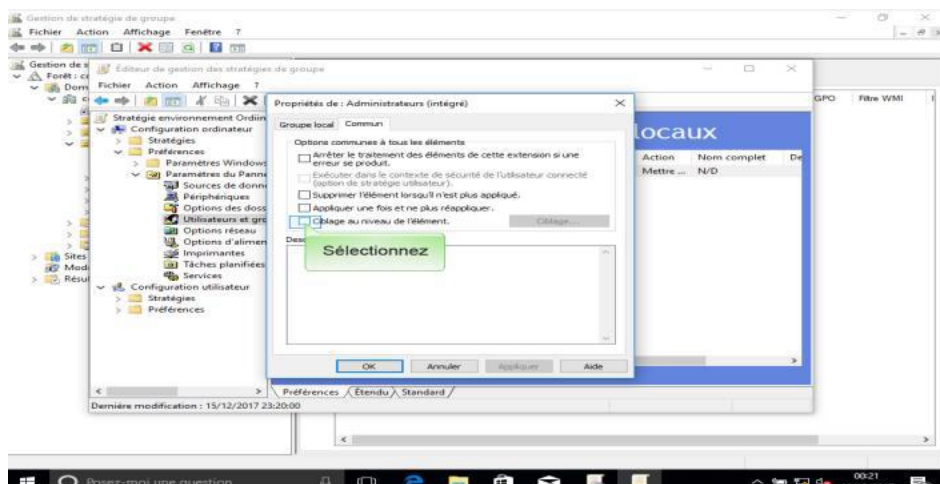
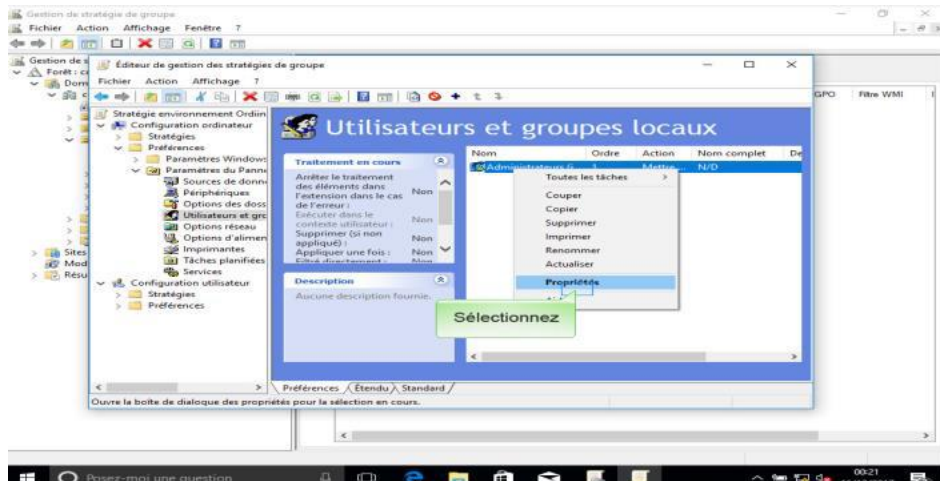
Cependant, il ne pourra pas modifier la date et l'heure du système et cela est rassurant puisque s'il existerait une trop grande différence de synchronisation du point de vue de l'horloge entre le client et le serveur AD alors les GPO ne s'appliqueraient pas.

