http://WWW.CABARE.NET ©

Stratégies GPO & AD sous Windows 2016 & 2012 R2 – sys 26 – Travaux Pratiques -

Stratégies GPO de Domaine 2016 2012R2

Michel Cabaré – Ver 2.5 – juin 2017-

Stratégies GPO & AD sous Windows 2016 & 2008R2
Travaux Pratiques

Michel Cabaré – Ver 2.5 – juin 2017

www.cabare.net ©

Table des matières

GESTION DU MOT DE PASSE 5

VALEURS PAR DEFAUT : 5
RESTRICTION MOT DE PASSE « VIDE » : 5

STRATEGIES LOCALES 7

OUVERTURE DE SESSION « SANS DERNIER LOGIN »: 7
AFFICHAGE D'UN MESSAGE = 2 STRATEGIES: 8

STRATEGIES GESTIONNAIRE LISTE RESEAU 9

RAPPELS PROFIL RESEAU WINDOWS 9
CHOISIR UN PROFIL RESEAU – WINDOWS 10 10
CHOISIR UN PROFIL RESEAU - SEVEN 12
LISTES DES RESEAUX IDENTIFIES 14
PERSONNALISER LE RESEAU DE DOMAINE 15
PERSONNALISER UN RESEAU « GOOGLE » 16

PARE-FEU WINDOWS 17

PRINCIPE ACTIVATION - DESACTIVATION 17
DEFINIE 1 STRATEGIES PARE-FEU 18
EXPORTER IMPORTER 1 STRATEGIES PARE-FEU 18
GPO PERSONNALISEE PARE-FEU ET REGLE 19
NETSH EXPORT IMPORT CONFIGURATION PARE-FEU 22
STRATEGIE LOCALE DESACTIVATION PARE-FEU 23
GPO DESACTIVATION PARE-FEU (APERÇU) 24

LGPO SEVEN - 10 25

CONTEXTE 25
MLGPO POUR ADMINISTRATEURS 25
MLGPO POUR NON-ADMINISTRATEURS 27
SUPPRIMER LES MLGPO 28

MONTAGE DOMAINE 2016-2012R2 30

MONTAGE D'UN CONTROLEUR DE DOMAINE SOUS 2016 - 2012 R2 : 30
STRATEGIES LOCALES SERVEUR AUTONOME : 30

GPO DE DOMAINE 31

AFFICHAGE D'UN MESSAGE: 31
DEVALIDATION MOT DE PASSE COMPLEXE: 32
DECONNEXION DE SESSION INACTIVE: 33
FORCER L'AUTHENTIFICATION SUR LE SERVEUR: 36
BEST PRATICE : 1GPO = 1 ACTION 37

PREFERENCES & STRATEGIES 38

MAPPAGE LECTEUR COMMUN : 38
MODIFICATION UTILISATEURS LOCAUX : 39
Ajout utilisateur de Domaine dans groupe Local des administrateurs 39
Ajout Groupe de Domaine dans le groupe Local des administrateurs 41
Ajout Groupe de Domaine dans groupe Local des utilisateurs avec pouvoir 43
CIBLAGE DES PREFERENCES EXEMPLE SYSTEME XP: 44

GPO GROUPES RESTREINTS 45

GERER LES GROUPES LOCAUX : 45
REMPLACER DANS UN GROUPE LOCAL : 45

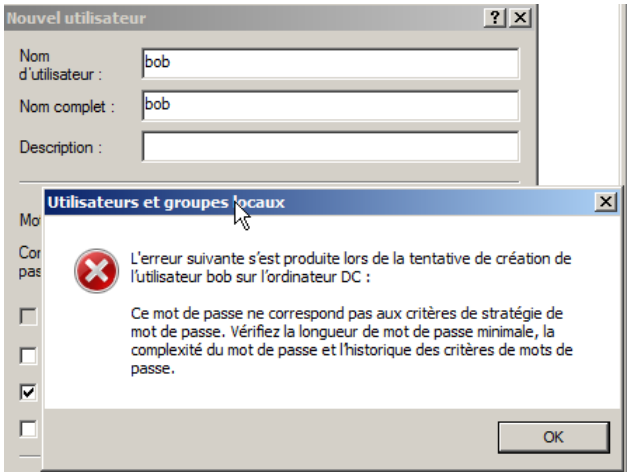
CREATION DE GPO SUR UNE UO 48
OBJECTIFS : 48
DEFINIR 2 UO DANS AD , ET CREER LEUR GPO : 48
CHANGER D'UO = CHANGER DE GPO : 49
PREFERENCE CREATION DE DOSSIER 50
CREATION DE DOSSIER 50
STRATEGIE RE-DEFINITION SECURITE NTFS 51
MODIFICATION NTFS SUR UN DOSSIER 51
RESULTAT ET TEST 53
GPO & MODELES D'ADMINISTRATION 55
OBJECTIFS : 55
BLOCAGE DE LA STRATEGIE POUR L'ADMINISTRATEUR: 55
CREATION DES STRATEGIES : 55
Supprimer executer 55
Interdire le panneau de configuration 56
Désactiver Windows Defender 57
GPO - SCRIPTS 58
SCRIPTS DE DEMARRAGE – ARRET – FIN DE SESSION : 58
SCRIPTS DE FIN DE SESSION : 58
Copier le script dans la GPO : (Afficher…) 59
Utiliser le script dans la GPO (Ajouter…) 60
PARAMETRAGE EXECUTION DU SCRIPT : 61
TEST ET VISUALISATION : 62
DESACTIVATION UAC: 63
GPO – SCRIPTS - NETSH 64
PARAMETRAGE VIA FICHIER WFW: 64
PARAMETRAGE VIA COMMANDE NETSH DIRECTE: 65
GPO VS SCRIPTS ARRET PC 66
WINDOWS COMMANDE SHUTDOWN: 66
GPO – PREFERENCE PLANIFICATION ARRET SHUTDOWN DES POSTES: 67
UTILITAIRES PSSHUTDOWN: 70
GPO - INSTALLATION DE LOGICIELS 72
LES 3 ELEMENTS WINSTALLER – GPO - AD 72
WINDOWS INSTALLER ET FICHIERS MSI 72
PROCEDURE D'INSTALLATION ET DE MAINTENANCE LOGICIELS 73
CREATION DU POINT D'INSTALLATION DE LOGICIEL 73
ATTRIBUTION - PUBLICATION DE LOGICIEL 73
STRATEGIE DE DEPLOIEMENT DE LOGICIEL 74
STRATEGIE DE RE-DEPLOIEMENT / DESINSTALLATION 75
PROPRIETES DE DEPLOIEMENT DE LOGICIEL 76
DEPLOYER ADOBE READER PAR MSI 77
RECUPERATION FICHIER ADOBE : 77
DECOMPRESSION FICHIER ADOBE : 78
MSIEXE /A - CREATION D'UN AIP ADMINISTRATION INSTALLATION POINT : 80
GPO DE DEPLIEMENT MSI : 81
DEPLOIEMENT DE FIREFOX 84
FRONTMOTION - RECUPERATION D'UN MSI FIREFOX : 84

GPO – PARAMETRAGE OFFICE 2016 87
RECUPERATION DES GPO TEMPLATES OFFICE 2016 87
LANCEMENT WORD 2016 PAR DEFAUT 88
GPO – FILTRE WMI 89
SELECTIONNER UN OS WINDOWS – EXEMPLE WMI 89
Windows Clients : *89*
Windows Sever : *90*
Les clients Windows : *91*
Les serveurs Windows : *91*
Les clients Windows posterieur ou égal au build 1803: *91*
TEST WMI VIA POWERSHELL 91
WINDOWS INSIDER PREVIEW 92
GESTION ACTIVATION WINDOWS 10 INSIDER PREVIEW : 92

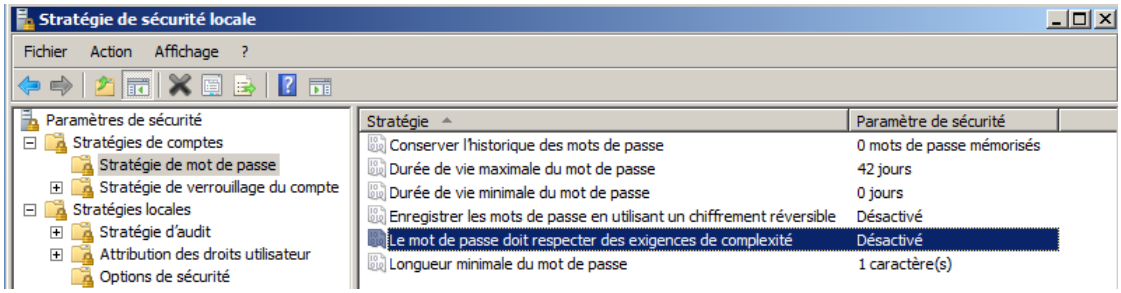
GESTION DU MOT DE PASSE

Valeurs par défaut :

Par défaut il se peut que l'on demande de créer des mots de passe respectant des **exigences de complexité**, une **longueur minimale** et une **durée de vie minimale** Cela provoque lorsque on crée un utilisateur ne respectant ces impératifs (par exemple **bob**, mot de passe **b**…) le message suivant :



La solution se trouve dans le **Panneau de Configuration / Stratégies de sécurité Locale**, **/stratégies de compte/stratégies de mot de passe**

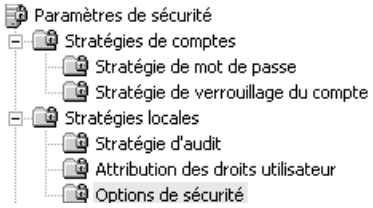


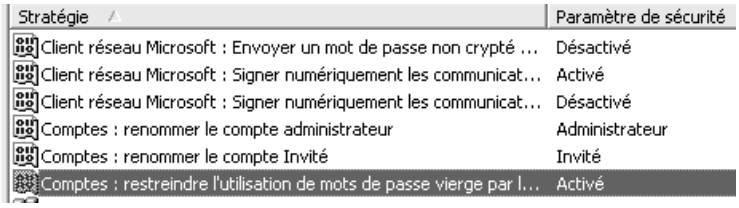
Restriction mot de passe « vide » :

Il est toujours nécessaire de spécifier un mot de passe depuis XP, car une nouvelle stratégie est apparue

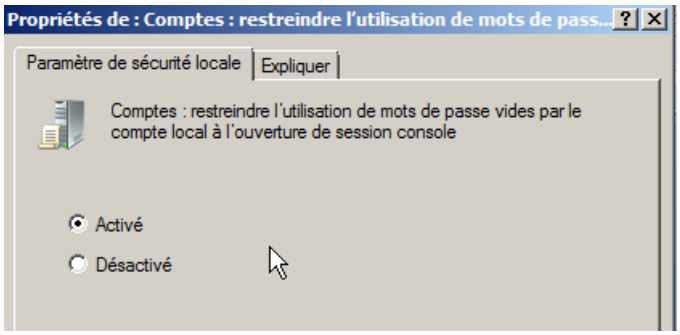
stratégies locales

Options de sécurité

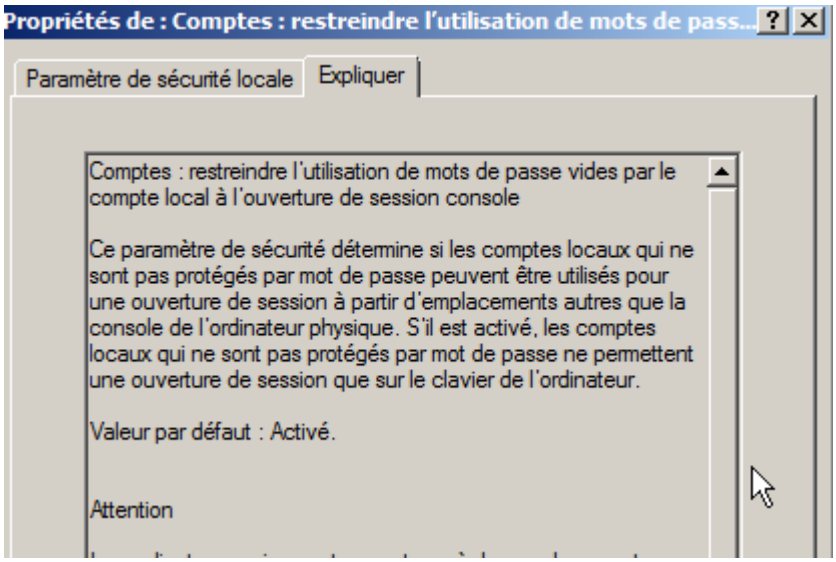




la valeur par défaut étant



Cela peut poser des pb au niveau réseau, même si l'explication n'est pas très explicite...



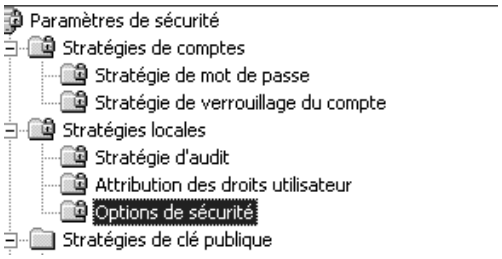
STRATEGIES LOCALES

Ouverture de session « sans dernier login »:

Pour augmenter la sécurité, on souhaite ne pas faire afficher le dernier identificateur de session utilisé sur cette machine

Mettez en œuvre localement cette stratégie, testez là, puis redonnez les valeurs par défaut…

Il faut aller dans

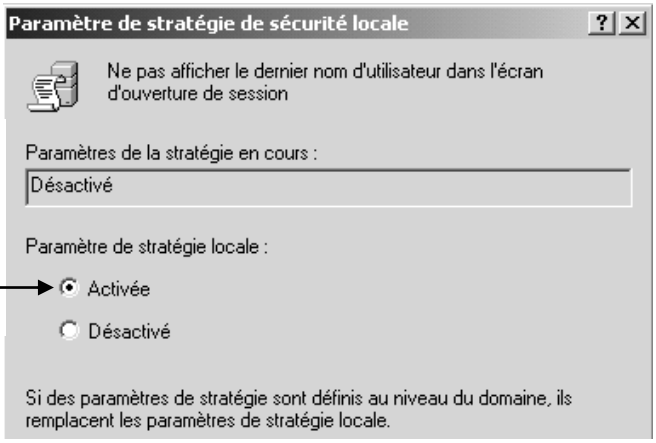


Stratégies locales

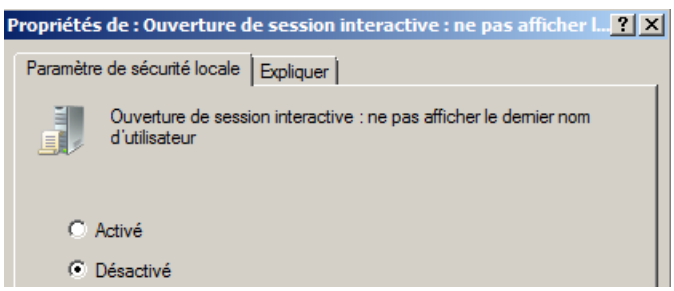
Options de sécurité

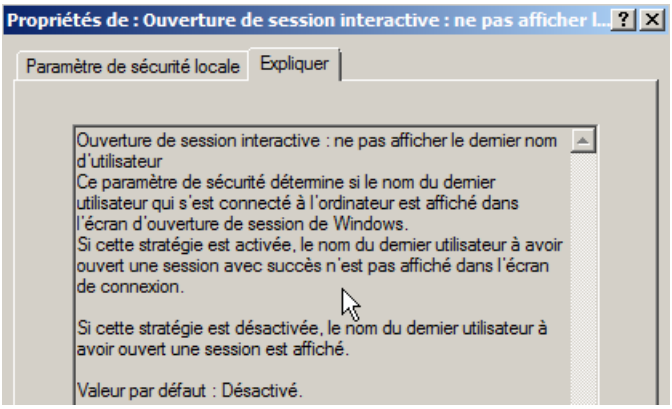
Ouverture de session interactive : ne pas afficher le dernier nom utilisateur

On double clic puis on demande **Activée**



N.B : on « active » le fait de « ne pas faire afficher » !





Affichage d'un message = 2 stratégies:

Il est possible de faire afficher un message au démarrage d'un poste, avant même l'ouverture de session. Soit dans une boîte de dialogue (pour XP et 2000) soit sur un fond d'écran (pour SEVEN…)

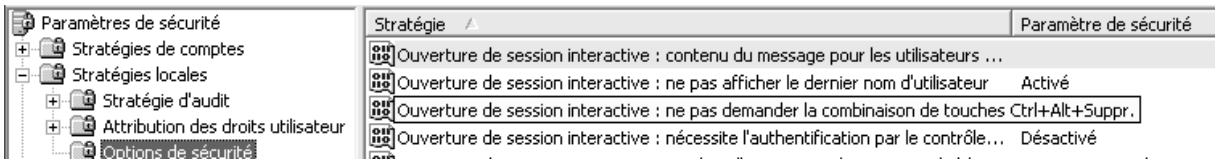
N.B : Il s'agit de deux stratégies conjointes **qui ne marchent pas isolément** !

Il faut aller dans

Stratégies locales

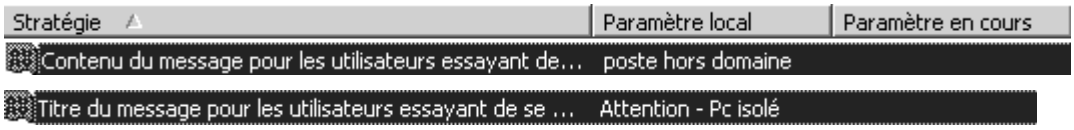
Options de sécurité

Depuis SEVEN-XP



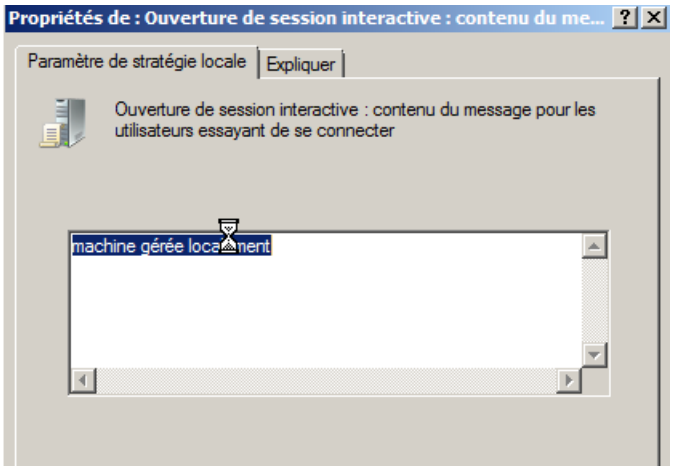
Les deux stratégies conjointes à paramétrer sont

Sous 2000 le libellé diffèrais légèrement



N.B : il peut être intéressant d'utiliser cette stratégie pour « rappeler » sur le PC l'appartenance du poste à tel domaine, ou a tel Service (si les GPO sont utilisées en ce sens…), ou au contraire que la machine est gérée en local...

Essayer dans un premier temps de ne remplir que la stratégie « **Contenu du message pour les utilisateurs** »...

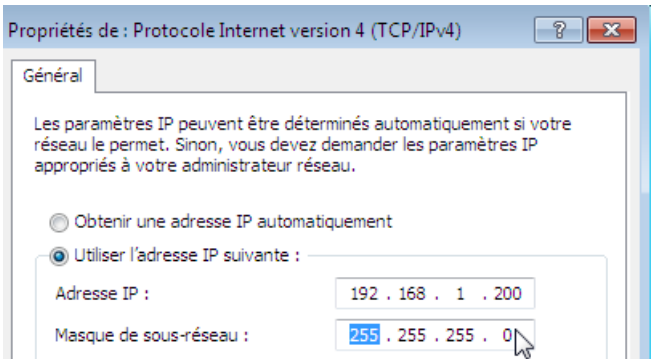


sans le « titre », rien ne se passe...

STRATEGIES GESTIONNAIRE LISTE RESEAU

Rappels Profil Réseau Windows

L'adressage de base minimum consiste en une **Adresse IP** et un **Masque de sous-réseau**.

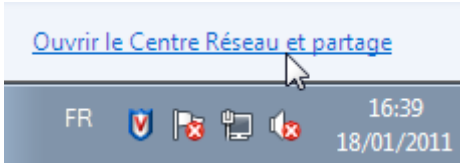


N.B : Pour l'identification du profil réseau Windows, une passerelle facilite les choses

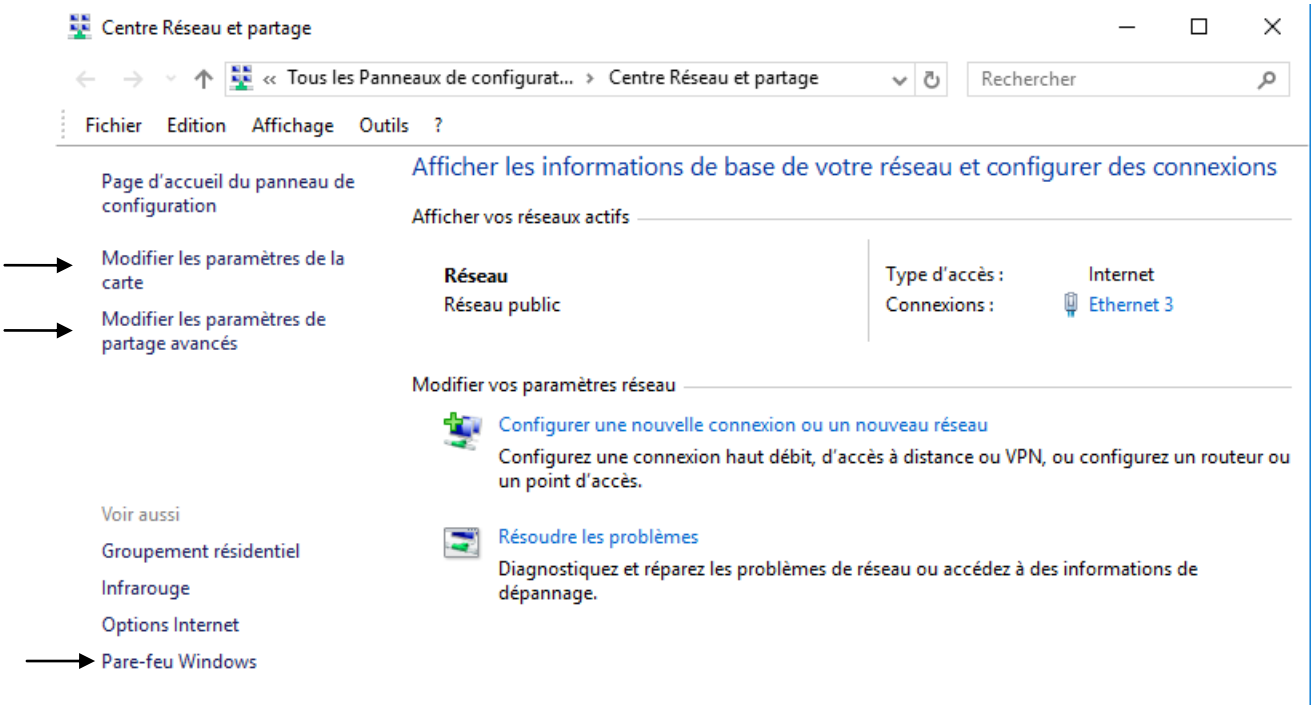
Si une carte réseau (minimum) est installée correctement, une icône « réseau » devrait apparaître en bas à droite…

Quel que soit l' aspect…

Un clic dessus puis « **Ouvrir le Centre Réseau et partage** »



Devrait amener



Modifier les paramètres de partage avancés / Profil – Type Réseau :

Sous Windows, on a toujours un « **profil réseau** »… Des que un réseau est détecté (pour ce faire il faut un adressage IP minimum, Adresse/Masque + Passerelle) alors il faut décider de son « type » parmi ceux proposés

De l'appartenance à tel ou tel type de réseau, découleront

- Les paramètres des partages avancés
- Les réglages du Pare-Feu

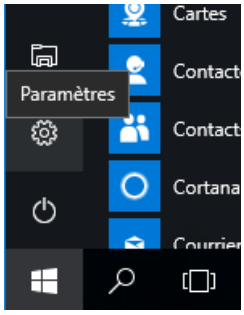
Il existe trois type de réseau au sens Windows mais l'utilisateur ne peut choisir que entre **Privé / Public** , car si **Domaine** existe, il ne peut être remis en cause:

- Domaine
- Privé
- Public

La différence entre **Public / Privé** c'est une différence des paramétrages par défaut des « partages avancés » et des règles du pare-feu.