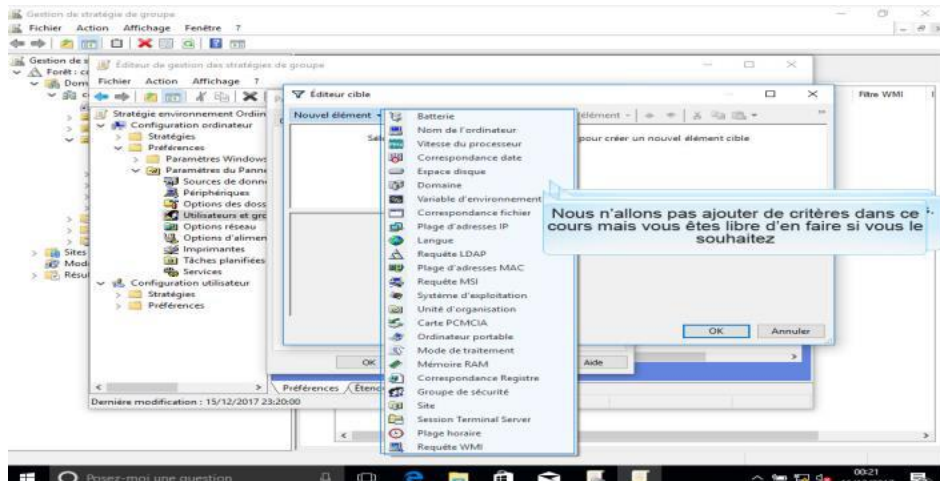
Nous allons maintenant voir si l'utilisateur peut installer un logiciel.

Vous pouvez maintenant essayer de vous connecter avec une personne qui n'appartient pas au groupe admins_locaux et vérifier qu'elle ne peut pas installer de programme.

Rappelez-vous, nous avons dit dans un cours précédent qu'il y avait une option ciblage au niveau de l'élément qui remplace les filtres WMI. Cette option est uniquement accessible pour des GPP.







Comme nous pouvons le voir, il est possible, de sélectionner des critères d'application pour cette GPP.

Il est possible de combiner plusieurs critères. Libre à vous d'imaginer des scénarios application.

Nous n'allons pas ajouter de critères dans ce cours mais vous êtes libre d'en faire si vous le souhaitez.

Gestion des fichiers ADMX

Notre client souhaite que l'on lui personnalise l'environnement Windows 10.

Par défaut, il existe environ 4 000 paramètres de stratégies qui permettent de personnaliser l'environnement Windows et les serveurs.

Toutefois, il est possible d'ajouter de nouveaux paramètres de stratégie afin de personnaliser des logiciels tiers ou des versions de Windows non connues par le serveur.

Par exemple, si vous souhaitez personnaliser l'environnement d'Office 2013 ou 2016, il existe un fichier ADMX qu'il est possible d'ajouter.

De même qu'ils en existent pour des logiciels comme Firefox ou autres...vous pouvez d'ailleurs les créer vous-même.

Quand Windows serveur 2012 est sorti, Windows 10 était en développement.

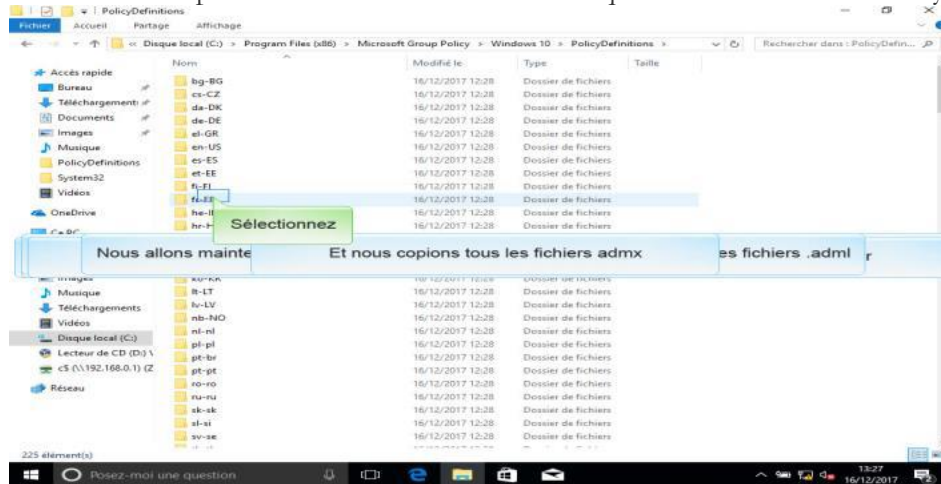
Il existe un fichier ADMX de Windows 10 que l'on va ajouter et qui va nous permettre de personnaliser son environnement.