Choisir un profil Réseau – Windows 10

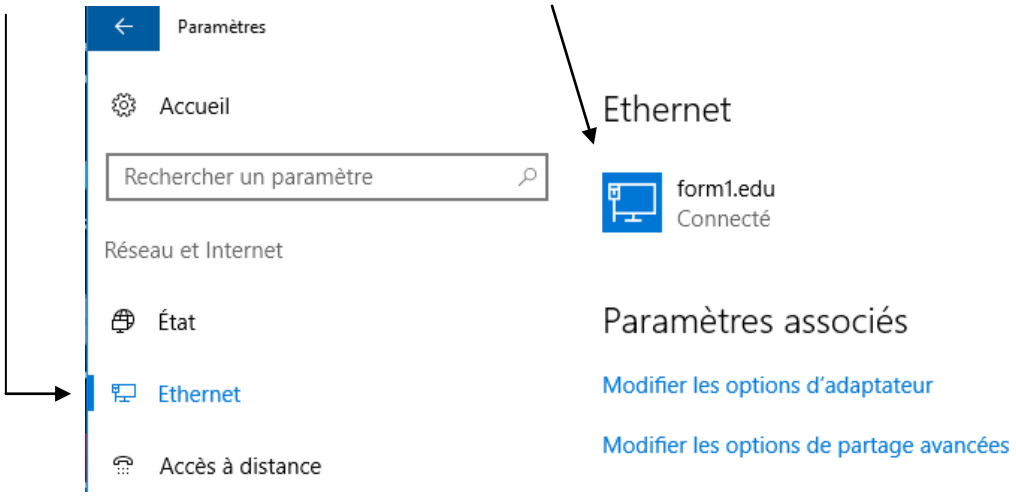
Si on n'est pas dans un domaine, alors on peut en cliquant sur **paramètre**



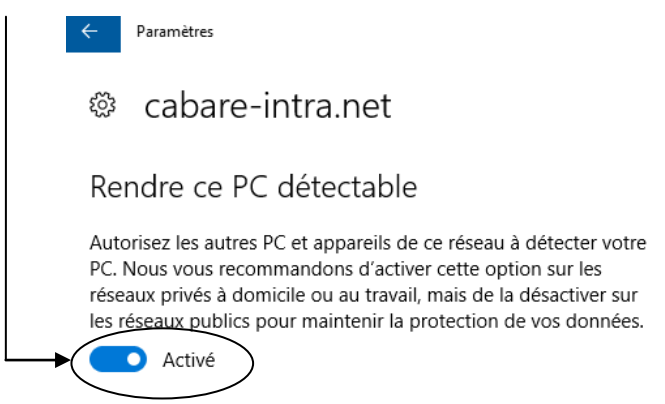
demander d'accéder aux réglage **Réseau et Internet**

On choisit notre connexion **Ethernet** sur la gauche

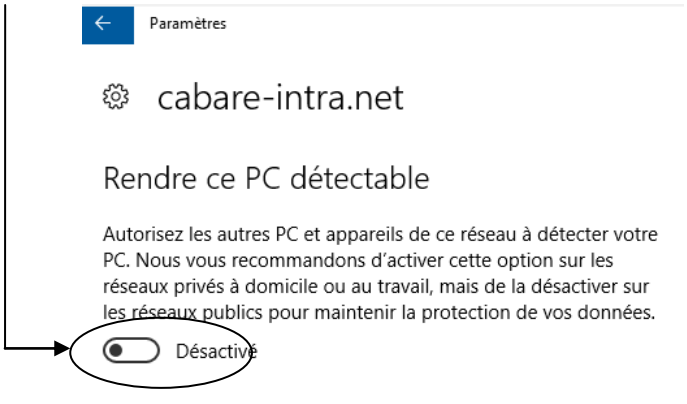
puis on clique sur notre liaison



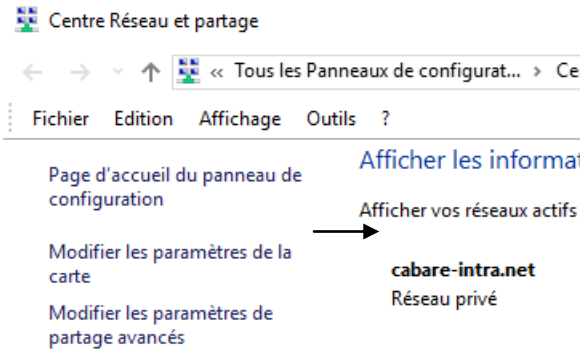
Mode **Privé**

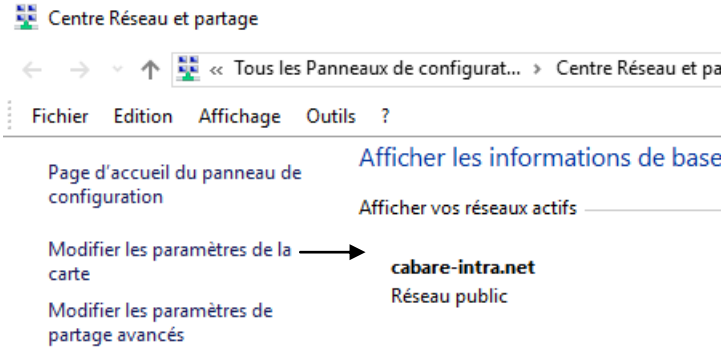


Mode **Public**

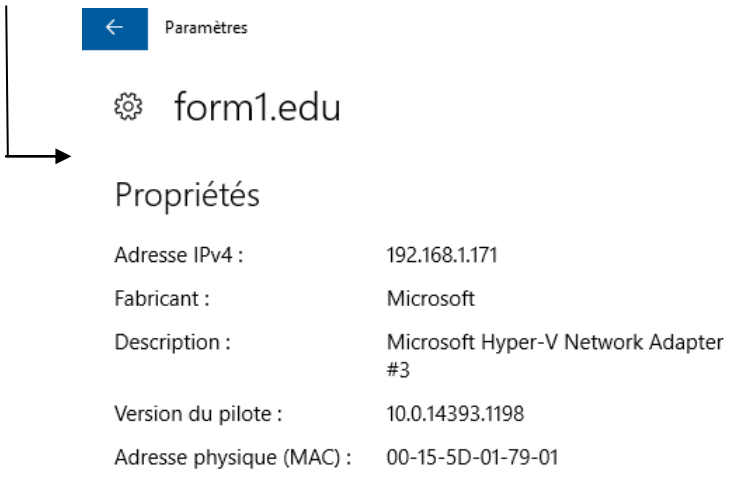


avec



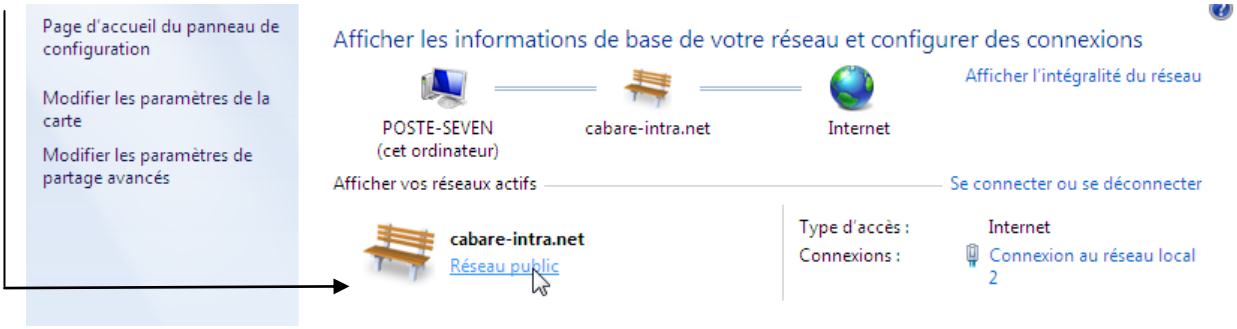


N.B : sur un réseau en domaine, ce bouton bascule n'apparaît pas

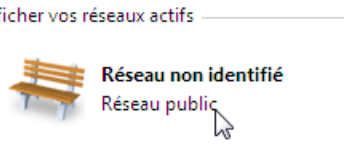


Choisir un profil Réseau - Seven

Si on n'est pas dans un domaine, alors on peut en cliquant sur le type de réseau en cours… choisir le nouveau profil réseau.

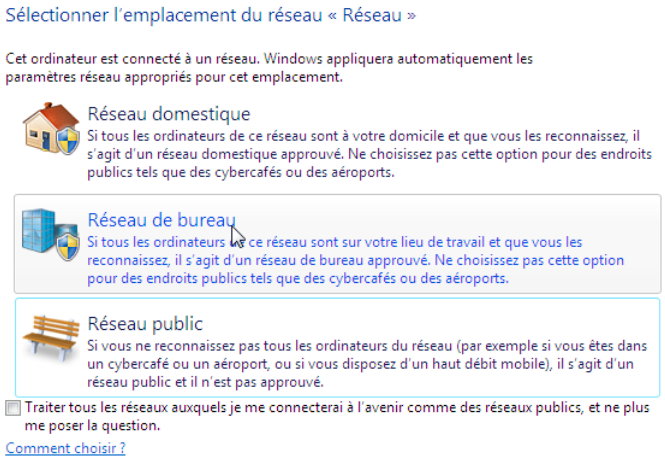


N.B: Si **Réseau non identifié** s'affiche, une passerelle sera la bienvenue…!

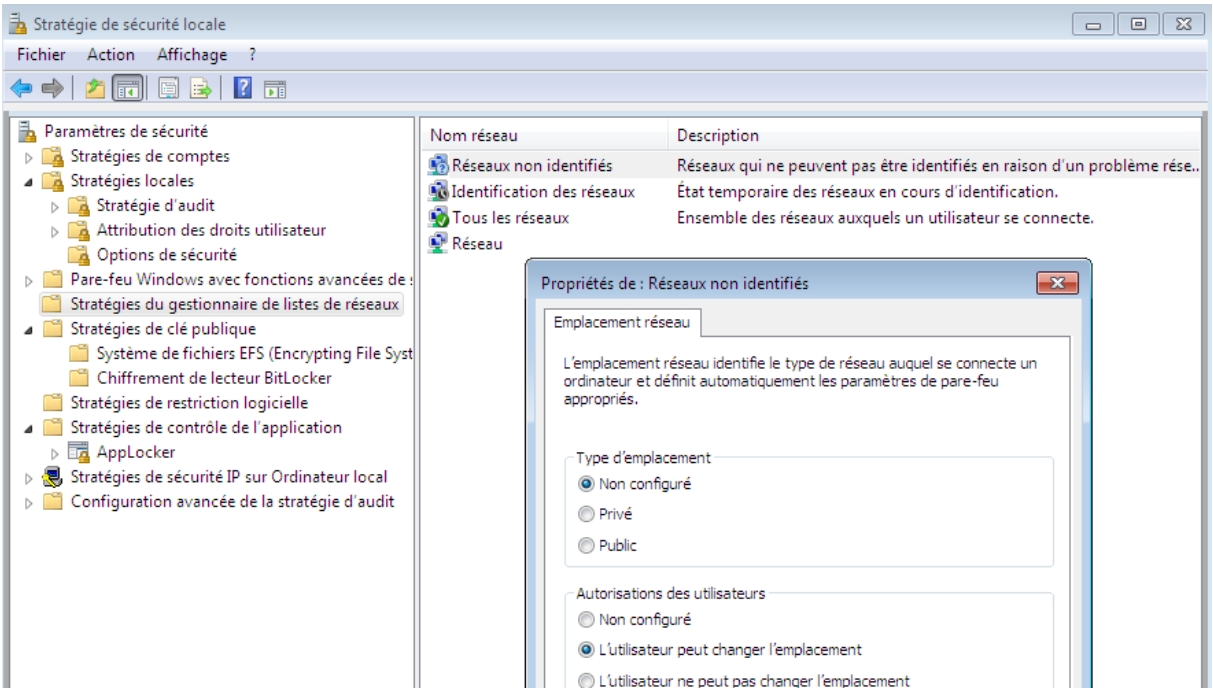


Car dans ce cas on ne peut pas changer de profil…

Dès que l'on donne une adresse IP en passerelle, cela débloque la détection, et Windows nous demande de choisir un profil



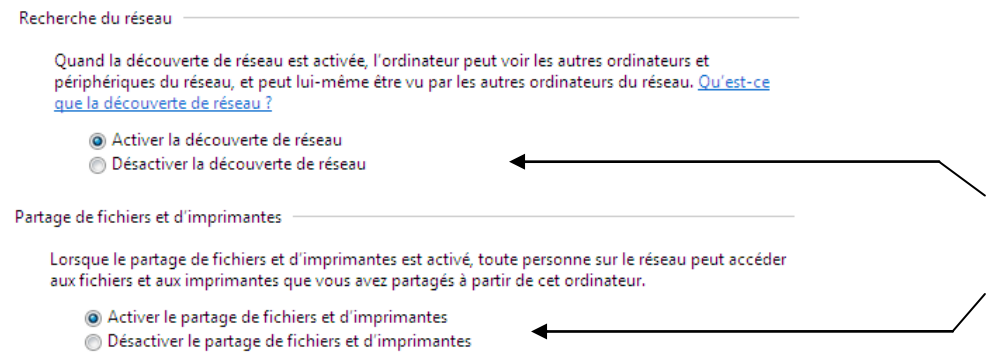
Cet état de fait est réglable dans les stratégies locales de sécurité, dans les Stratégies du gestionnaire de liste de réseaux …



Paramètres Partage Avancé Windows

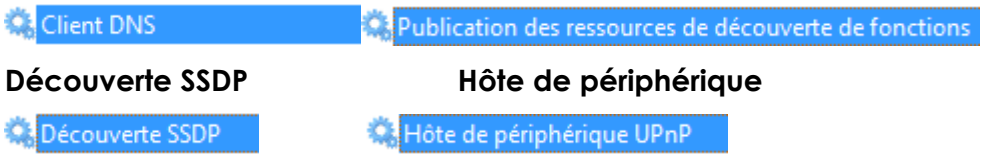
Réglage Disponibles:

Les réglages suivants existent selon les profils réseaux… Surtout

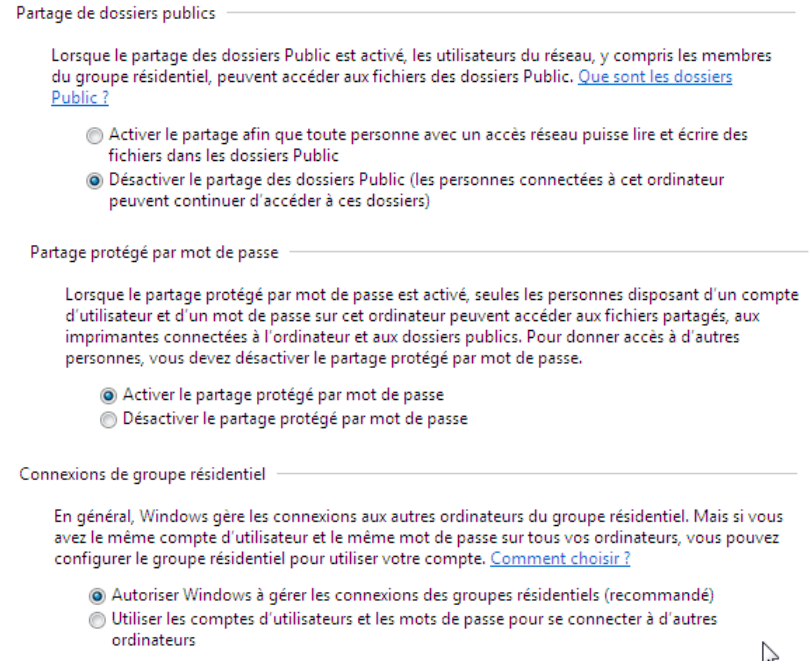


Pour que cela soit possible, il faut absolument que les 4 services suivants soient démarrés sur le poste (ce qui n'est pas toujours le cas):

Client DNS

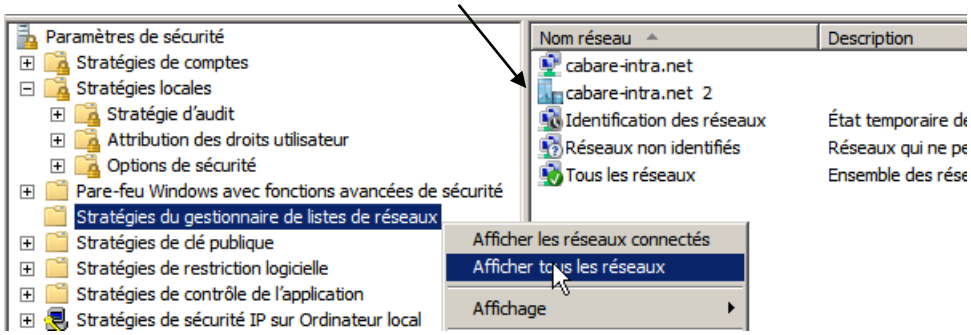


Tout le reste ne devrait pas être activé…



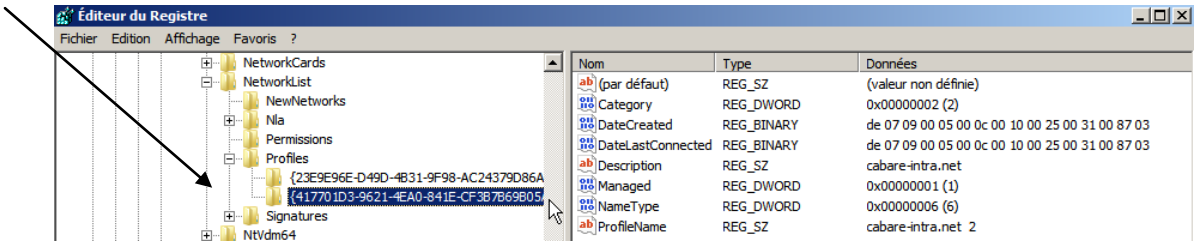
Listes des réseaux identifiés

N.B : la liste de tous les réseaux détectés par Windows se trouve en demandant la **stratégie du gestionnaire de liste de réseaux / Afficher tous les réseaux**



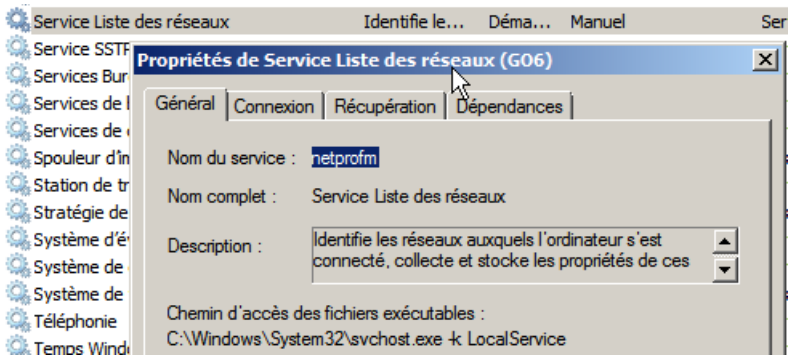
N.B : la liste des réseaux détectés par Windows est stockée en dans la base de Registre en

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles



Category valant **0** — Public Network -**1** Private Network **2** Domain Network

Le service qui gère les réseaux est Service Liste des réseaux

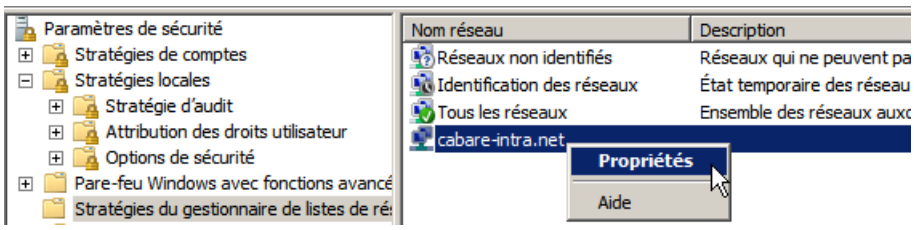


Pour faire un Reset de la situation il peut être necéssaire de

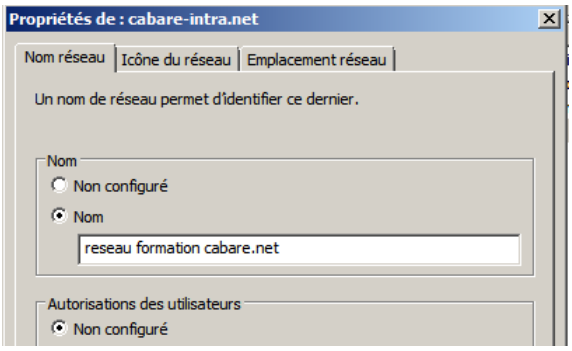
- Désactiver la carte réseau
- Modifier l'adressage IP
- Purger les **NetworkList\Profiles** de la base de registre
- Re-demarrer le service Service Liste des réseaux
- Réactiver la carte réseau

Personnaliser le réseau de domaine

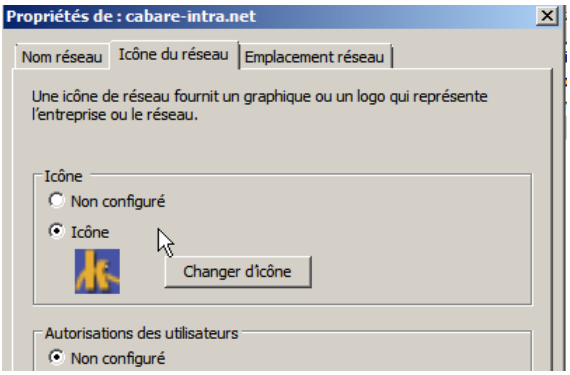
On souhaite personnaliser le type de réseau de domaine en **privé** avec un non qui soit parlant, et non modifiable… Une fois la connection correctement prise, on peut paramétrer le « réseau »



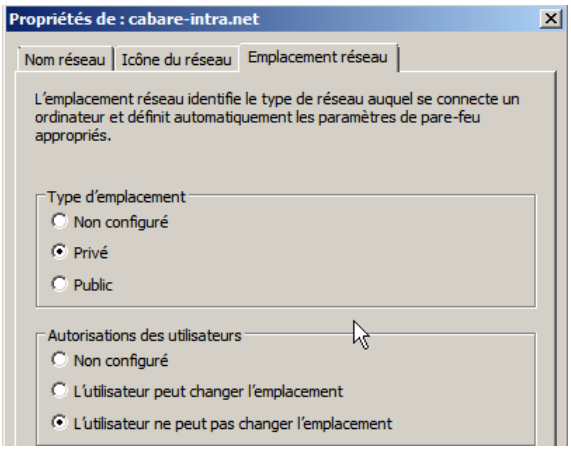
Nouveau nom



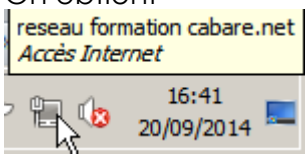
Logo perso



Type Privé et non modifiable



On obtient

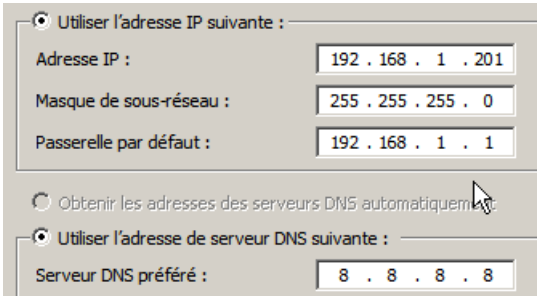


avec

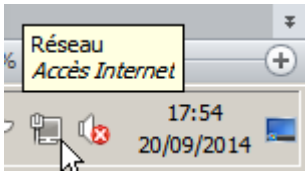
Et si on essaye de modifier le type de réseau en public, on a un message d'erreur

Personnaliser un réseau « google »

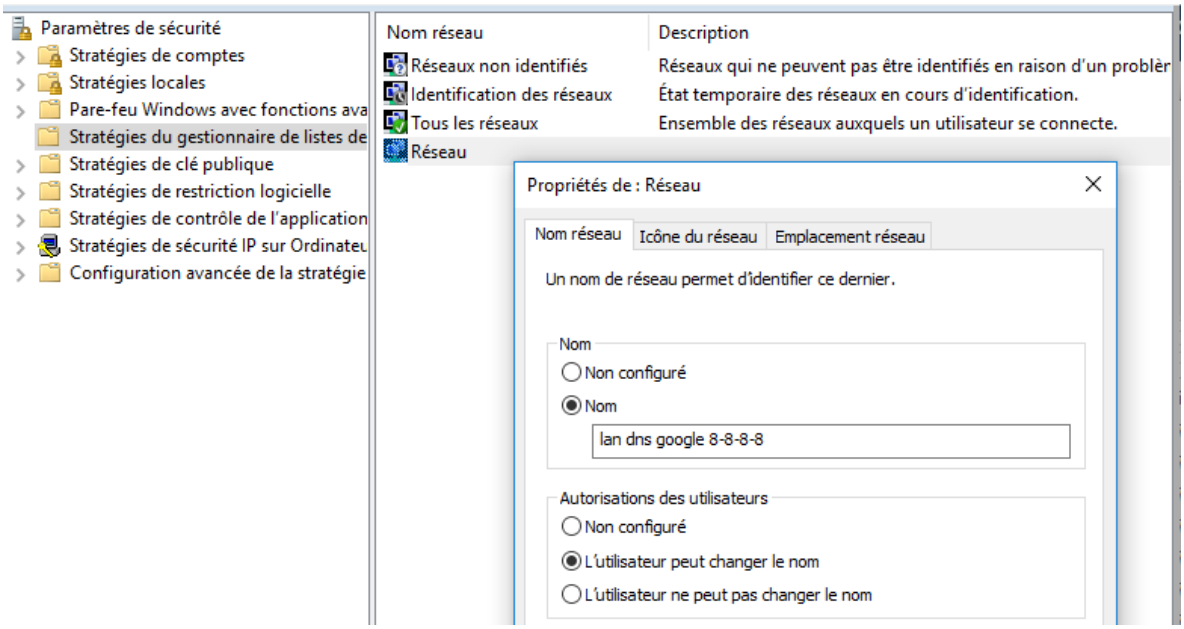
On souhaite personnaliser un réseau anonyme, donc par défaut public et modifiable par l'utilisateur



Ce type de réseau est analysé puis nommé …puis classé en public non modifiable



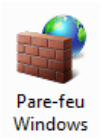
Via la GPO Stratégie du gestionnaire de liste de résaux onglet Nom réseau



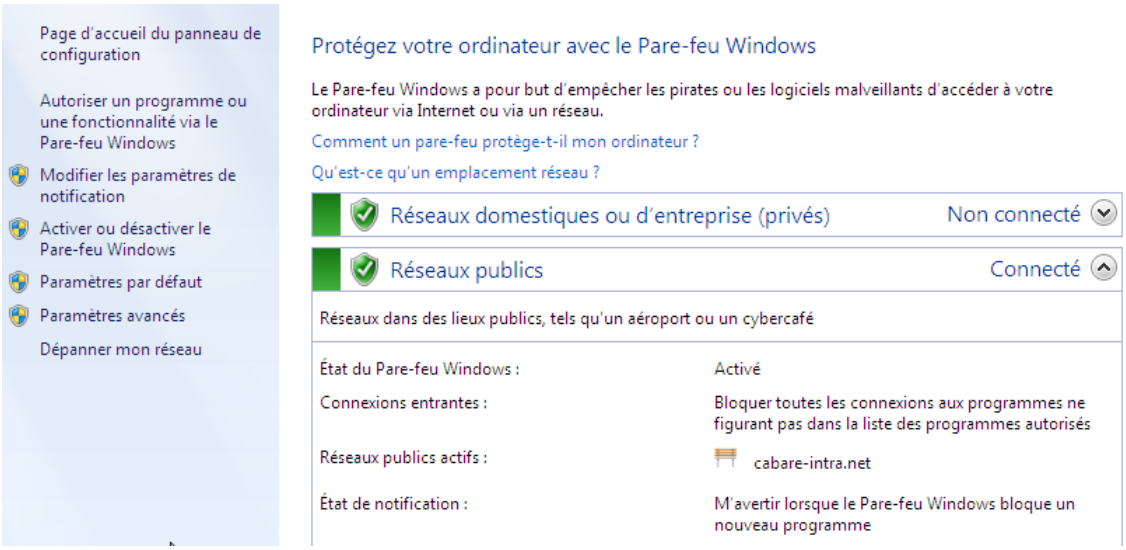
PARE-FEU WINDOWS

Principe Activation - Désactivation

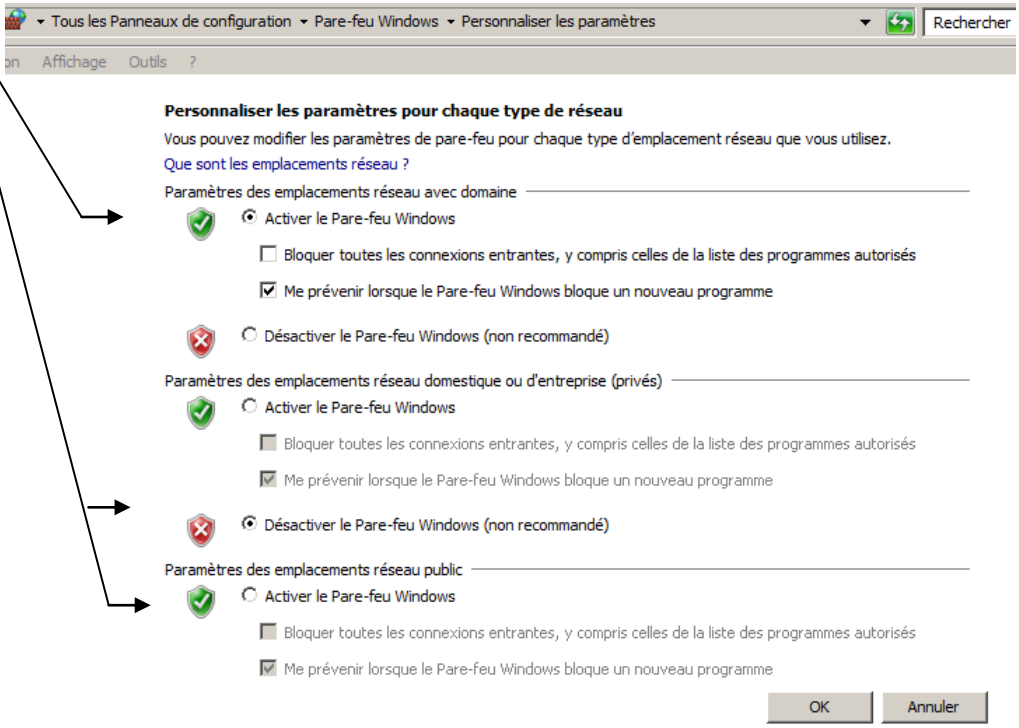
L'accès standard, permettant l'activation ou la désactivation, et la gestion de quelques exceptions « prévues », se trouve dans le



Panneau de Configuration / Pare feu Windows

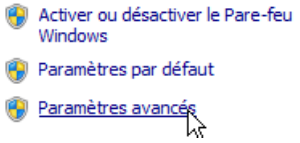


On peut **Activer – Désactiver** selon les 3 profils existants… public, privé, domaine



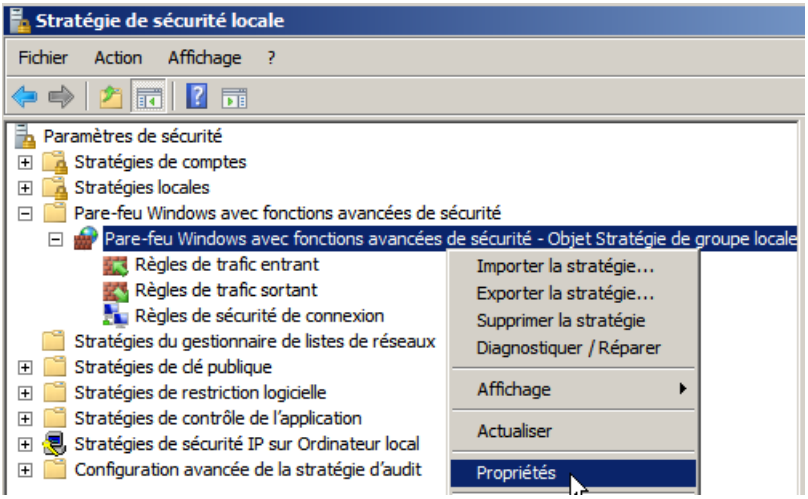
Version Avancée :

La version avancée, permettant des réglages plus fins, (règles entrantes, sortantes) est disponible via les **Paramètres avancés** du Pare-feu standard…

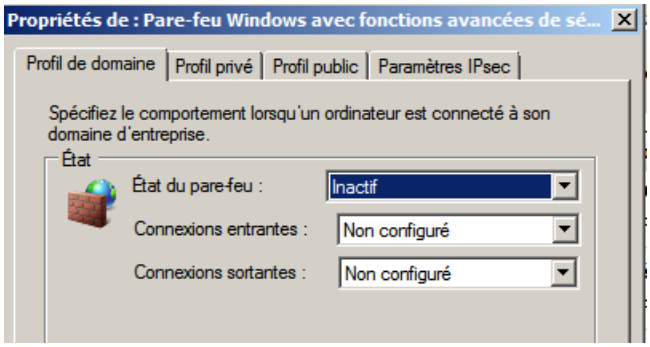


Définie 1 stratégies Pare-Feu

On peut définir une stratégie via les GPO locales, Paramètres de Sécurité, Pare-feu Windows avec fonctions avancées de Sécurité / Propriétés



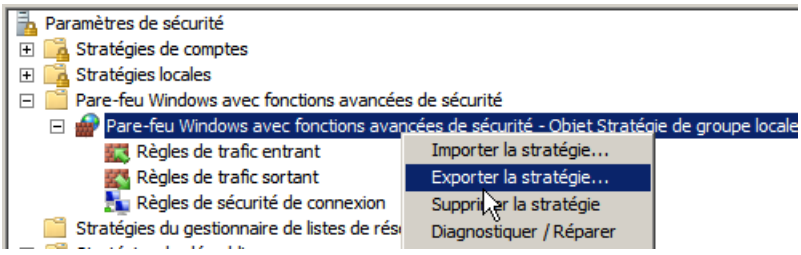
On va inactiver le pare-feu pour ses 3 Profils…(domaine – Privé – Public)



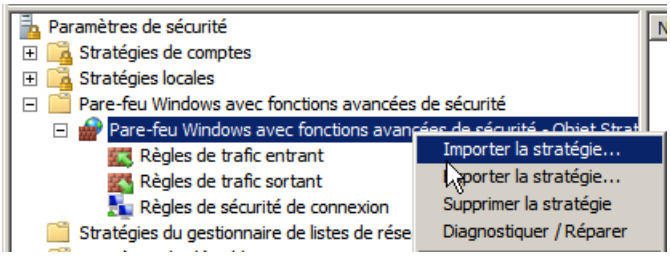
Exporter Importer 1 stratégies Pare-Feu

Exporter une stratégie :

On peut importer ou exporter une configuration de pare-feu via des fichiers ….**wfw** spécifiques: cela marche à partir de **Seven** et **2008**…



L'importation se fera de manière très similaire



GPO personnalisée Pare-Feu et Règle

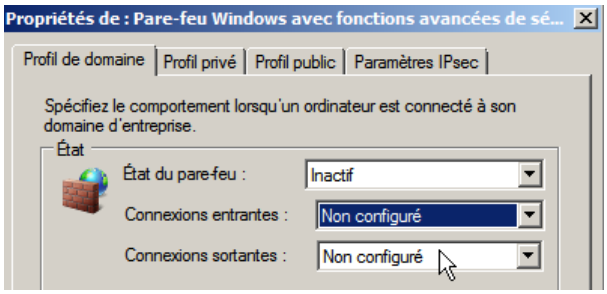
On va créer une stratégie permettant d'obtenir :

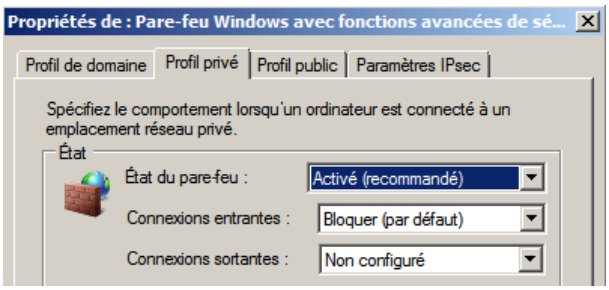
Pour le **Profil Domaine** la désactivation du Pare-feu

Pour le **Profil Public et Privé** l'activation du Pare-feu

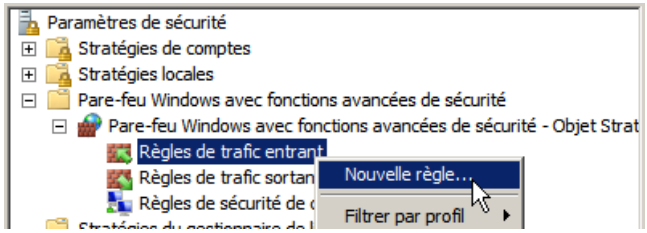
avec une règle autorisant les connexion entrantes ICMP (requête ECHO sur un PING)

Armement Pare Feu:

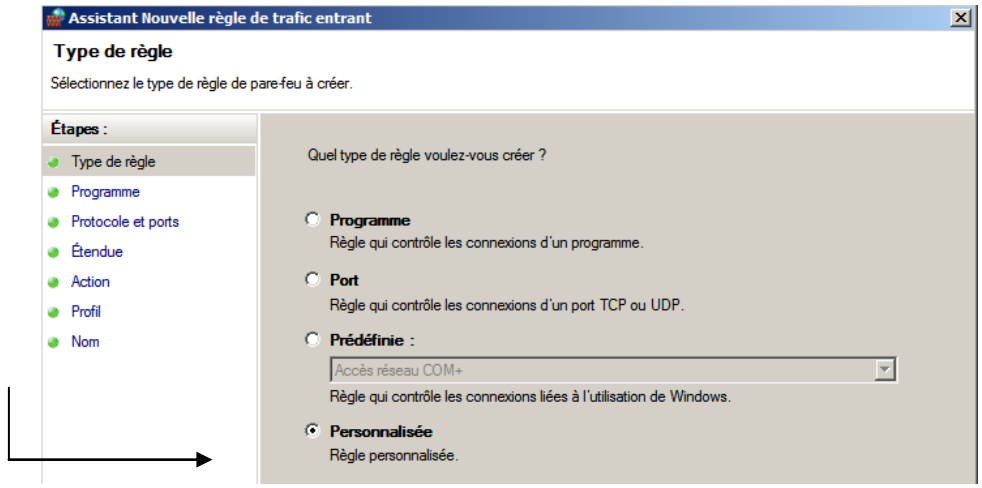




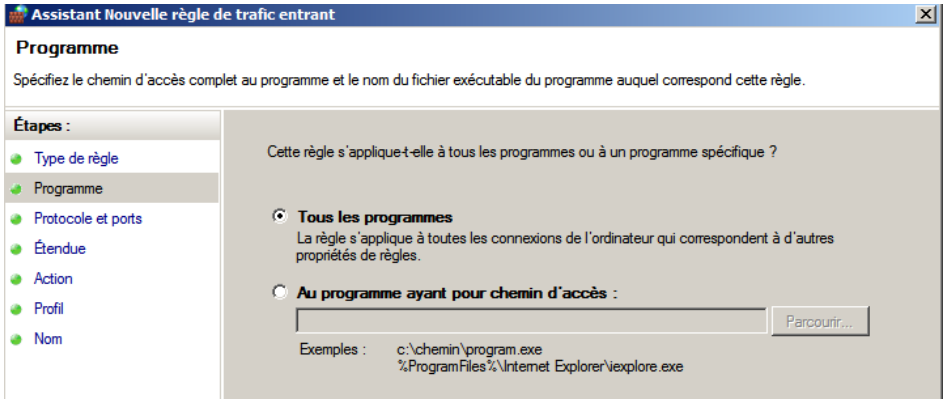
Règles entrantes personnelles:



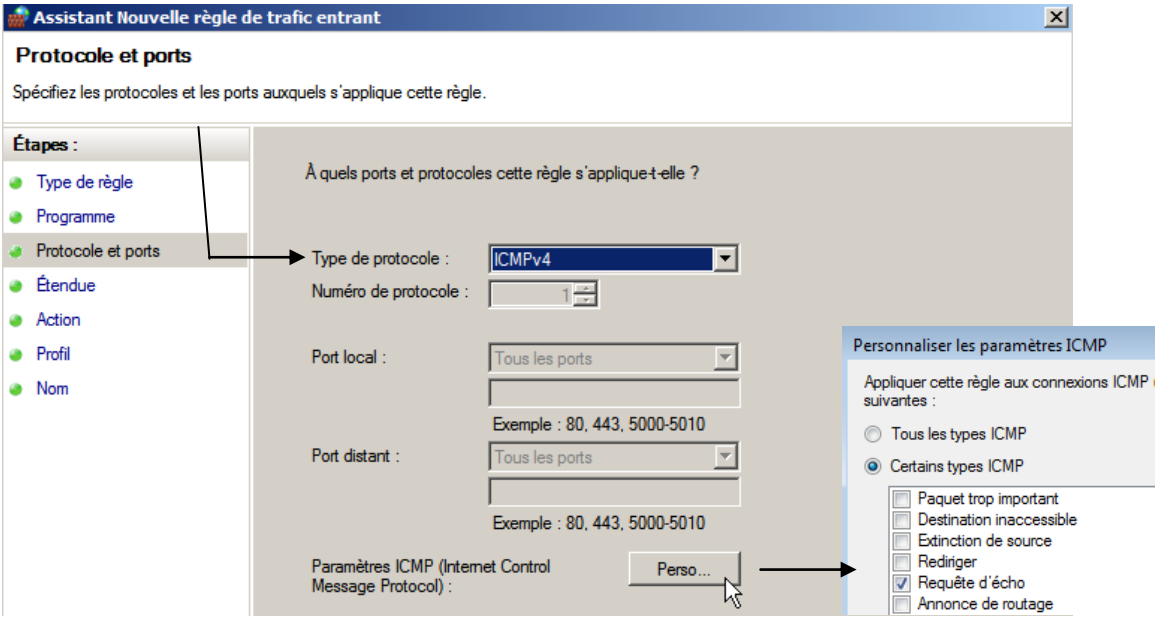
On demande Personnalisée



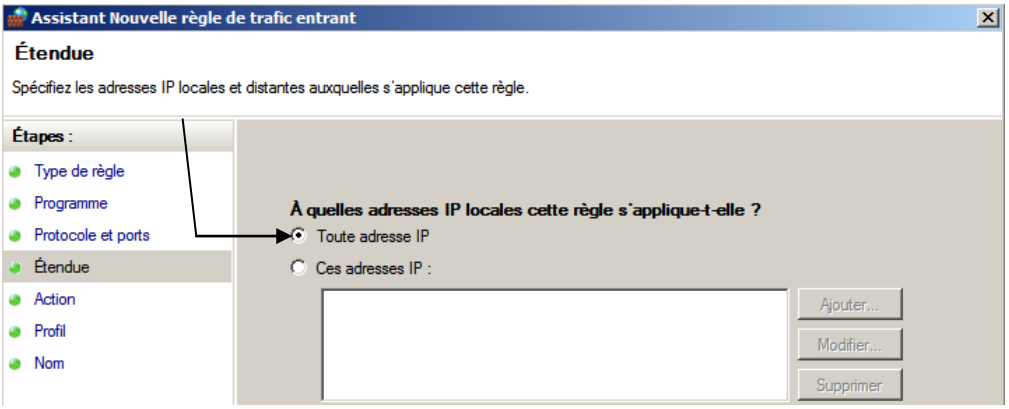
Puis Tous les Programmes



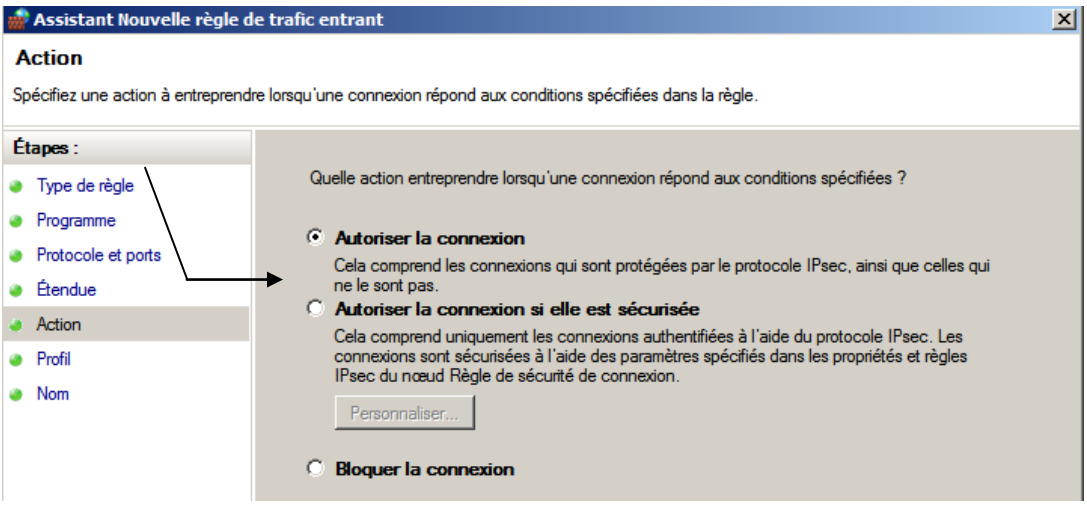
On affine les réglages ICMPv4 requête ECHO



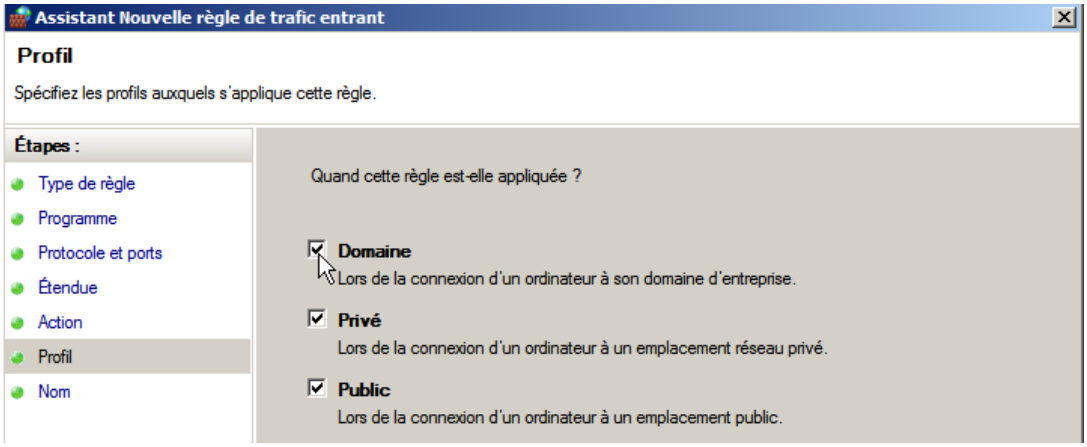
On spécifie les adresses ip éventuellement concernées



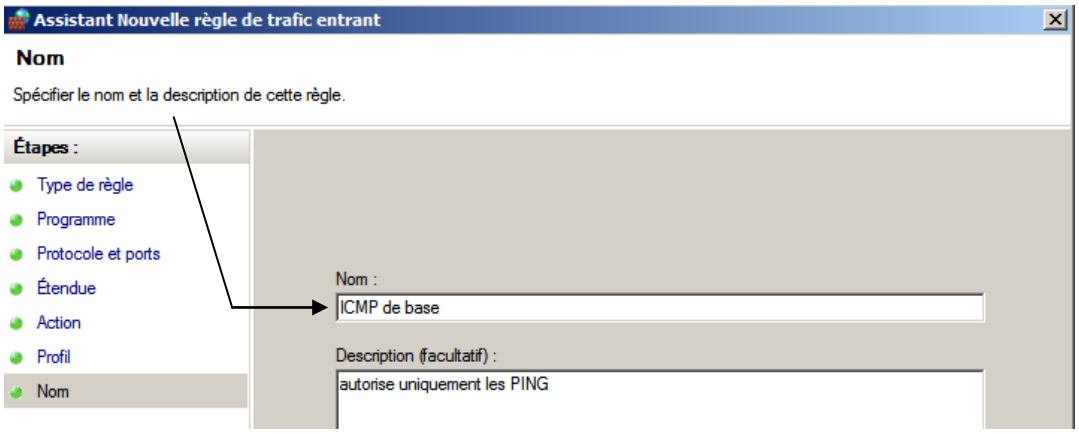
Et le comportement de la règle, on Autorise la connexion



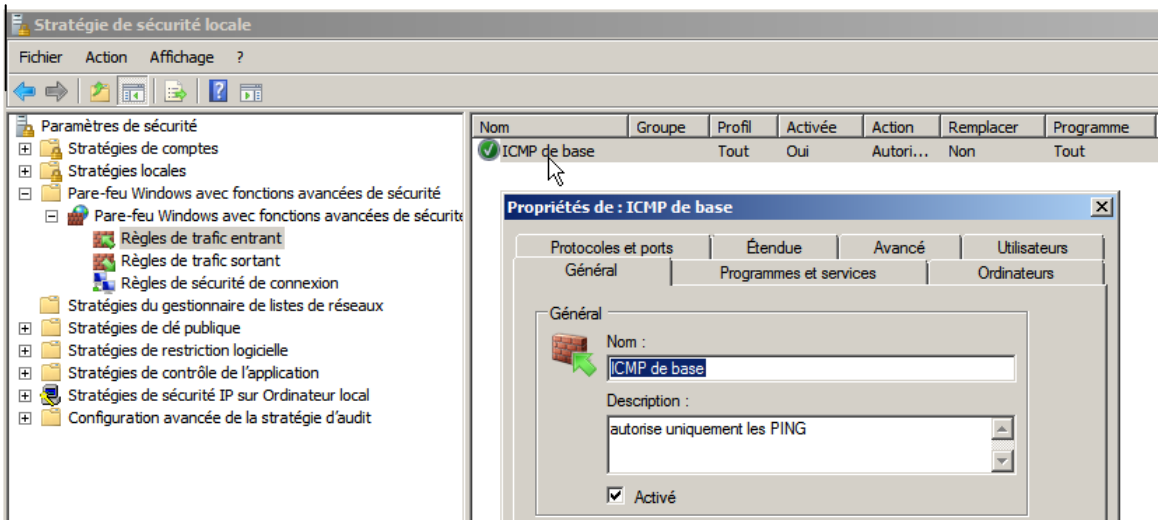
Selon le profil réseau



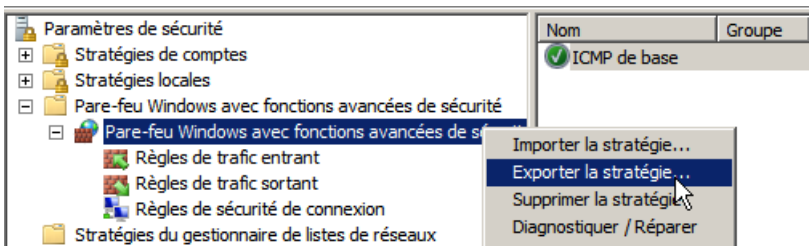
Il ne reste plus qu'a lui donner un nom



Et voici notre nouvelle règle !