La première chose à faire est de télécharger le fichier ADMX sur le site de Microsoft et de le copier dans la VM client.

Il faut l'installer.

Les fichiers ADMX se sont copiés mais pour pouvoir les importer dans la console gestion des stratégies de groupe, il est nécessaire de créer un magasin central qui contiendra un ou plusieurs fichiers ADMX.

Nous allons copier les fichiers d'administration qui ont été installés sur le système.



Les fichiers ADMX sont divisés en fichiers de langue neutre portant l'extension .admx et de langue spécifique avec une extension .adml (visible dans le répertoire fr-FR etc...)

Les fichiers de langue neutre garantissent la similitude entre les principales stratégies d'une GPO.

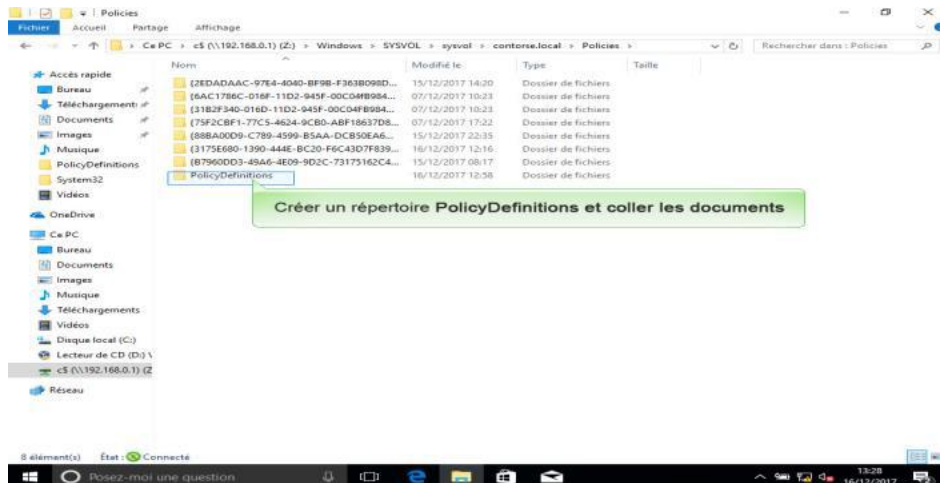
Grâce aux fichiers de langue spécifique, les stratégies peuvent être visionnées et éditées en plusieurs langues.

Comme les fichiers de langue neutre stockent les principaux paramètres de stratégie, les stratégies sont éditables, quelle que soit la langue dans laquelle l'ordinateur est configuré, ce qui permet par exemple à un utilisateur de visionner et d'éditer des stratégies en français tandis qu'un autre les visionne et les édite en anglais.

Le mécanisme qui détermine la langue utilisée est le pack de langues installé sur l'ordinateur.

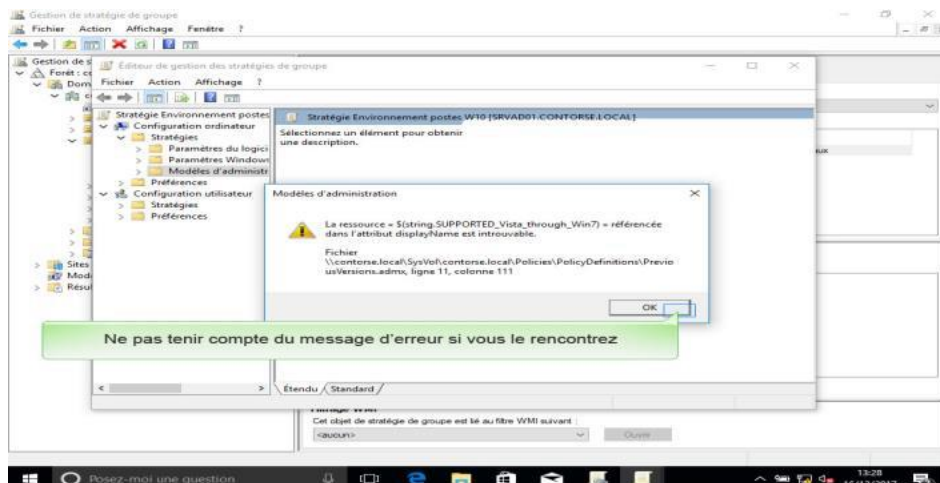
Nous allons maintenant copier les répertoires fr-FR, us-US qui contiennent les fichiers .adml et tous les fichiers admx.