Et il n'y a plus qu' exporter la règle…



Netsh Export Import configuration Pare-Feu

On peut **importer / exporter** une configuration de pare-feu stockée dans un fichier **wfw** par batch via **netsh**

```
C:\Users\Administrateur>netsh advfirewall export /?

Utilisation : export <chemin\nom_fichier>

Remarques :

      - Exporte la stratégie actuelle vers le fichier spécifié.

Exemple :

      netsh advfirewall export "c:\advfirewallpolicy.wfw"
```

Donc par exemple

```
C:\Users\Administrateur>netsh advfirewall export "d:\export.wfw"
Ok.
```

Un reset du pare-feu peut se faire via

```
C:\Users\Administrateur>netsh advfirewall reset /?

Utilisation :  reset [export <chemin d'accès\nom de fichier>]

Remarques :

      - Restaure la stratégie par défaut du Pare-feu Windows avec
        la stratégie Sécurité avancée.  La stratégie active actuelle peut
        être exportée en option vers un fichier spécifié.
      - Dans un objet de stratégie de groupe, cette commande rétablit tous
        les paramètres notconfigured et supprime toutes les règles
        de pare-feu et de sécurité de connexion.

Exemples :

      Sauvegarder la stratégie actuelle et restaurer la stratégie prête à
      l'emploi :
      netsh advfirewall reset export « c:\backuppolicy.wfw »
```

Un armement du pare-feu en important un fichier de configuration **.wfw** peut se faire via

```
C:\Users\Administrateur>netsh advfirewall import /?

Utilisation : import <chemin\nom_fichier>

Remarques :

      - Importe une stratégie à partir du fichier spécifié.

Exemple :

      netsh advfirewall import "c:\newpolicy.wfw"
```

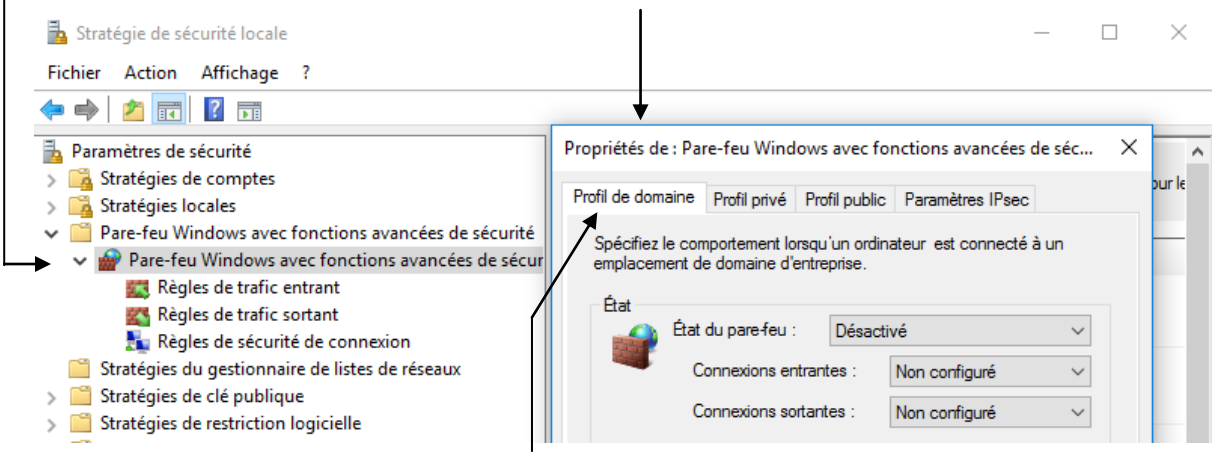
Donc par exemple

```
C:\Users\Administrateur>netsh advfirewall import "d:\export.wfw"
Ok.
```

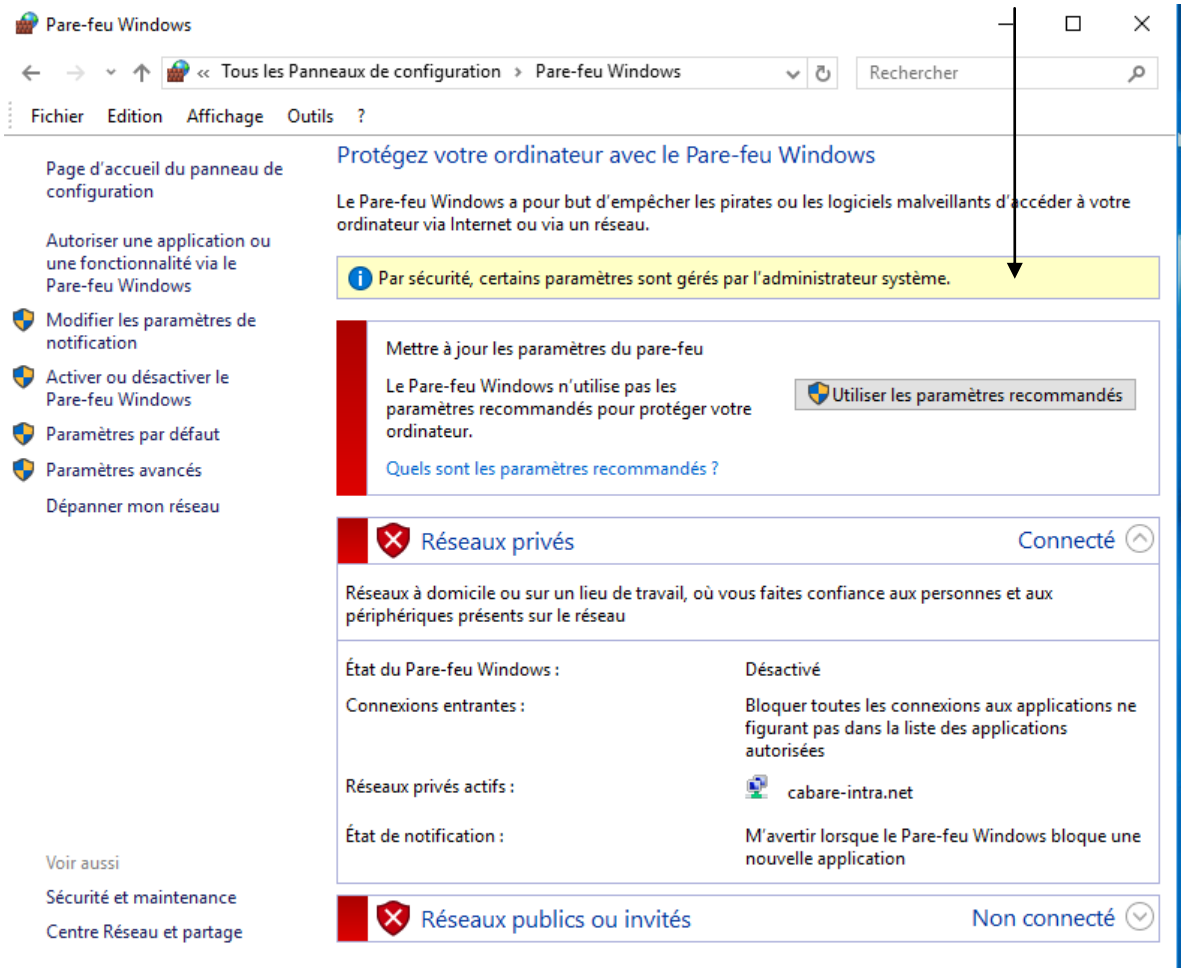
Stratégie Locale Désactivation Pare-feu

Cela peut se faire via le Panneau de configuration – Outils d'administration, Stratégies locales Puis Pare-feu avec fonctions avancées de sécurité

On se place sur pare-feu et on demande les propriétés via clic droit



On désactive l'état du pare-feu pour les 3 profils possibles, et on aura bien

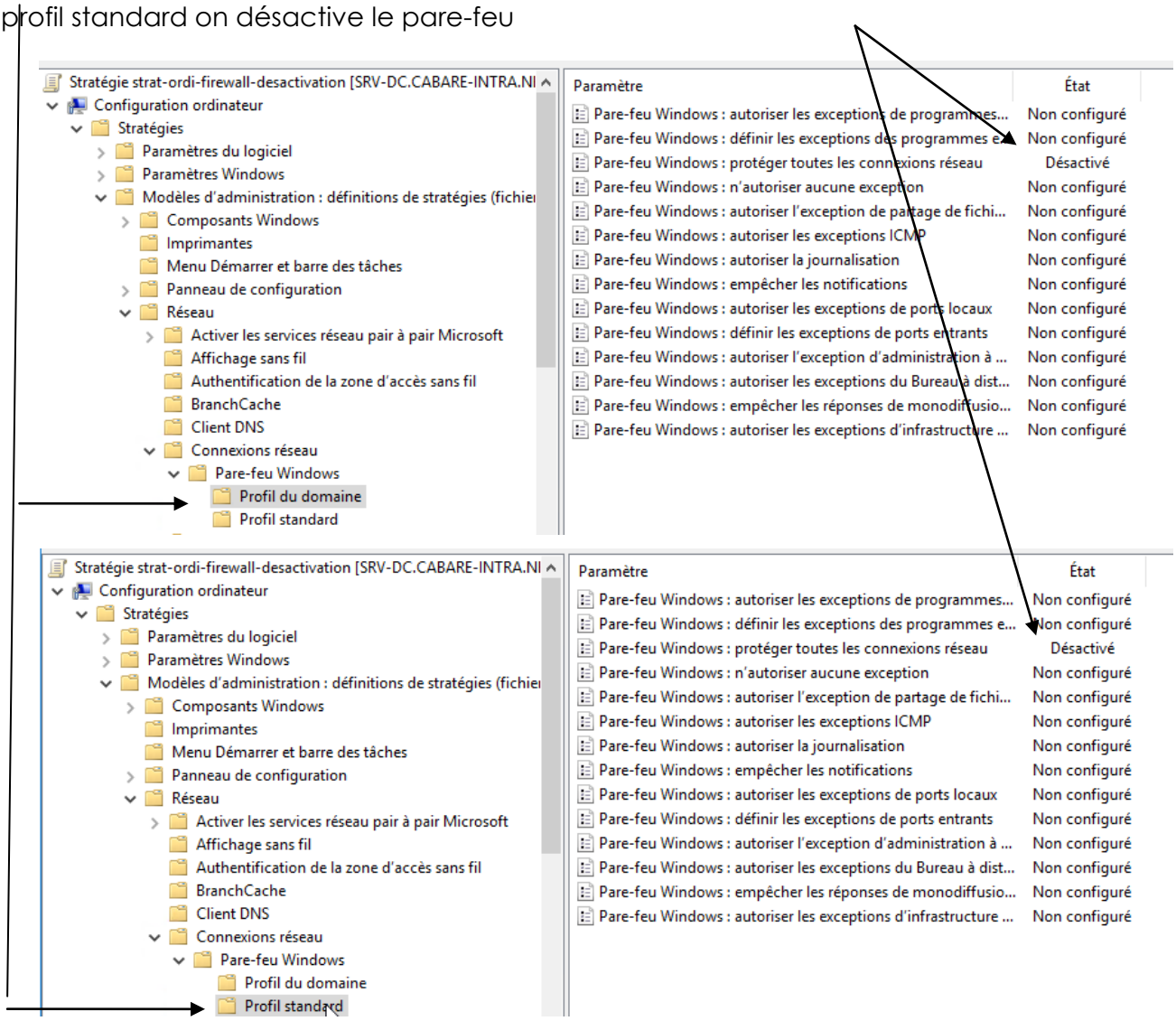


N.B : Mais l'administrateur local pourra toujours retourner dans les stratégies locales et re-activer le Pare-feu !

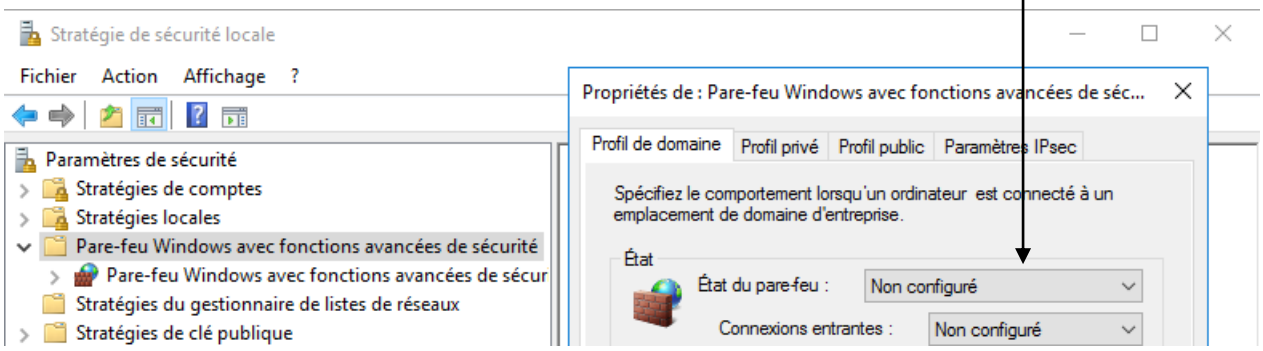
GPO Désactivation Pare-feu (aperçu)

Si on fait cela via une **GPO** de **domaine :**

Configuration ordinateur / modèles d'administration / Réseau Puis Connexions réseau / Pare-feu Windows puis dans les 2 réglages selon le profil du domaine et le profil standard on désactive le pare-feu



N.B : Mais l'administrateur local ne pourra plus aller dans les stratégies locales pour tenter de re-activer le Pare-feu ! Elles apparaîtront carrément comme **Non configurées** !



LGPO SEVEN - 10

Contexte

Soit une machine Seven native en Workgroup, avec 4 utilisateurs respectivement

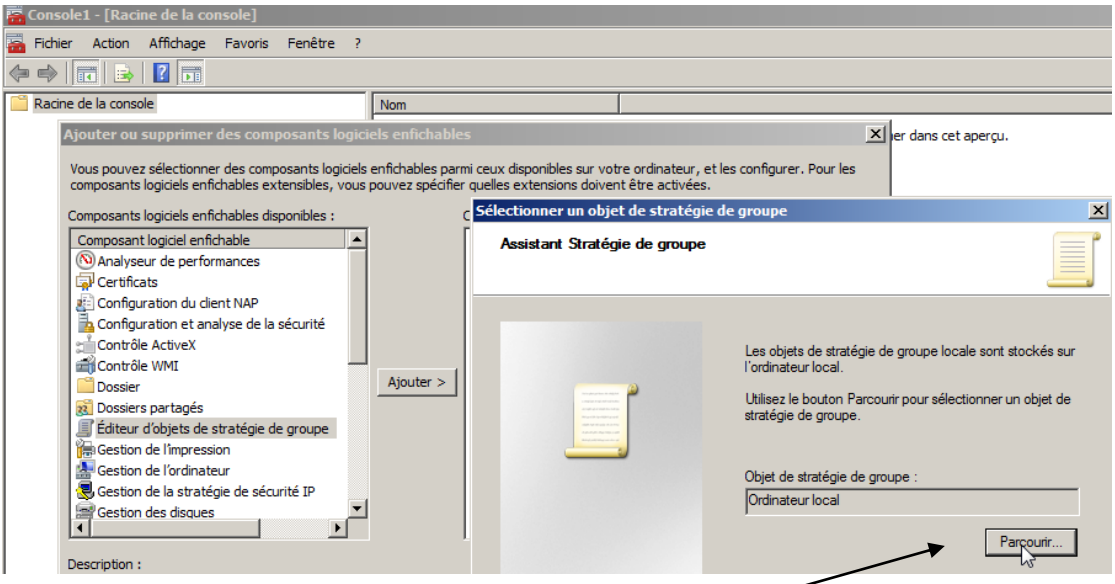
- **bob/b** utilisateur
- **toto/t** utilisateur
- **admin/local** membre des Administrateurs
- **administrateur** Compte administrateur intégré ré-activé

on souhaite faire 3 MLGPO gérant respectivement l

- **les administrateurs**, (Admin et Administrateur en font partie) : on veut
  le menu executer disponible
  effacer l'historique des documents ouverts
  paramétrer un écran de veille avec un mot de passe
- **les non -administrateurs**, (Bob et Toto en font partie) : on veut
  empêcher l'accès au panneau de configuration
  supprimer la corbeille du bureau
- **bob**, : on veut
  empêcher de modifier sa page de démarrage dans IE

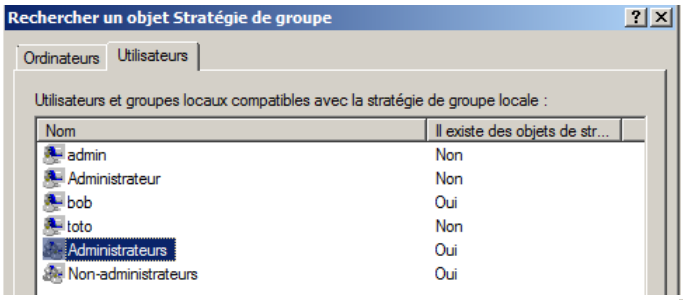
MLGPO pour administrateurs

On crée donc une **mmc Editeur d'objet de stratégies de groupe**

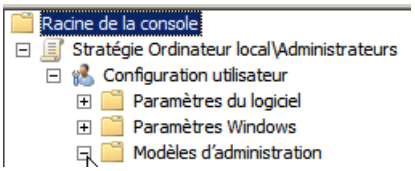


On demande parcourir

pour les **Administrateurs**

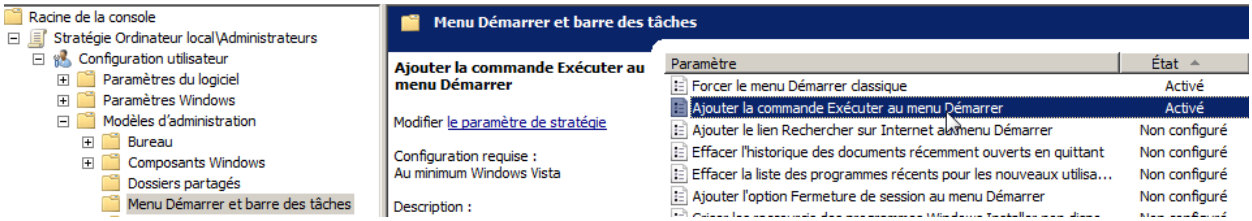


Les réglages se trouvent dans

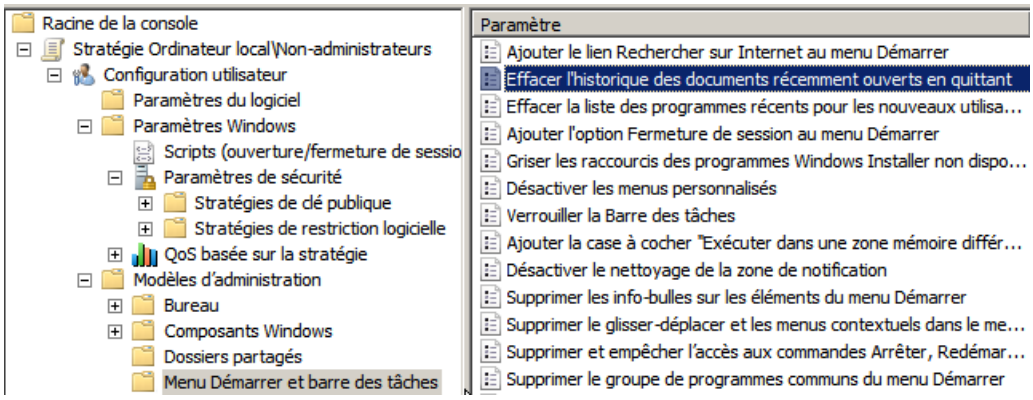


Stratégie Ordinateur local \Administrateurs - Configuration utilisateur - Modèles d'administration

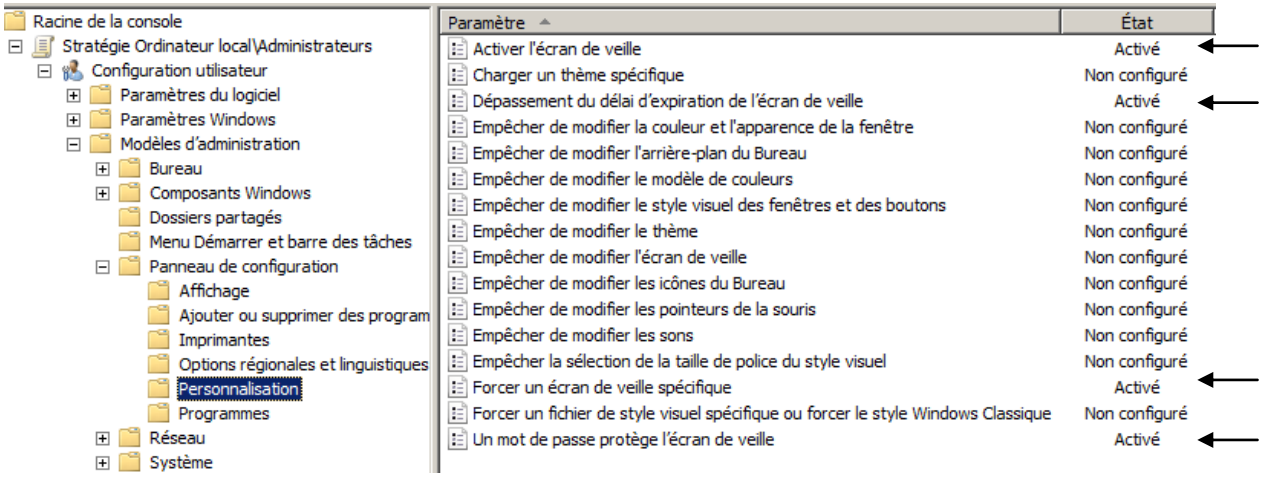
Ajouter la commande executer au menu démarrer



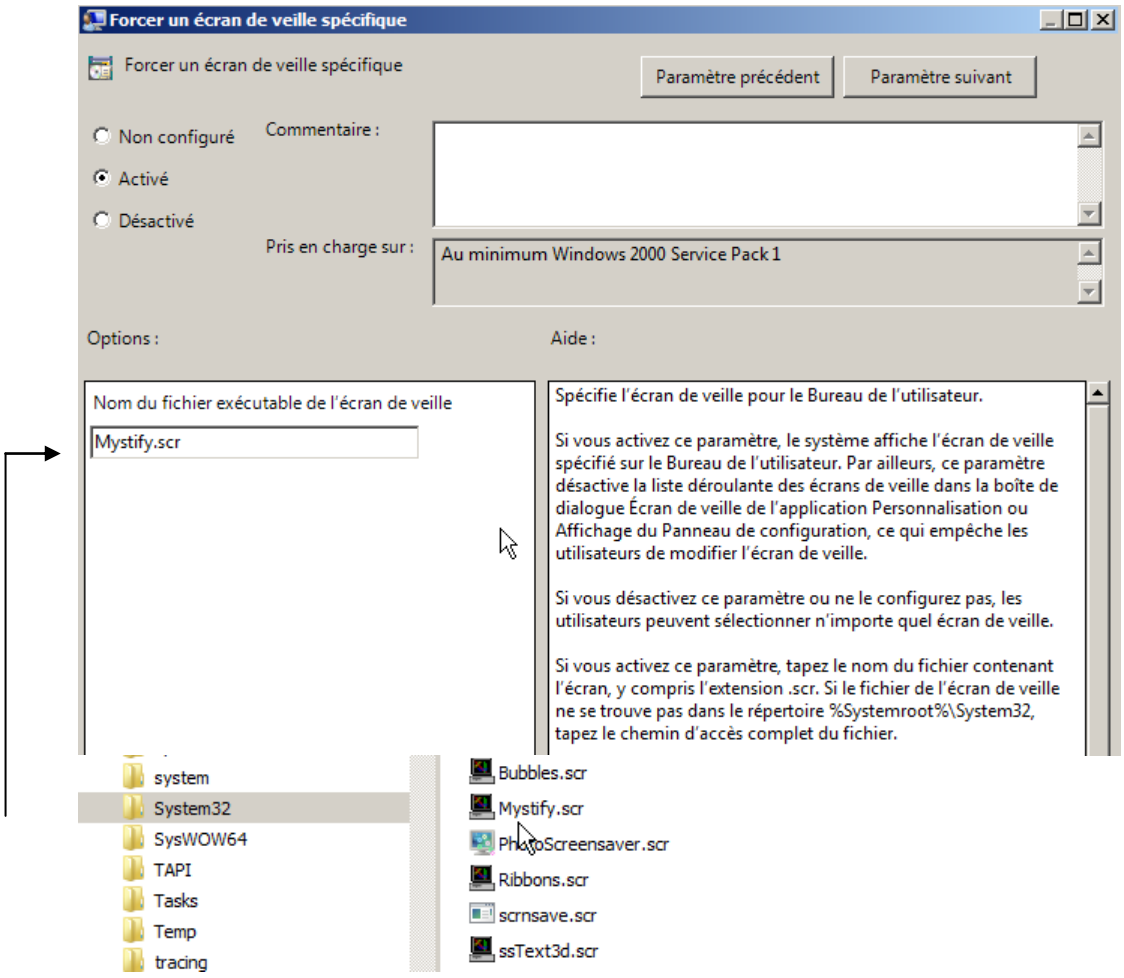
Effacer l'historique des documents récemment ouvert



Activer un écran de veille + associer un mot de passe + forcer un écran spécifique + définir le délais d'expiration

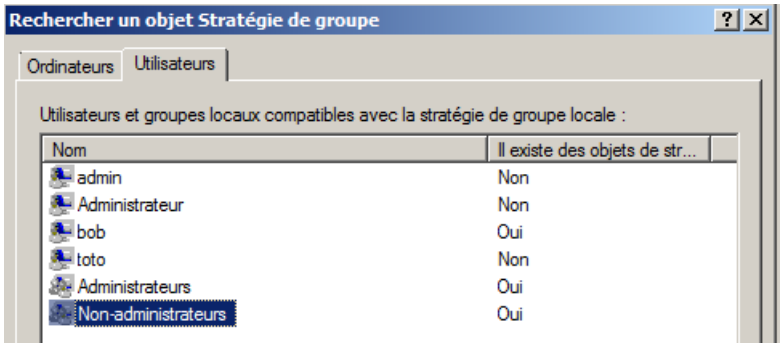


Avec un réglage un peu fin, c'est le nom du fichier economiseur d'écran , dont on sait que c'est un **.scr** stocké dans le dossier **system32**…



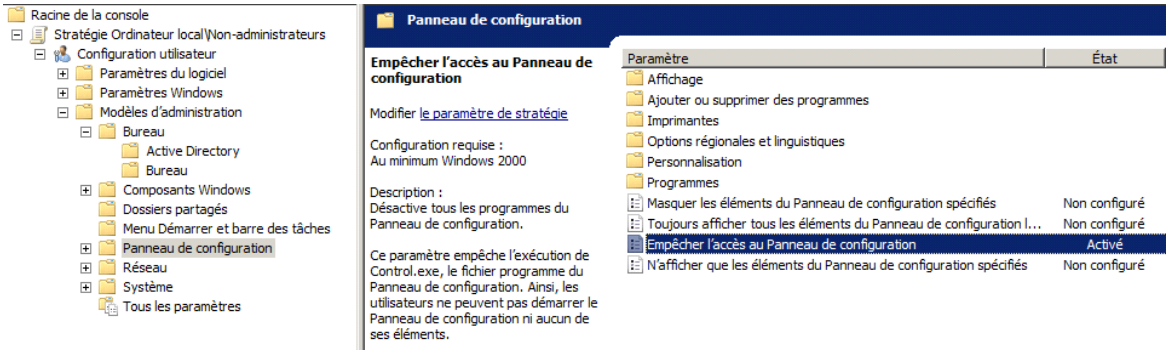
MLGPO pour non-administrateurs

on refait une console, mais en demandant cette fois-ci **Non-administrateurs**

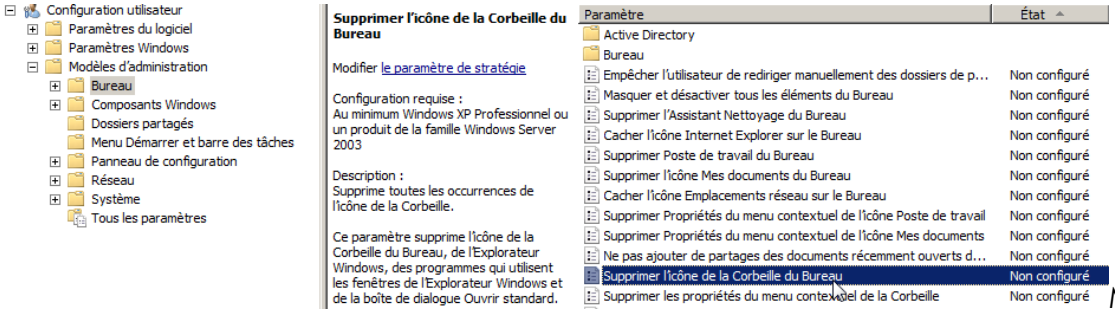


Modèles D'administration / Panneau de Configuration/

Empêcher l'accès au panneau de configuration

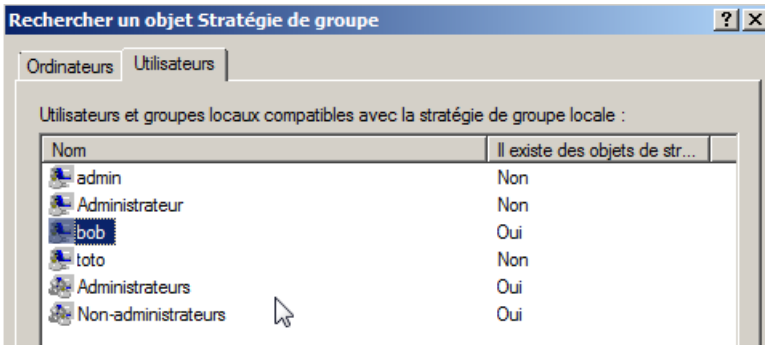


supprimer la corbeille



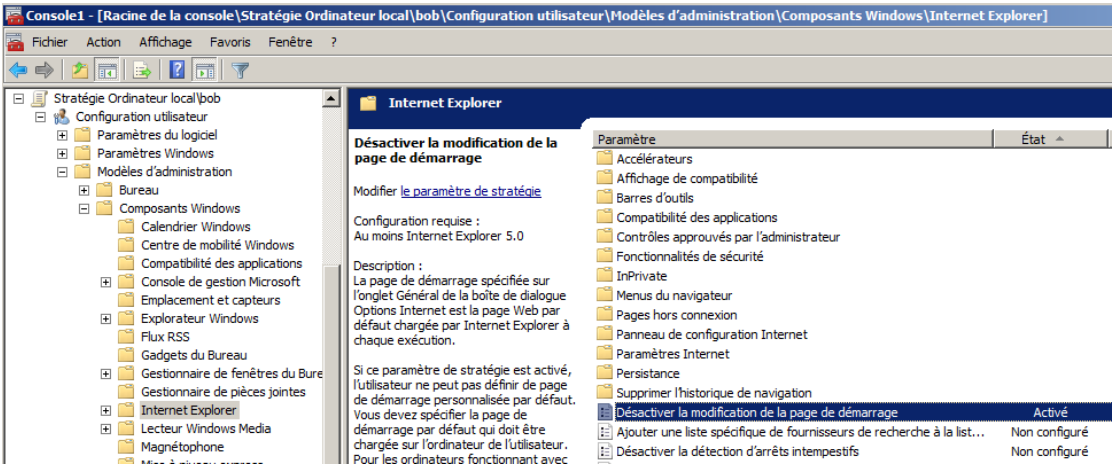
LGPO pour bob

on refait une 3° console, mais en demandant cette fois-ci **Bob**



Modèles D'administration / Composants Windows/

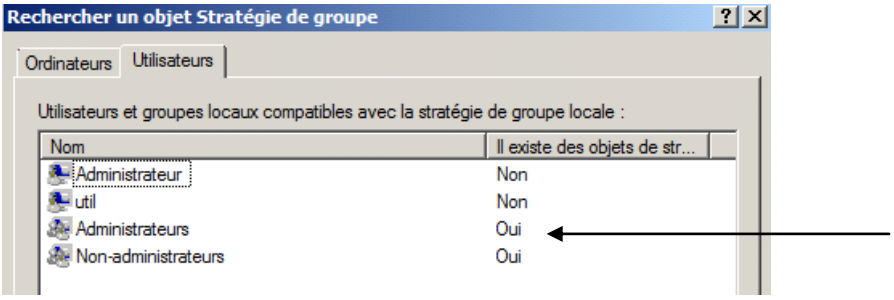
Internet Explorer / Désactiver la modification de la page démarrage



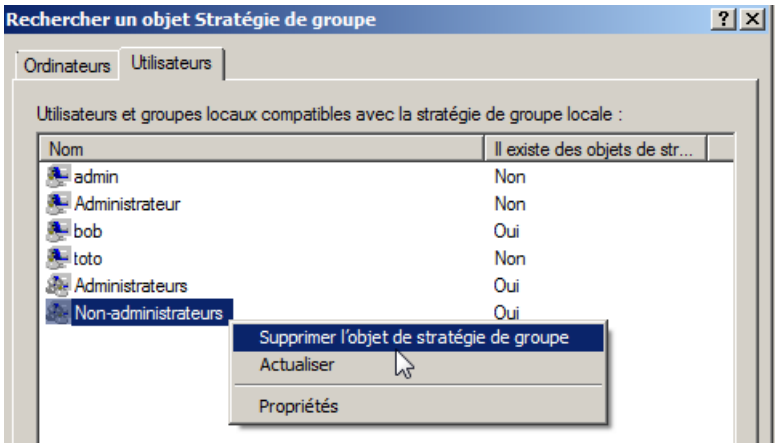
N.B: Attention Sous **Windows 10** à ne pas confondre **Edge** et **Internet Explorer**

Supprimer les MLGPO

Pour faire le ménage



le clic droit souris permet de Supprimer une **MLGPO**


Rechercher un objet Stratégie de groupe
Ordinateurs
Utilisateurs
Utilisateurs et groupes locaux compatibles avec la stratégie de groupe locale :
Nom
Il existe des objets de str...
admin
Non
Administrateur
Non
bob
Oui
toto
Non
Administrateurs
Oui
Non-administrateurs
Oui
Supprimer l'objet de stratégie de groupe
Actualiser
Propriétés

MONTAGE DOMAINE 2016-2012R2

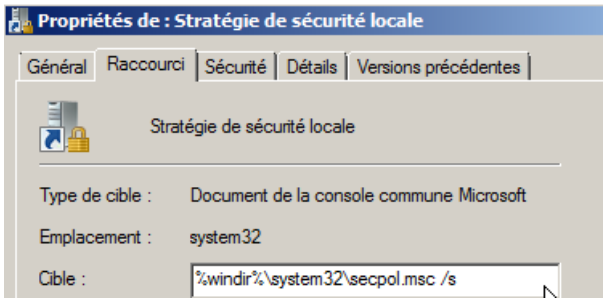
Montage d'un Contrôleur de Domaine sous 2016 - 2012 R2 :

Sur notre serveur 2016 2012R2 autonome :

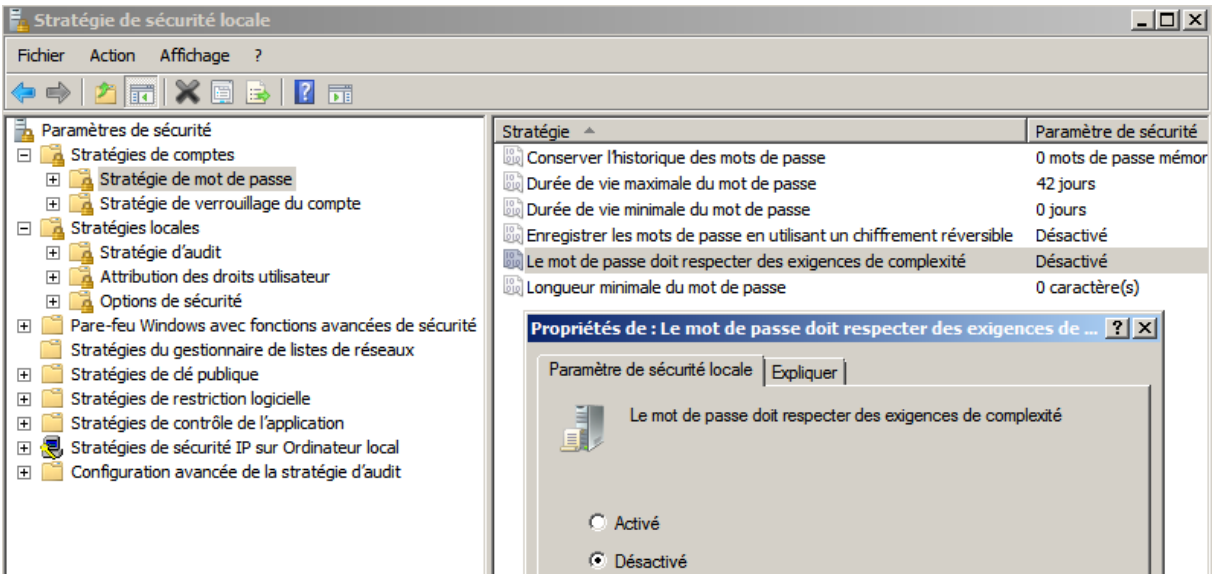
- Vérification du nom de serveur
- Vérification adressage Ip en ipv4 + passerelle + dns 8.8.8.8

Stratégies locales serveur autonome :

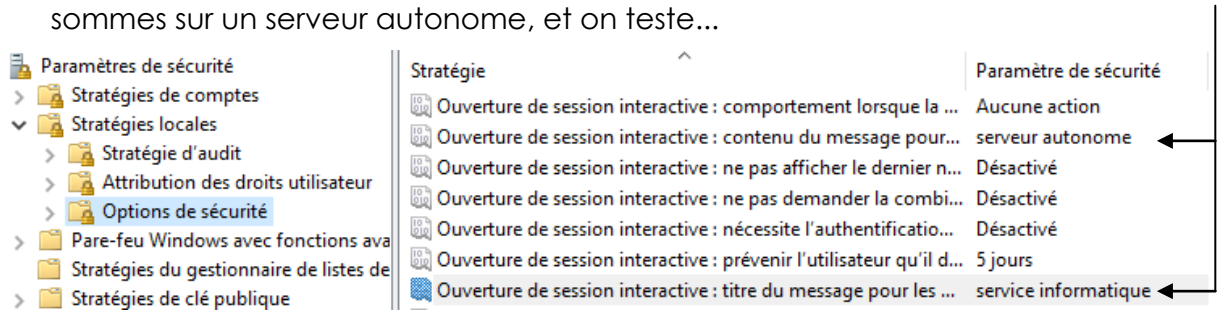
- On envoie une copie du raccourci **Stratégies Locales de Sécurité** sur le bureau… correspondant à **secpol.msc /s**



- On dévalide les exigences de complexité (et on donne un mot de passe à l'administrateur simple genre ***local2016***)



- On affiche un message avant l'ouverture de session indiquant que nous sommes sur un serveur autonome, et on teste…



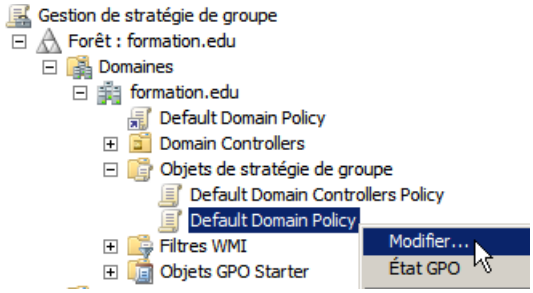
GPO DE DOMAINE

Affichage d'un message:

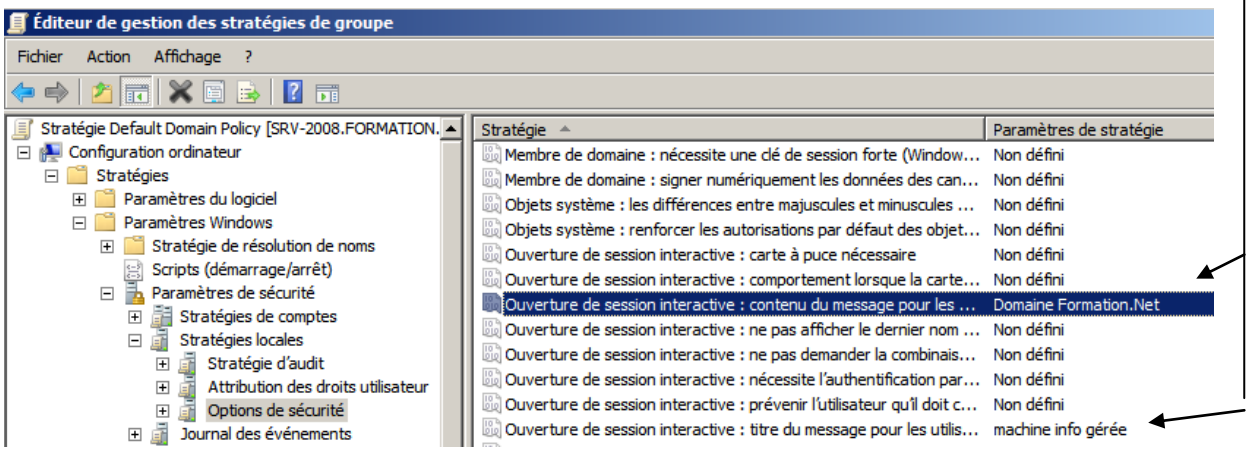
Informons clairement nos utilisateurs comme quoi désormais ils font partie de notre domaine…

Il s'agit des deux stratégies (déjà abordées) conjointes dans

la Gestion des stratégies de groupe dans les Outils d'Administration



On demande Modifier… la Default Domain policy



Après une propagation sur les clients (**gpupdate /force**), vérifier que :

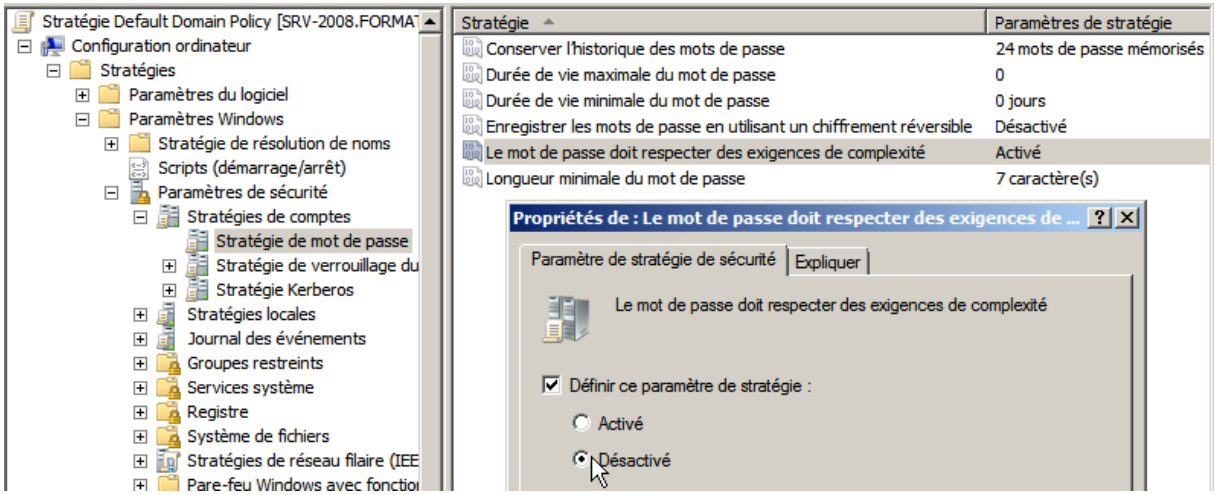
- Au démarrage du poste on a bien un message informant que la machine est info gérée
- Que devient alors le message paramétré dans les stratégies de sécurités locales…
- Que se passe-t-il s'il n'y a pas de connexion réseau lors du démarrage du poste ?
- Que se passe-t-il si la machine sort du Domaine ? (revient en workgroup)

Dévalidation mot de passe complexe:

On veut pouvoir dévalider l'obligation des mots de passe complexes

N.B : cette stratégie doit obligatoirement se faire sur la totalité du Domaine, faute d'obtenir très rapidement des incohérences fatales…

Soit on demande Modifier… la Default Domaine policy



Dans Paramètres windows / Paramètres de Sécurité / Stratégies de Compte / Stratégies de mot de passe

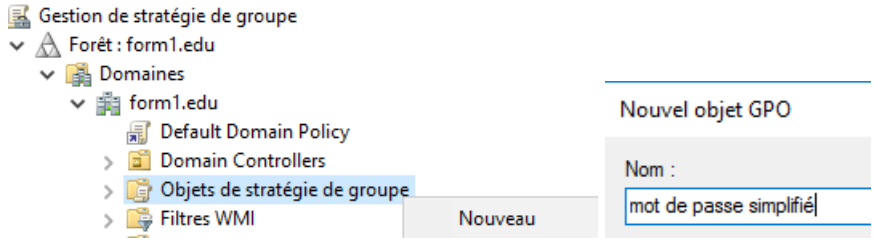
On demande alors

Le mot de passe doit respecter des exigences de complexité

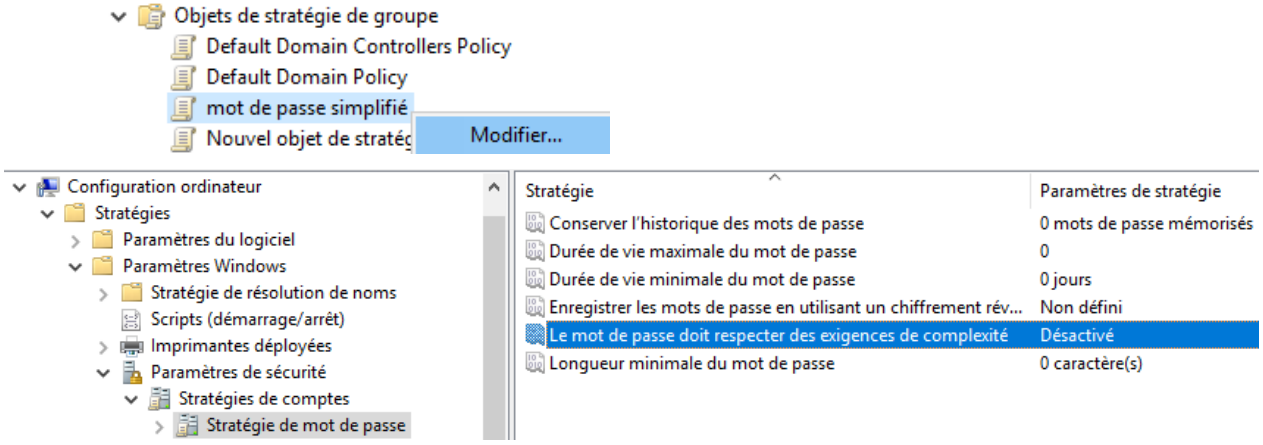
Longueur minimale du mot de passe

…

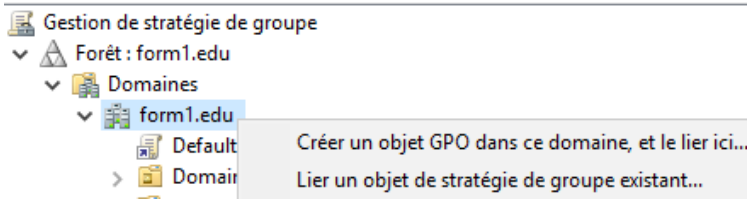
Soit, mieux, on crée un nouvelle **GPO** de Domaine, dans **Objets de stratégie de groupe**, on demande clic droit / **Nouveau…**

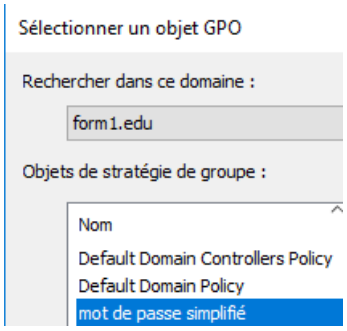


Ensuite on édite cette GPO via clic droit / Modifier…

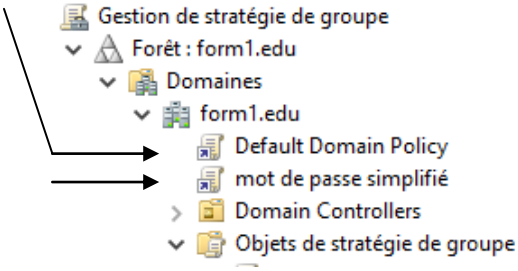


Il ne reste plus qu'à se mettre au niveau du domaine, et lier notre nouvelle GPO, via clic droit **/ lier un objet de stratégie de groupe existant**





Au final on devrait avoir 2 GPO au niveau du domaine



N.B : bien noter que on est en train de commettre un faute classique, de contradiction au niveau des GPO. En effet les mêmes réglages sont définis dans 2 GPO différentes, il va falloir choisir :

- Soit on ne laisse les réglages que dans une seule GPO
- Soit on hiérarchise les GPO, de manière à ce que 2 GPO contradictoires ne soient pas données au même niveau de l'AD
- Soit on gère l'ordre d'application, sachant que c'est la dernière qui s'appliquera qui aura raison !