Une fois que les fichiers sont sélectionnés, nous allons les coller sur le serveur Active Directory. Un lecteur réseau a été monté. Il pointe sur le partage administratif \\192.168.0.1\c\$. Le répertoire est indiqué ci-dessous :



Créer un répertoire PolicyDefinitions et coller les documents.

Nous allons maintenant nous connecter à la console MMC Éditeur de stratégie de groupe, pour modifier la GPO « environnement poste windows10 ».



Ne pas tenir compte du message d'erreur si vous le rencontrez

On voit que les stratégies ont bien été importées dans magasin central.

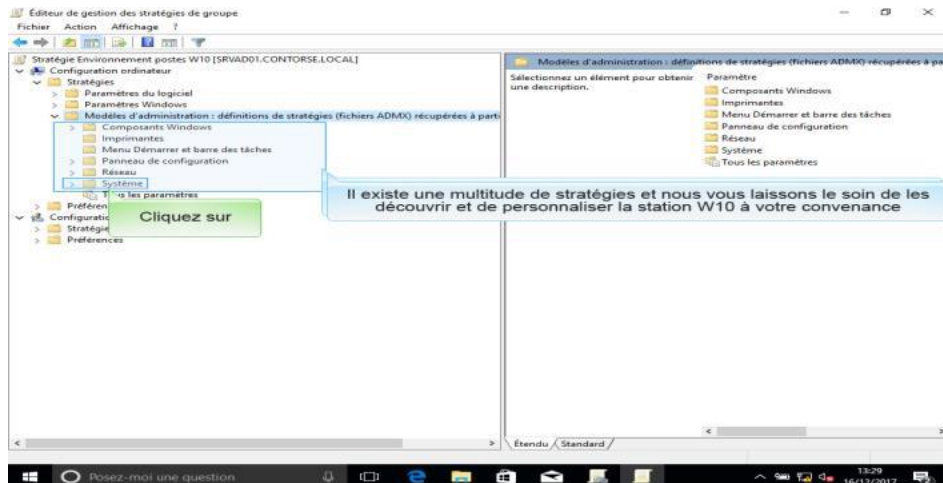
La création d'un magasin central est très intéressante car on centralise les fichiers ADMX dans un même endroit (ceux de Windows, office etc...)

En effet, dorénavant toutes les GPO seront en mesure de lire ces fichiers d'administration

Avant il fallait importer les fichiers ADMX dans la GPO, mais la problématique était que ces nouvelles stratégies n'apparaissaient que pour la GPO concernée.

Si nous avons une deuxième GPO et que l'on voulait utiliser ces fichiers d'administration, il fallait de nouveau les importer.

Par conséquent, le répertoire Sysvol pouvait devenir très lourd et créer des problèmes de répliquations entre serveurs AD.



On voit ici les paramètres de stratégies ordinateurs qu'il est possible d'appliquer pour les stations Windows 10.

Il existe une multitude de stratégies et nous vous laissons le soin de les découvrir et de personnaliser la station W10 à votre convenance.

Conclusion

Ce cours sur les mappage d'un groupe de domaine à un groupe local et la création d'un magasin central ADMX est à présent terminé.

Nous avons pu voir qu'il était assez simple d'ajouter un groupe de domaine à un groupe local grâce aux GPP.

L'intérêt est de pouvoir donner des droits particuliers à des utilisateurs du domaine sur les stations de travail.

Nous avons pu voir qu'il est possible d'affiner l'application d'une stratégie grâce à l'option ciblage au niveau de l'élément.

Enfin, nous avons terminé ce cours par la création d'un magasin central ADMX, qui permet de centraliser les fichiers ADMX pour un ensemble de stratégies de groupe.