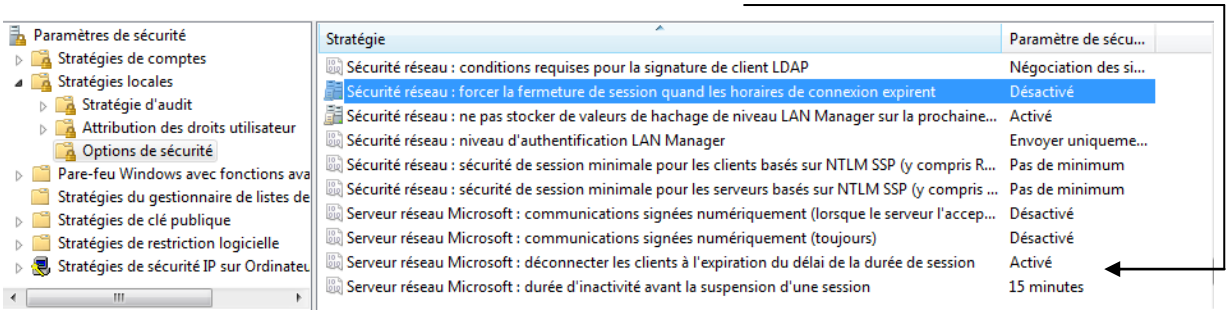
Déconnexion de session inactive:

Pour augmenter la sécurité à propos de l'accès réseau et l'ouverture de session, on souhaite déconnecter l'utilisateur lorsque l'heure de sa session est terminée. (déconnexion réseau, pas fermeture session locale…) 2 stratégies sont couplées ici… (et une troisième peut intervenir…)

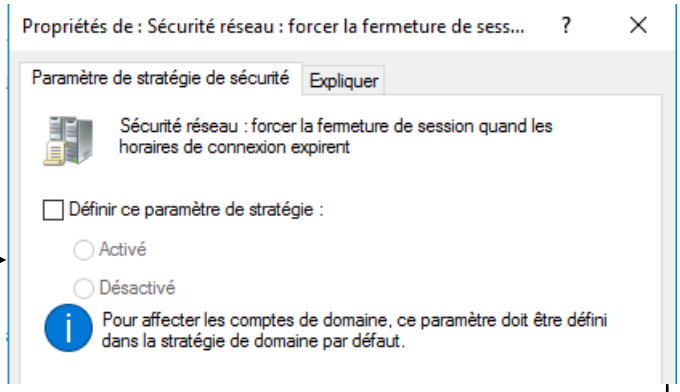
Sécurité Réseau : forcer la fermeture de session quand les horaires de connexion expirent

Serveur réseau Microsoft : déconnecter les clients à l'expiration du délai de la durée de session

Par défaut les réglages diffèrent selon les versions de Windows, Xp…

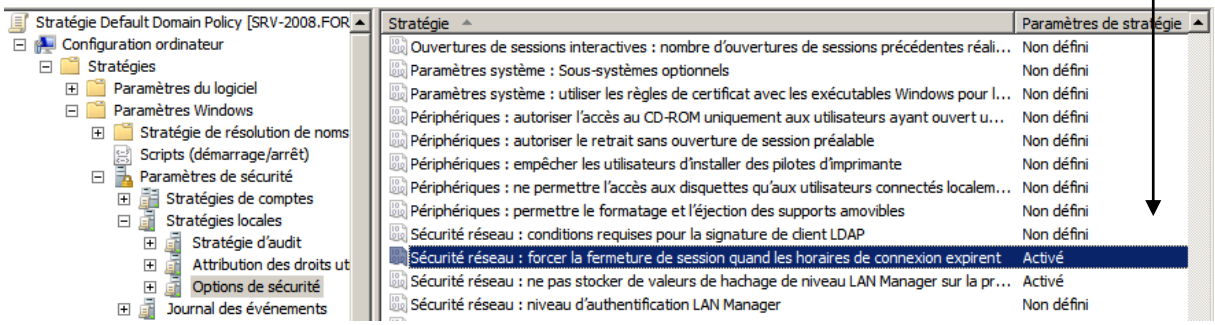


La seule solution c'est de faire une modification de la **default domain Policy**, et non pas de créer une stratégie de Domaine, tout simplement parce que on nous l'indique dans la documentation

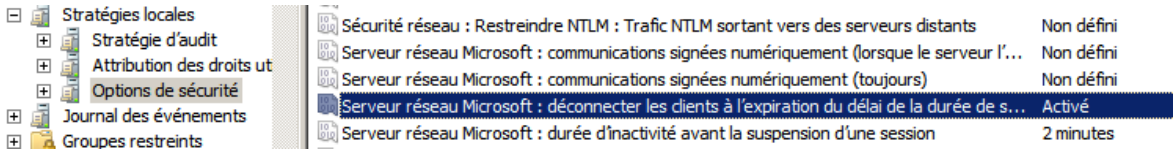


on active

Sécurité Réseau : forcer la fermeture de session quand les horaires de connexion expirent

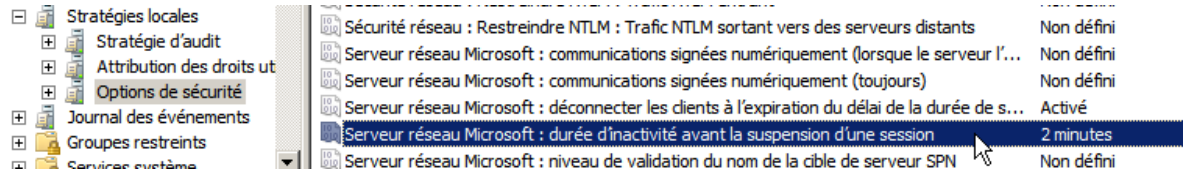


Serveur réseau Microsoft : déconnecter les clients à l'expiration du délai de la durée de session

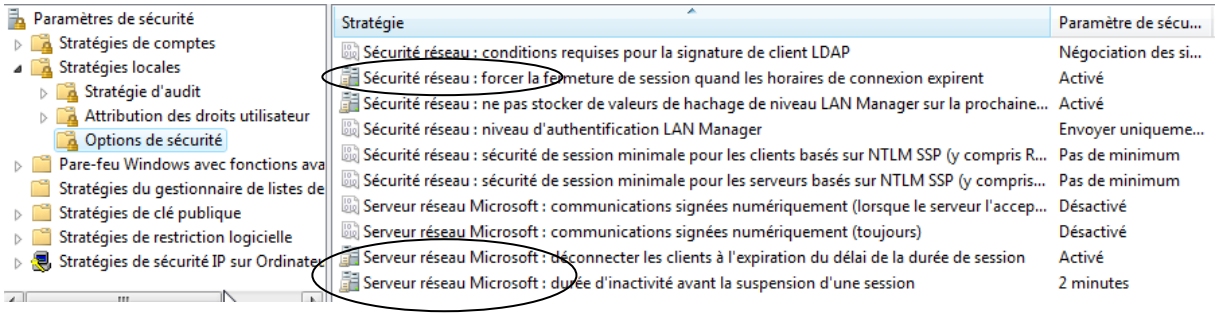


Et on peut aussi mettre 1 timing à 2 minute (15 min par défaut)

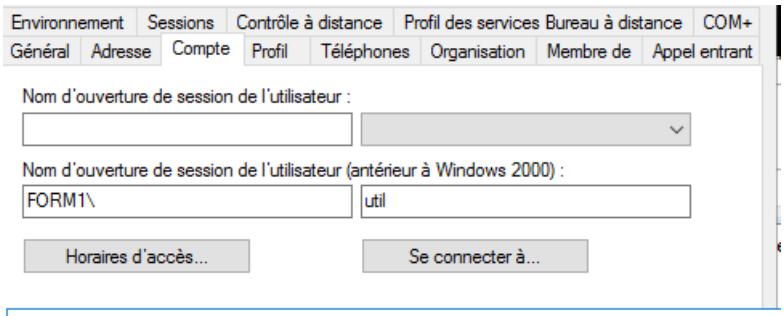
Serveur réseau Microsoft : durée inactivité avant suspension de session



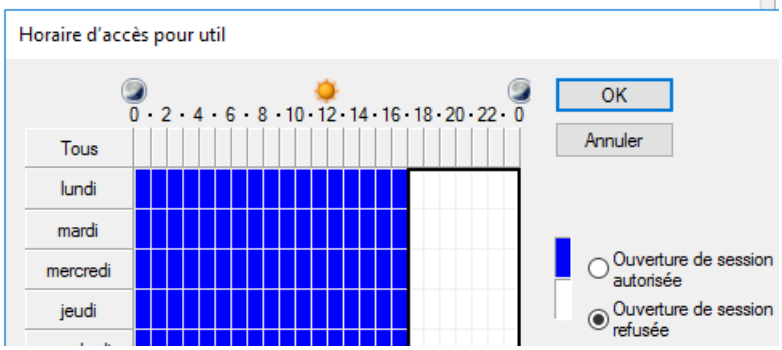
De cette manière-là, sur les clients on devrait avoir les 3 stratégies de domaine qui se répercutent :



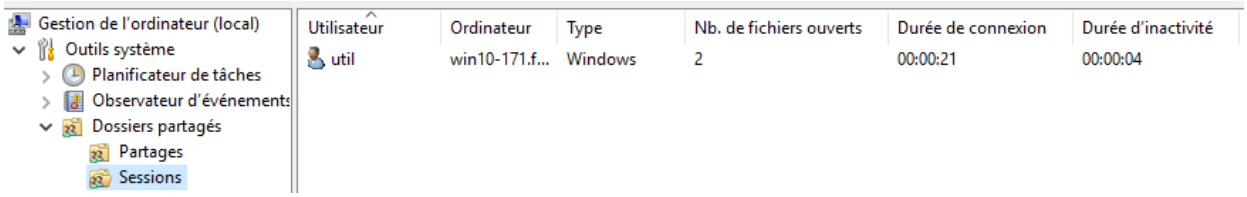
Il faut ensuite définir des horaires d'accès pour un utilisateur (ici **util**)



Ensuite, lorsque après propagation de la GPO (y compris sur le serveur) cet utilisateur ouvre une session depuis un poste,



on peut vérifier que le décompte s'amorce



ou avec la commande **net session**

```
Ordinateur            Nom d'utilisateur    Type de client   Ouv.  Inactivité

-------------------------------------------------------------------------------
\\192.168.1.171       util                                    2 00:00:48
\\192.168.1.171       WIN10-171$                             14 00:01:32
La commande s'est terminée correctement.
```

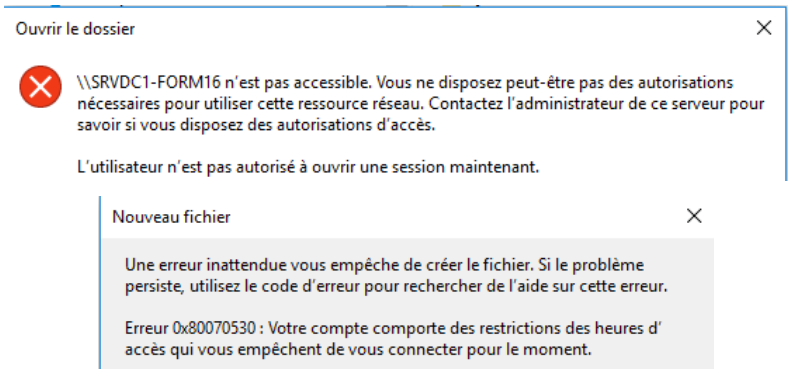
Puis augmente

```
Ordinateur            Nom d'utilisateur    Type de client   Ouv.  Inactivité

-------------------------------------------------------------------------------
\\192.168.1.171       util                                    2 00:01:04
\\192.168.1.171       WIN10-171$                             14 00:01:48
La commande s'est terminée correctement.
```

Jusqu'au moment où la session est stoppé (ici après 2 mn)

```
C:\Windows\system32>net session
La liste est vide.
```

Si son heure limite est non atteinte, la reconnexion se fera de manière automatique, Si son heure limite est atteinte il sera automatiquement déconnecté du serveur (mais sa session locale ne sera pas fermée) et toute tentative de re-connection donnera des messages d'erreur

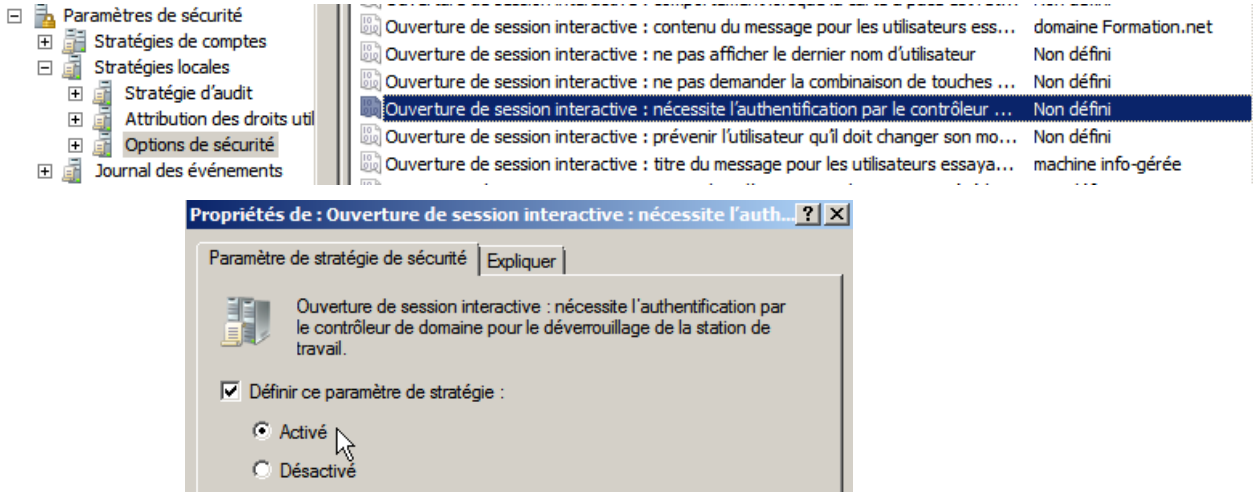


Forcer l'authentification sur le serveur:

On peut trouver qu'il est dangereux d'autoriser les ouvertures de session sans authentification systématique sur le serveur. 2 paramètres de sécurité dans **stratégies locales / Options de sécurité** déterminent si un contrôleur de domaine doit être contacté obligatoirement pour ouvrir une session sur un ordinateur.

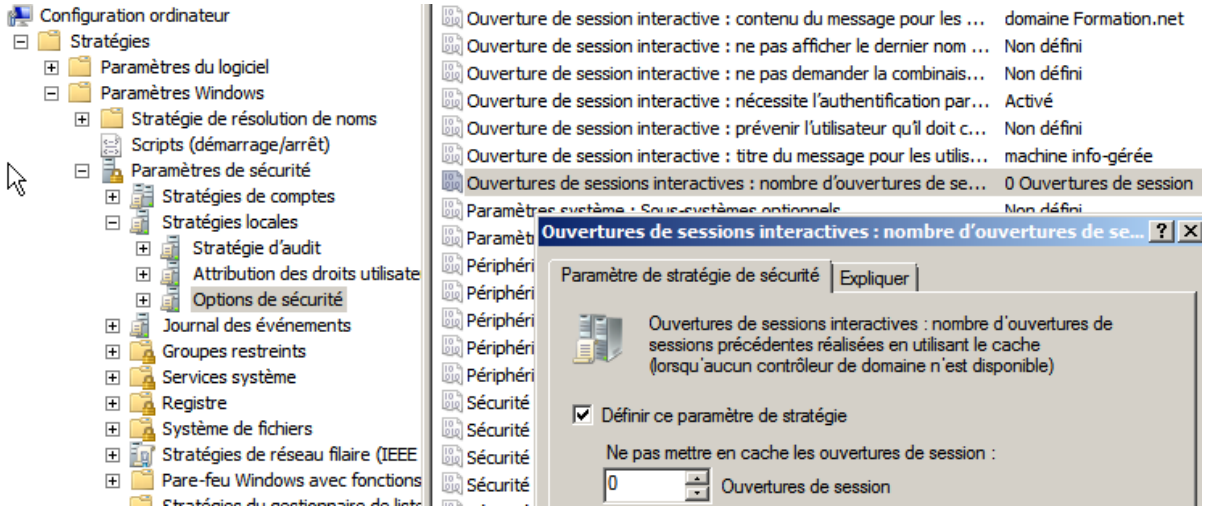
N.B : ces deux stratégies sont couplées, une fois armées, il faut les dévalider toutes les deux…

Ouverture de session Interactive : nécessite l'authentification par le contrôleur de domaine…

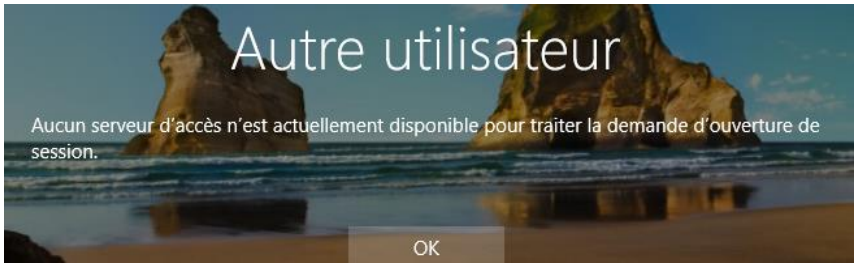


Ouverture de session Interactive : nombre d'ouvertures de

permet de spécifier le nombre de cache sessions utilisable



Test : on dévalide la carte réseau de notre CD, et on tente ou ouverture de session sur le client avec un login de domaine **Si on propage ces 2 réglages** l'ouverture de session échoue

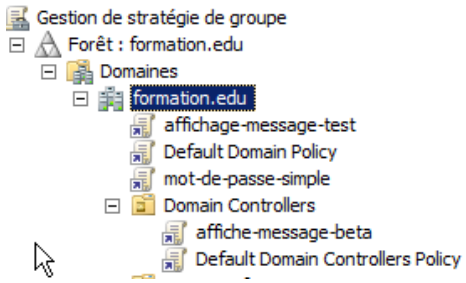


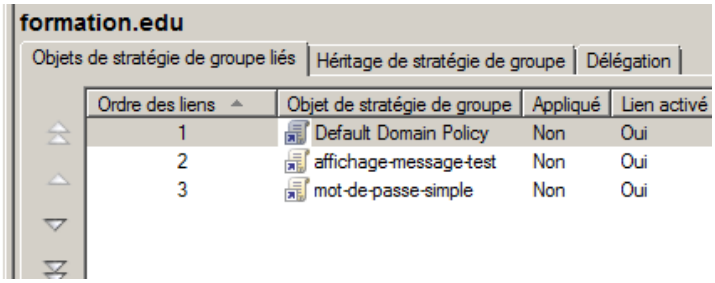
Best pratice : 1GPo = 1 Action

Il vaut mieux travailler correctement, et ne pas modifier les GPO par défaut

on va donc se créer 1 GPO par objectif. comme par exemple

et ensuite les lier comme on le souhaite, dans l'exemple, un message au niveau du domaine, et des mots de passe simple, et un message spécifique pour les contrôleurs de domaine



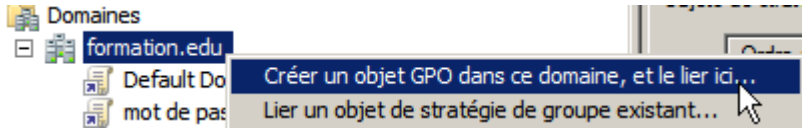


N.B: attention entre le conflit pour la gestion des mots de passe entre la **GPO default domaine policy** et notre **gpo *mot de passe simple***...

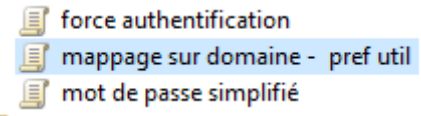
PREFERENCES & STRATEGIES

Mappage lecteur commun :

On souhaite créer un lecteur réseau pour tout le monde, sur tout le domaine… On va créer une préférence de stratégie au niveau du domaine…

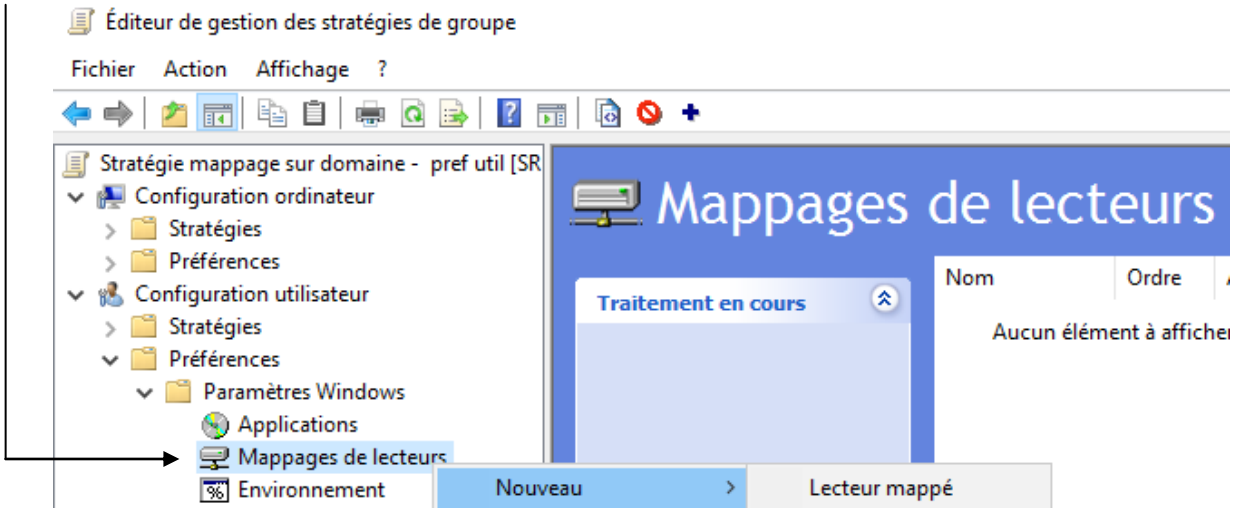


Et on lui donne un nom parlant

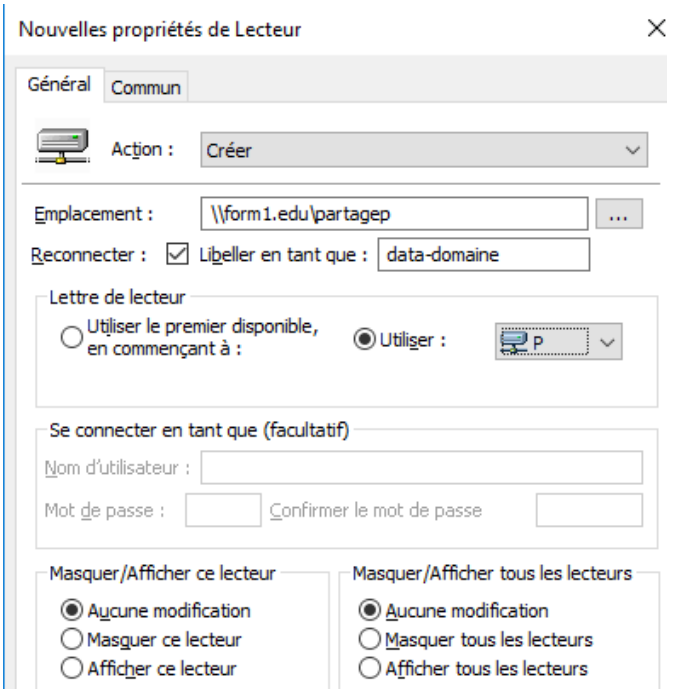


On se place sur notre stratégie

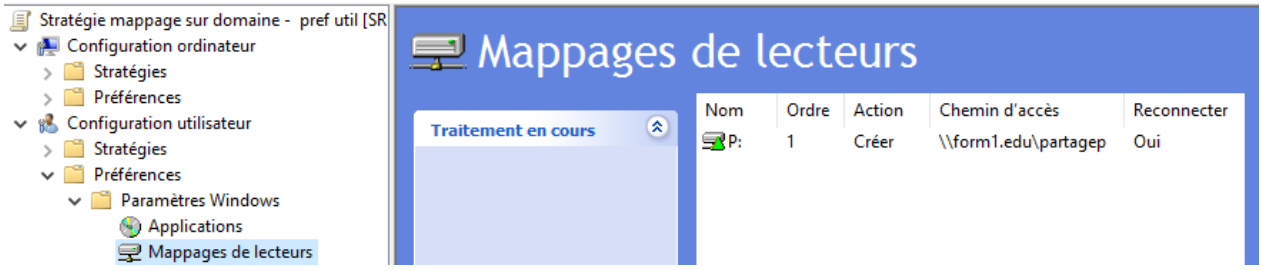
Configuration Utilisateur / Préférences / Paramètres Windows / Mappage de Lecteurs et on demande Nouveau / Lecteur mappé



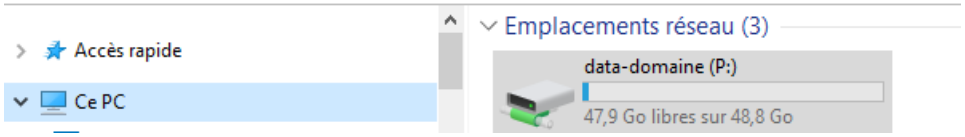
Et on indique les paramètres nécessaires



Notre préférence de stratégies est terminée.



Lorsque sur le client la GPO est tirée, le lecteur est monté



Modification Utilisateurs Locaux :

Globalement depuis mai 2014, on ne peut/doit plus faire des actions qui incorporent un mot de passe, c'est à dire que l'on ne peut plus créer par exemple un compte local sur le client et lui affecter un mot de passe, ou bien changer un mot de passe d'un utilisateur local !

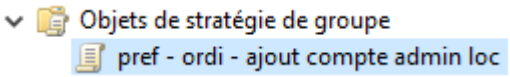
1. On souhaite ajouter un **compte de domaine *Albert*** comme membre du **groupe des Administrateurs** du poste client
2. On souhaite ajouter (ou remplacer)un **groupe global** d'utilisateur de domaine comme membre du **groupe des Administrateurs** du poste client
3. On souhaite mettre dans le groupe des Utilisateurs avec pouvoirs le groupe global des Utilisateurs du domaine

Ajout utilisateur de Domaine dans groupe Local des administrateurs

On souhaite ajouter un **compte de domaine *Albert*** comme membre du **groupe des Administrateurs** du poste client

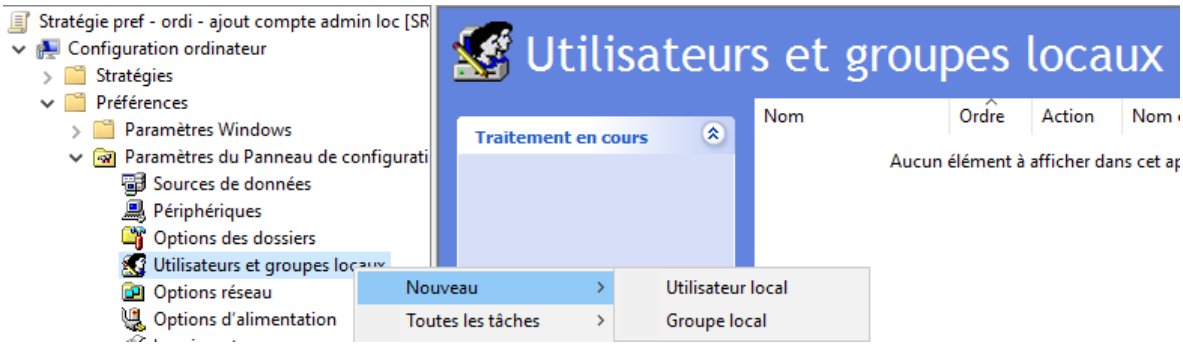
Le compte utilisateur *Albert* / *Domaine2016* existe dans le domaine

On crée une préférence

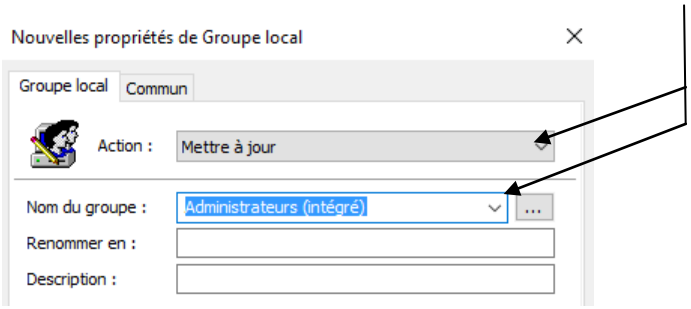


Dans laquelle on va demander de mettre à jour le groupe local des administrateurs (intégré) …

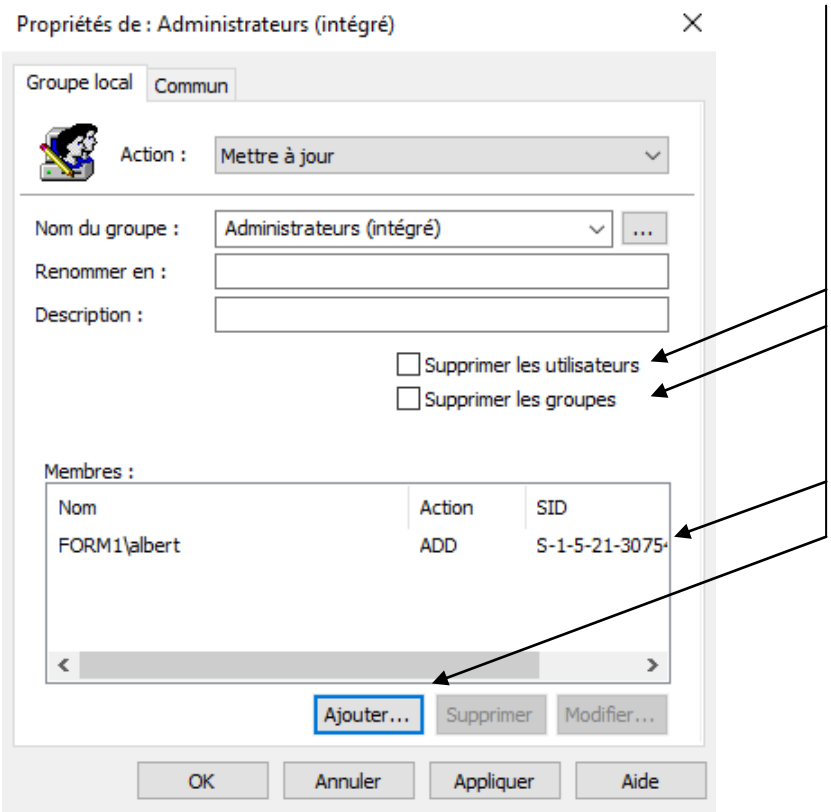
Dans **Préférences, paramètres du panneau de configuration / utilisateurs et groupes locaux**, on demande clic droit **Nouveau / Groupe local**



On demande de mettre à jour le groupe des Administrateurs (intégré)



Et on complète selon nos besoins (ici on ajoute simplement Albert)

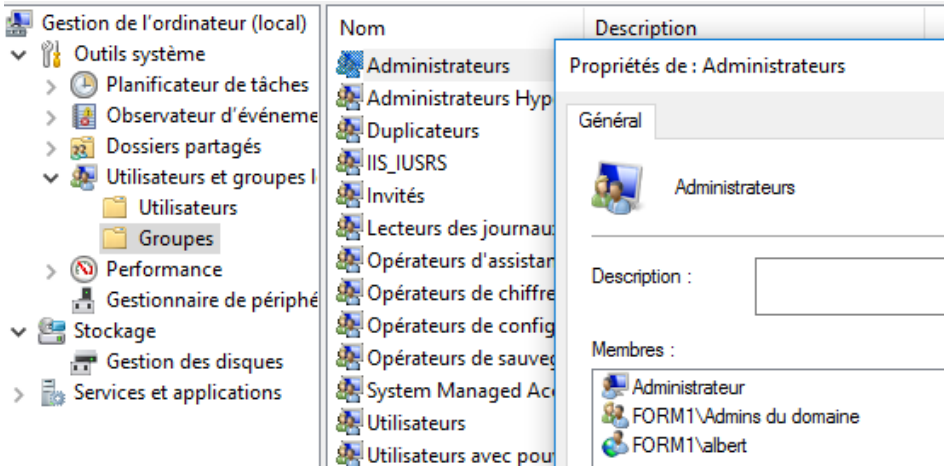


Et notre préférence est terminée

On propage la préférence sur un client

```
C:\Users\albert>gpupdate /force
Mise à jour de la stratégie...
```

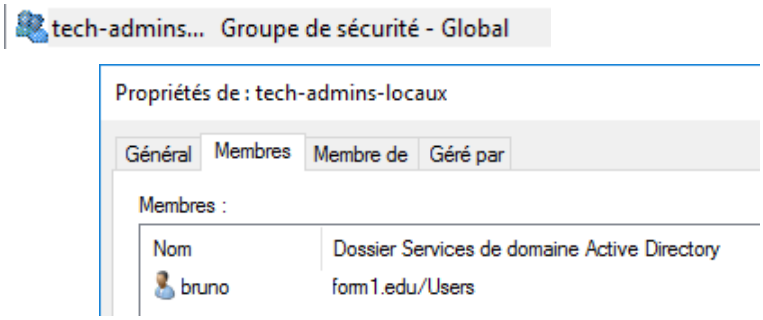
Et on vérifie bien que l'on a ***albert*** membre du **groupe des administrateurs**



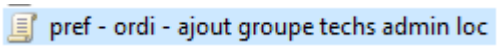
Ajout Groupe de Domaine dans le groupe Local des administrateurs

Le compte utilisateur ***Bruno / Domaine2016*** existe aussi dans le domaine

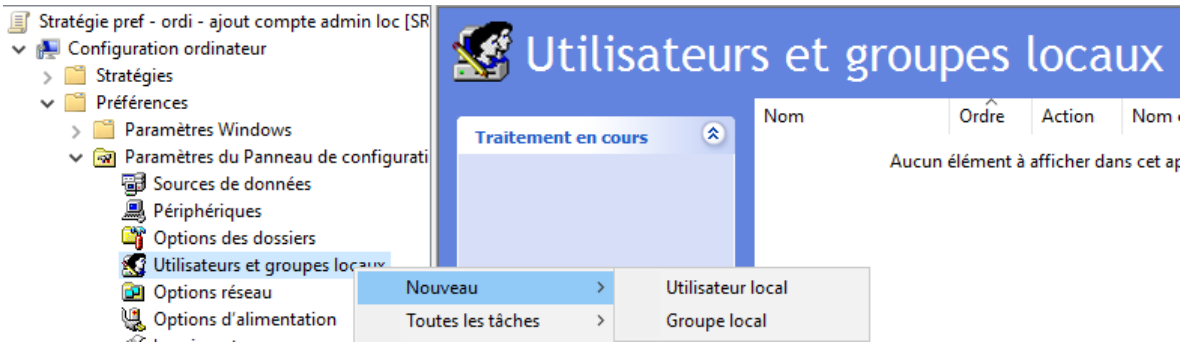
Le Groupe Global *tech-admins-locaux* existe dans le domaine



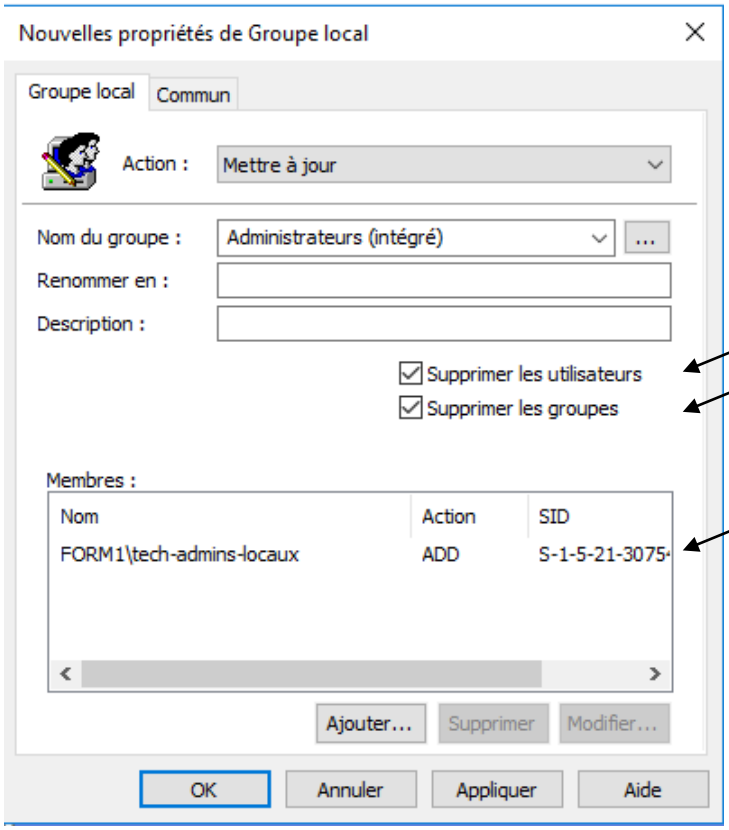
On crée une préférence



Dans Préférences, paramètres du panneau de configuration / utilisateurs et groupes locaux, on demande clic droit Nouveau / Groupe local

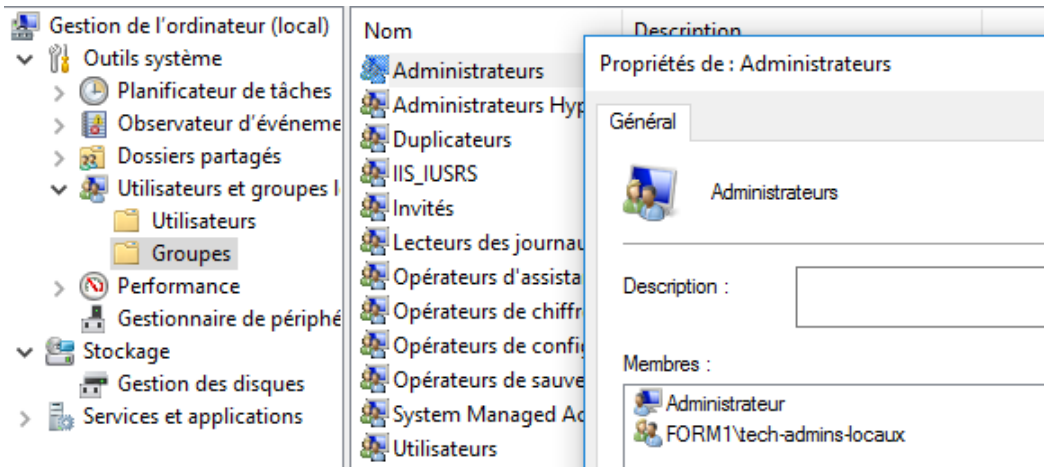


Et on complète selon nos besoins (ici on ajoute le groupe tech-admins-locaux et on supprime les utilisateurs et groupes pré-existants)



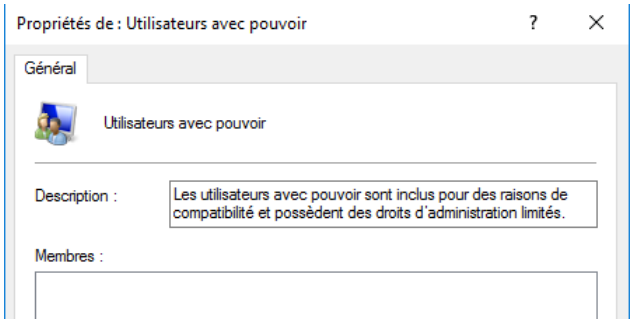
On propage la préférence sur un client

Et on vérifie qui est membre du **groupe des administrateurs**



Ajout Groupe de Domaine dans groupe Local des utilisateurs avec pouvoir

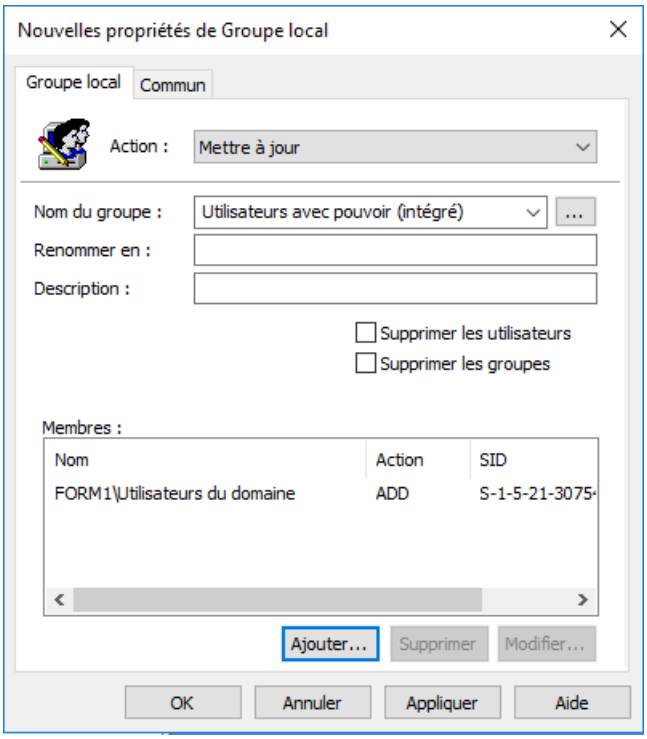
Par défaut le groupe des utilisateurs avec pouvoir est vide



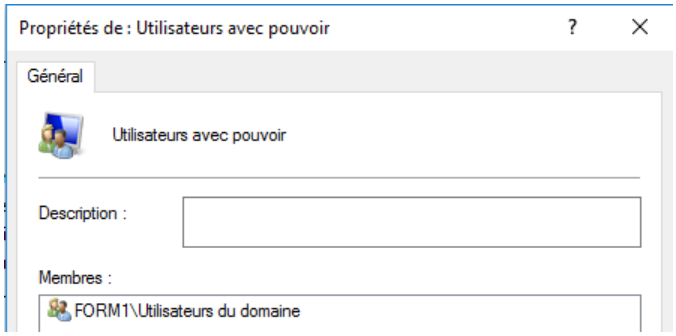
On se crée une préférence

pref - ordi ajout util domaine groupe loc des utils

avec



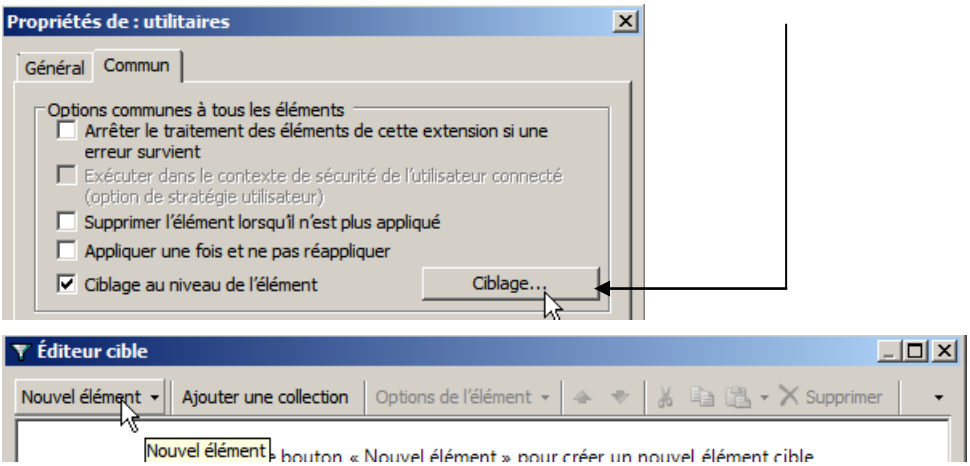
Et on devrait obtenir sur les clients impactés



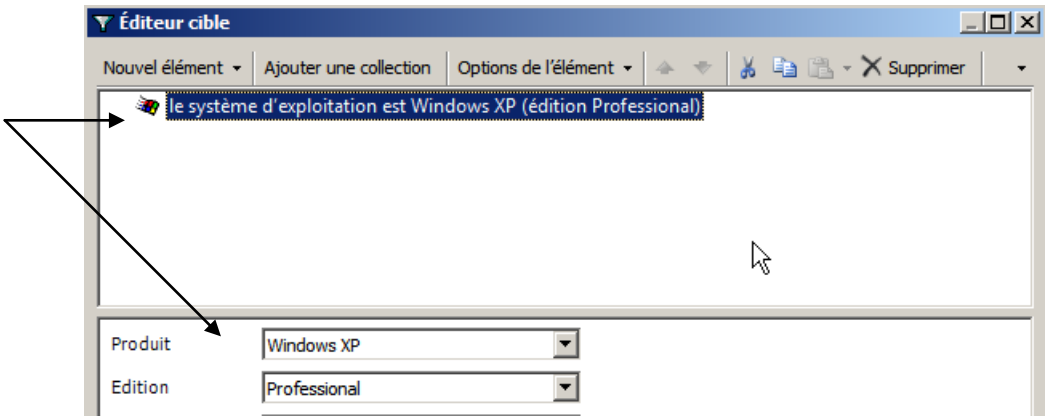
Ciblage des préférences exemple système XP:

Soit une préférence de stratégie qui créerait un dossier « utilitaires » sur les machines du domaine tournant encore sous Xp…

On veut cibler les postes sur lesquels le dossier se crée… donc on demande l'onglet **Commun / Ciblage au niveau de l'élément** et **Ciblage…**



Et on demande



GPO GROUPES RESTREINTS

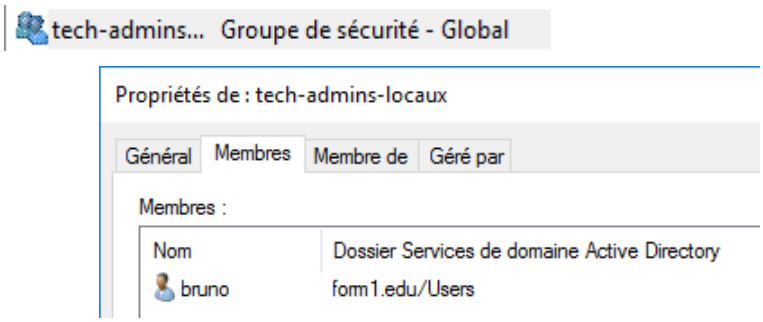
Gérer les Groupes Locaux :

On souhaite pouvoir intégrer des groupes de Domaine dans des groupes locaux des machines Visées.

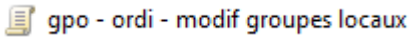
On vient de le faire à l'aide des préférences, mais la méthode existe avant 2008 sous la notion de groupe restreints (en fait il faut lire groupe pré-définis.)

Remplacer dans un Groupe Local :

Soit par exemple un **groupe global de domaine** nommé ***tech-admins-locaux*** que l'on crée sur notre AD

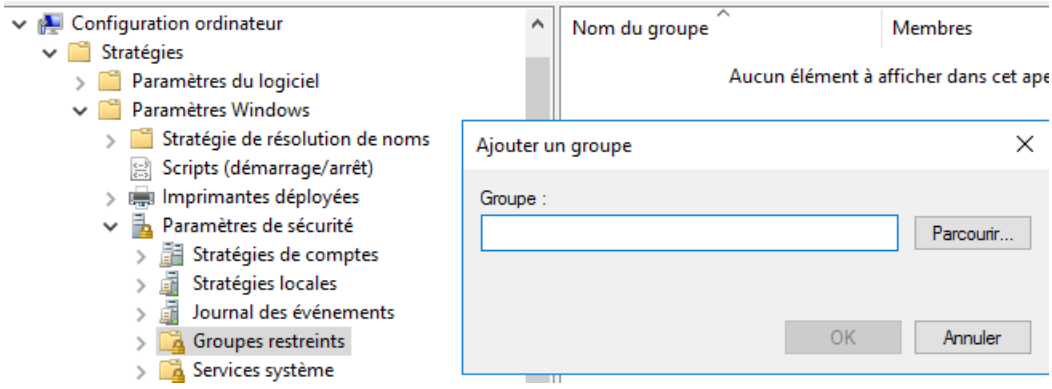


On se crée une nouvelle **GPO** nommée par exemple **gpo-ordi-modif-groupes-locaux**

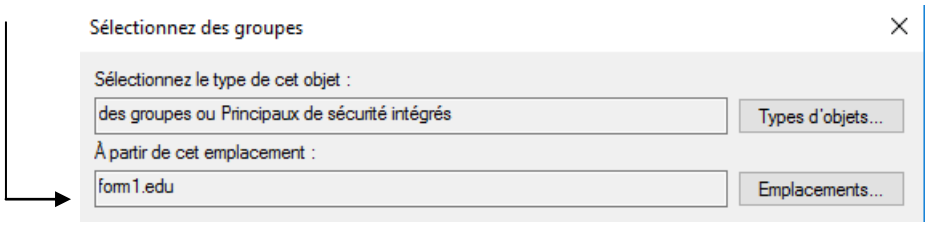


dans les Stratégies Configuration Ordinateurs, on demande

Paramètres Windows / paramètres de Sécurité et dans Groupes Restreints

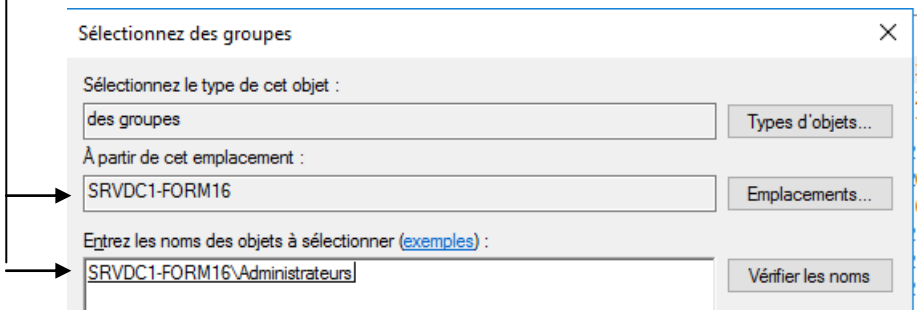


on ajoute le groupe restreint que l'on veut modifier, c'est-à-dire le groupe local des administrateurs du serveur..donc par rapport a ce qui est proposé (le domaine…)

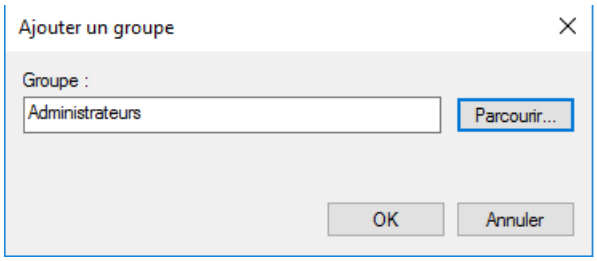


Il faut aller chercher le compte ordinateur du serveur

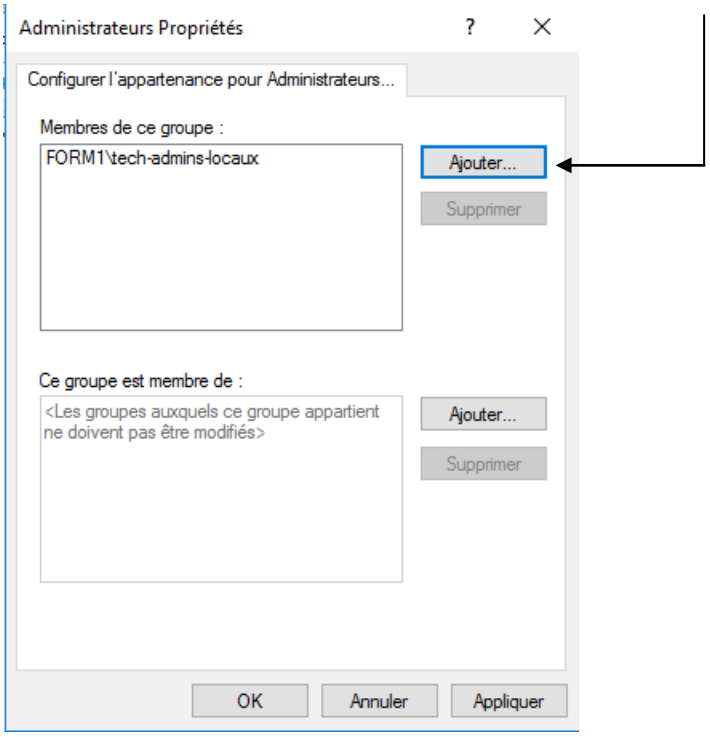
Et indiquer le **groupe local** du serveur **Administrateurs**



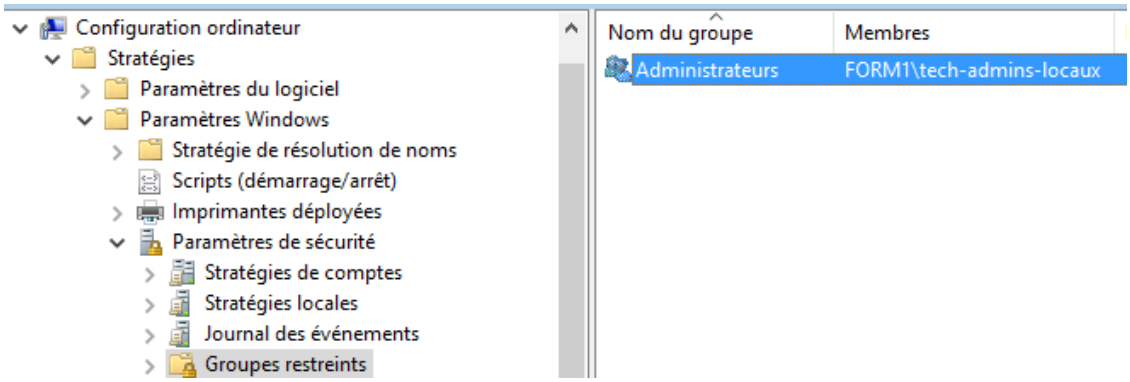
En fait on « cible » le groupe local des Administrateurs d'un ordinateur.



ensuite on indique qui devra faire partie de ce groupe local que l'on vient de choisir , donc notre groupe global ***admin-clients-locaux***

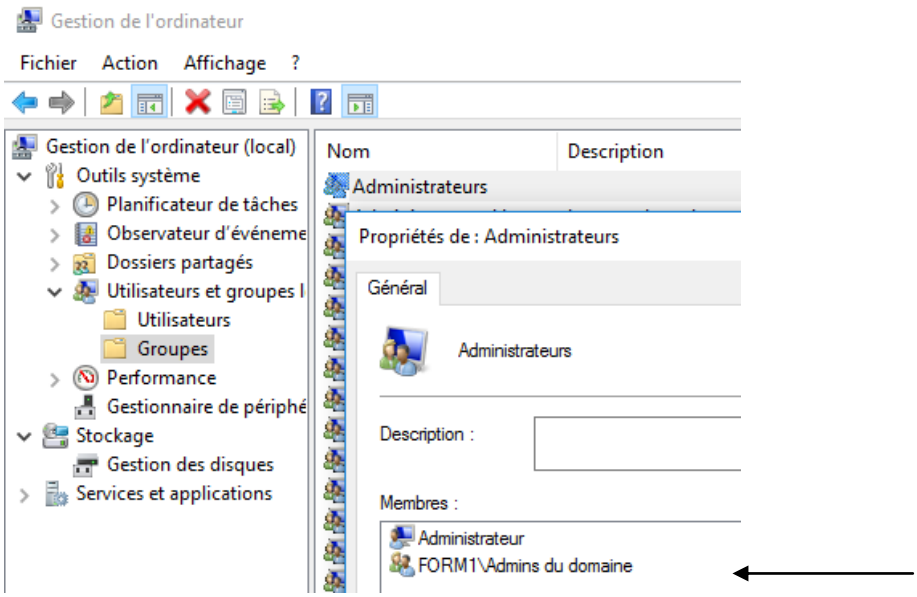


Ce qui donne au final

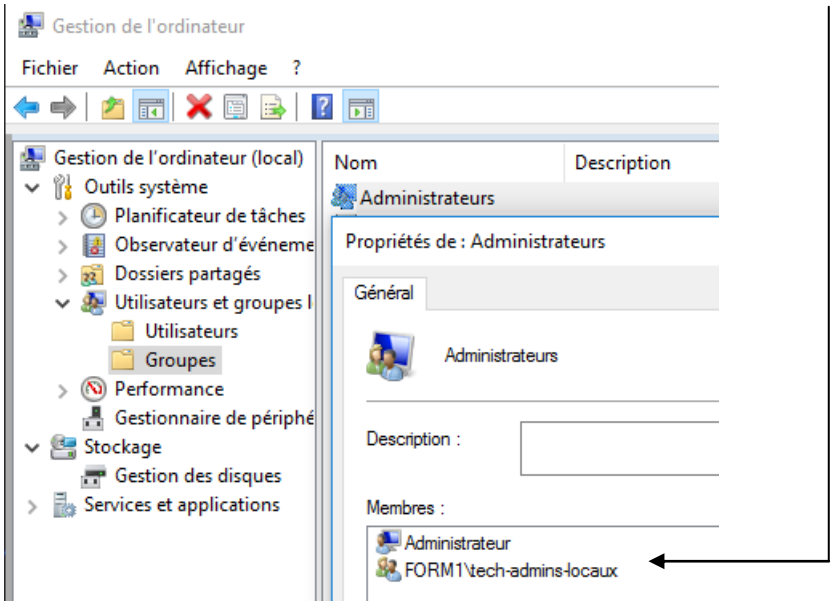


Après propagation et application de la **GPO** sur les clients concernés on devrait avoir notre **Groupe** qui a remplacé les groupes existants...

Si sur une machine le **Groupe** des **Administrateurs** Locaux ressemblait à cela



après application de notre **GPO** il ressemblerait plutot à ceci...



CREATION DE GPO SUR UNE UO

Objectifs :

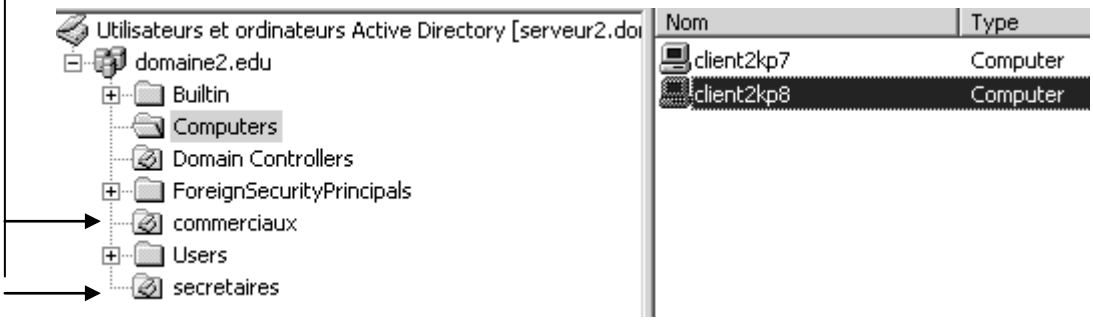
Dans le domaine, on dispose de deux services, un service pour les **commerciaux**, et un autre pour les **secrétaires**. A terme, la gestion des postes des commerciaux est radicalement différente de celle des postes des secrétaires, par conséquent on va se créer des **UO** et des **GPO** pour chacune de ces entités.

- Vérifier que lorsqu'un ordinateur fait partie d'une **UO** (commerciaux par exemple), il récupère automatiquement sa **stratégie**…
- Vérifier que pour récupérer la stratégie de l'autre **UO** (secretaire donc), il suffit de déplacer le compte ordinateur dans l'**UO** adéquate…

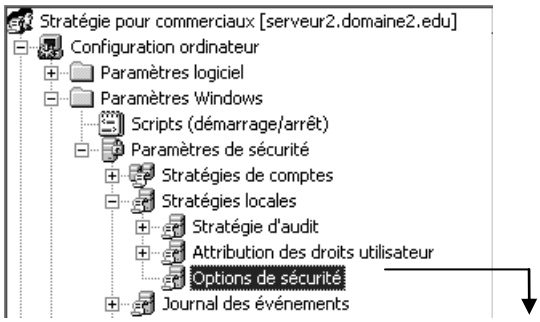
Le but ici étant pédagogique, les GPO n'auront pas d'autres effet que d'annoncer l'appartenance à telle ou à telle entité (du genre, « bonjours, votre poste est régit par le modèle affecté aux commerciaux/ *(ou)secrétaires*…. »)

Définir 2 UO dans AD , et créer leur GPO :

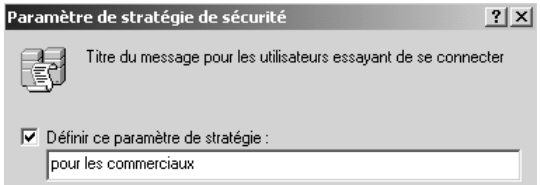
Il faut commencer par se créer deux **UO commerciaux** et **secretaires**

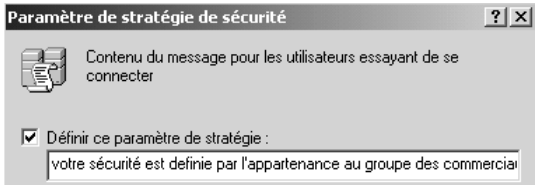


On va créer notre **GPO** pour les **commerciaux** affichant notre appartenance au groupe des commerciaux

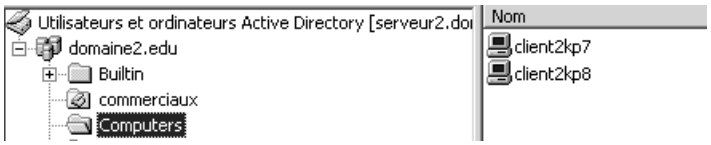


Changeons pour l'exemple uniquement :





Si on se place sur l'**UO** prédéfinie **Computers**, on voir normalement tous les postes du domaine…



Il est nécessaire de déplacer les postes faisant partie des commerciaux dans leur **UO** pour qu'ils héritent de leur stratégie.

- vérifier que lorsque l'on démarre le poste, un message indique bien l'appartenance aux commerciaux…

Changer d'UO = changer de GPO :

On va créer une **GPO** pour les secretaire affichant notre appartenance au groupe des secretaire.

Puis on déplace le poste faisant partie de la section des commerciaux dans leur **UO** pour qu'ils héritent de leur stratégie.

- vérifier que lorsque l'on ouvre une session, un message indique toujours l'appartenance aux commerciaux…et non pas aux secretaires !

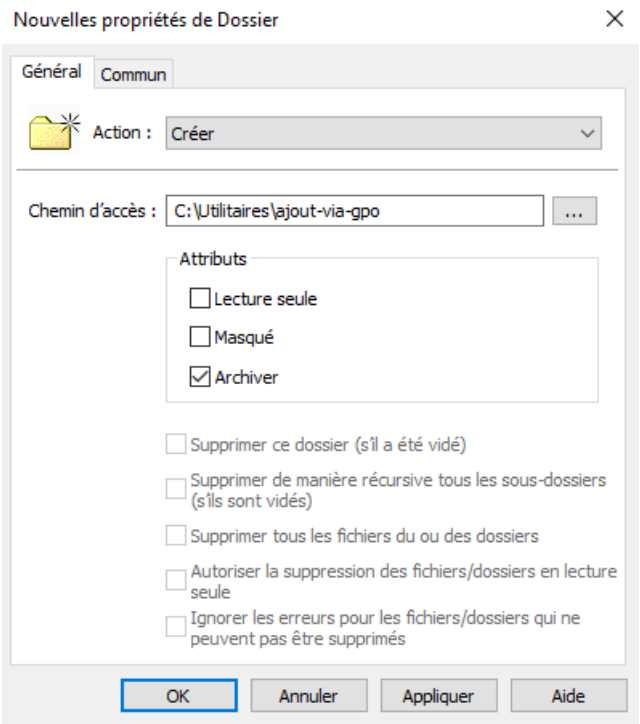
PREFERENCE CREATION DE DOSSIER

Création de dossier

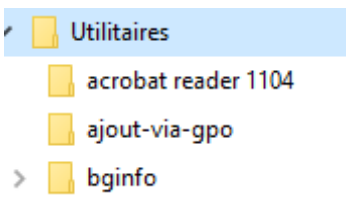
On crée une stratégie au nom parlant **pref-ordi-creation-dossier**

On demande dans les **Configuration Ordinateur / Préférences** / **Paramètres Windows / Dossiers** via clic droit **Nouveau / Dossier**

Et par exemple



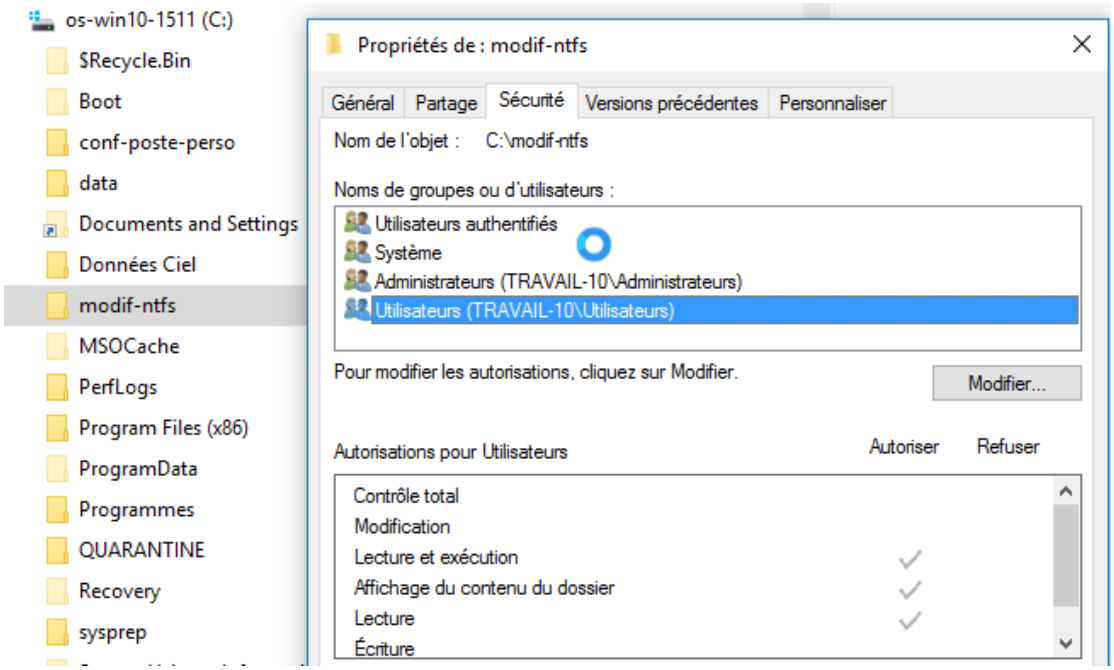
Une fois l'execution de la GPO effectuée on devrait avoir sur le client



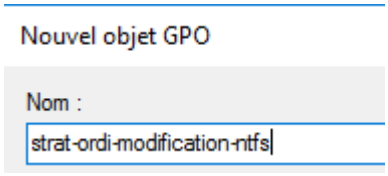
STRATEGIE RE-DEFINITION SECURITE NTFS

Modification NTFS sur un dossier

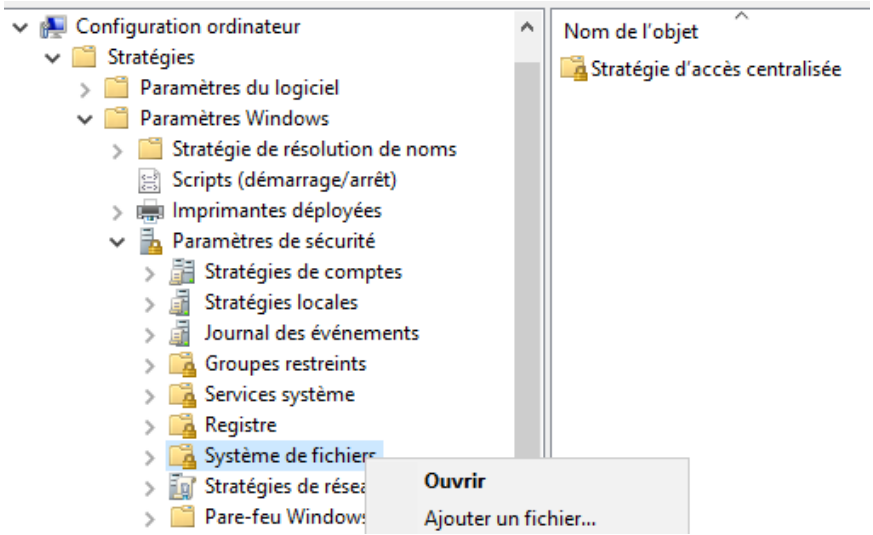
Soit un dossier ***modif-ntfs*** existant sur les clients, un **dossier homonyme** doit exister sur le serveur…avec des autorisations données par défaut



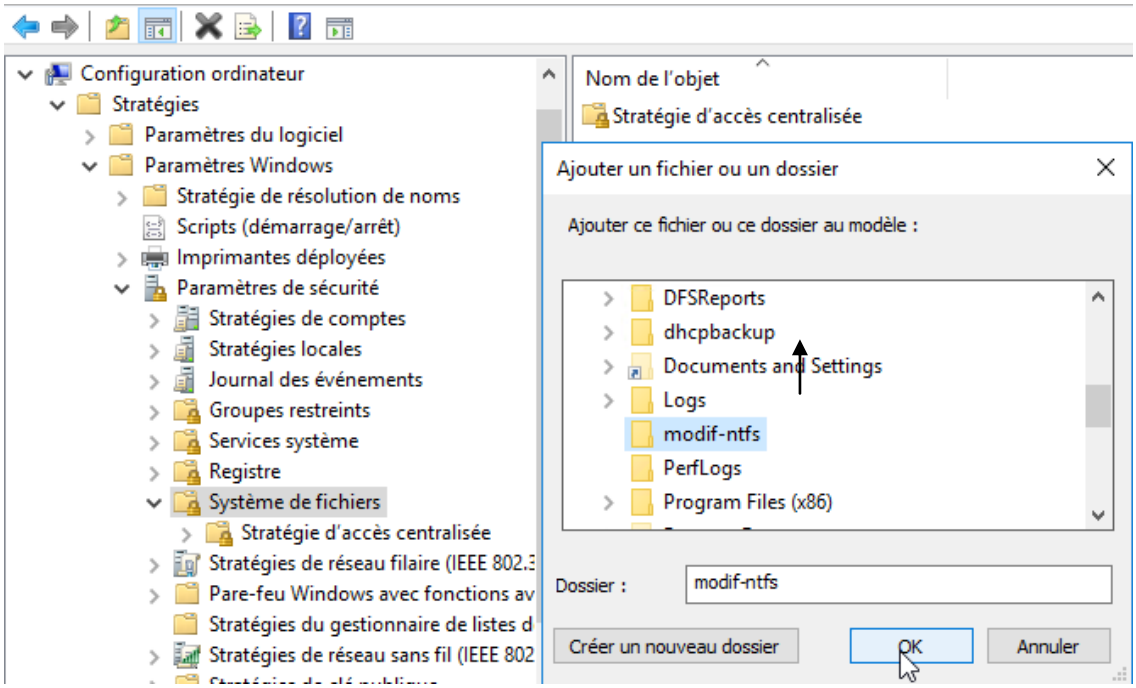
On crée une stratégie au nom parlant **strat-ordi-modification-ntfs**



On demande dans les **Configuration ordinateur / Strategies / Paramètres Windows / Paramètres de sécurité / Système de fichier** via clic droit **Ajouter un fichier**

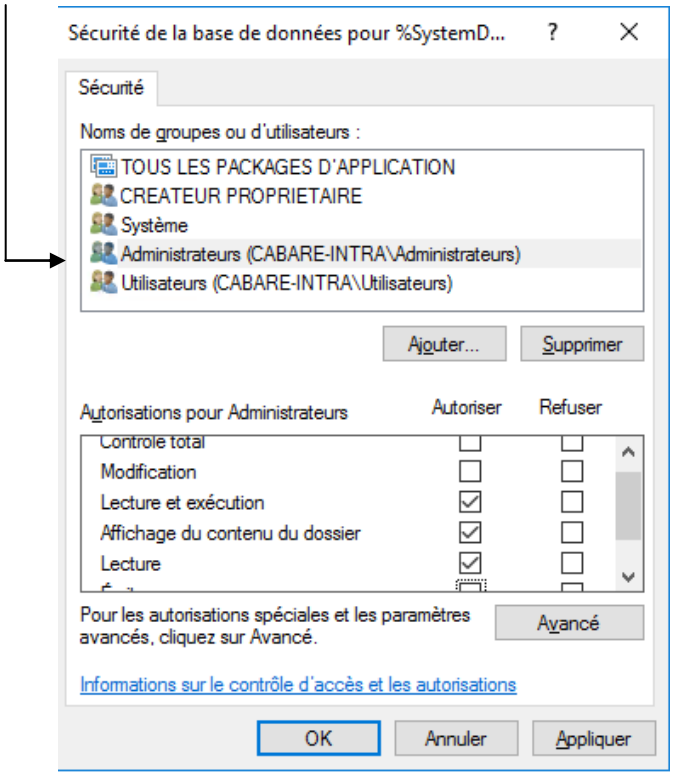


Il faut indiquer ici un dossier existant, éventuellement en utilisant les variables d'environnement,**%windir%, %systelmroot%, %programFiles%**



puis donner les autorisation NTFS voulues (par exemple ici administrateurs en lecture seule), et utilisateurs en accès complet…

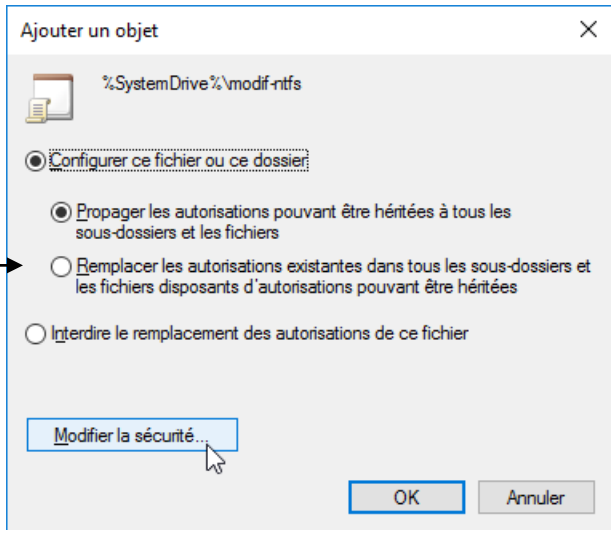
N.B: dans l'interface, ce sont les autorisations par défaut du serveur qui apparaissent, donc ici dans l'exemple ***CABARE-INTRA\Administrateurs*** !



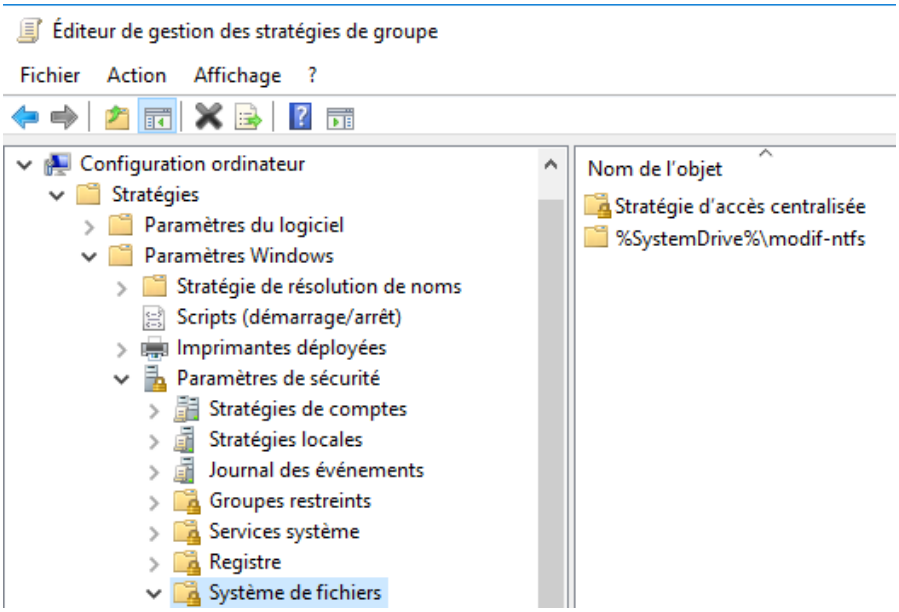
N.B Cela n'empeche pas d'ajouter des groupes ou utilisateur du domaine !

On confirme la sécurité NTFS

Choix le plus classique

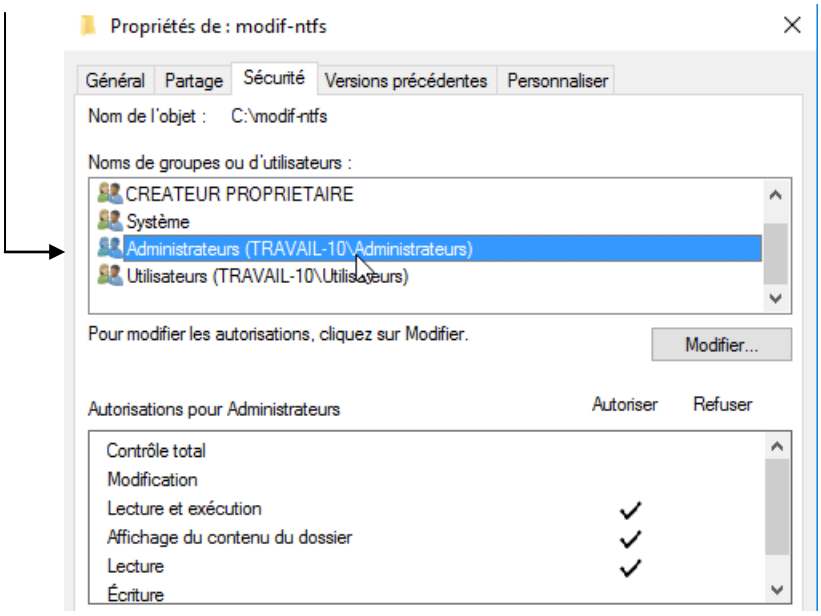


Et on obtient



Résultat et Test

On retrouve les autorisations locales "par défaut" du client modifiées, donc donc ici dans l'exemple ***travail-10\Administrateurs*** en lecture seule !



N.B On retrouveras les groupes / utilisateur du domaine si on les a ajoutés!

GPO & MODELES D'ADMINISTRATION

Objectifs :

On souhaite pour tous les utilisateurs du domaine sauf l'administrateur :

1. Désactiver les menus automatiques, et Supprimer le menu **exécuter** du menu **Démarrer**
2. Désactiver l'accès au Panneau configuration (ou que l'affichage)
3. Désactiver Windows defender

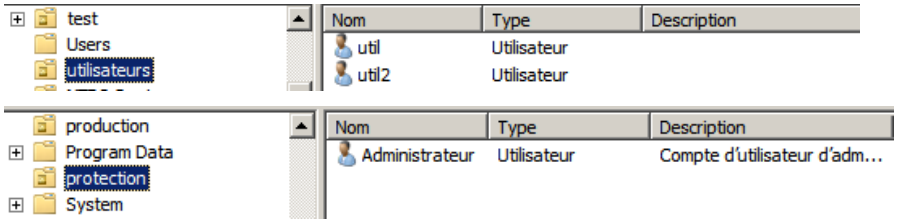
Blocage de la stratégie pour l'administrateur:

Puisque l'on veut travailler sur des **utilisateurs**, sauf l'**administrateur**, deux techniques peuvent exister :

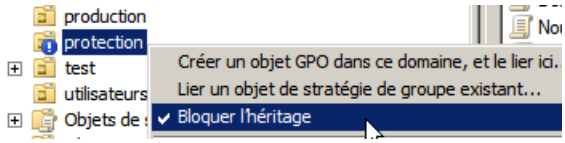
1. On crée des GPO de domaine (mais distinctes de Default Domain policy…), et comme on ne veut pas qu'elles s'appliquent à l'administrateur, il faut placer ce compte dans une UO spécifique et bloquer l'héritage sur cette UO...
2. On crée deux UO, une pour les utilisateurs, l'autre pour l'administrateur… Sur la première on applique les stratégies voulues, sur la deuxième on protège (on ne sait jamais l'administrateur)

Mettons en place la deuxième solution…

Dans **Utilisateurs et Ordinateurs Active Directory**, on crée deux UO, une pour les utilisateurs, l'autre pour l'administrateur



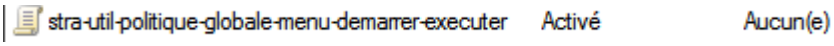
Dans **Gestion des stratégies de groupe**, on bloque l'héritage sur l'UO protection



Création des stratégies :

Supprimer executer

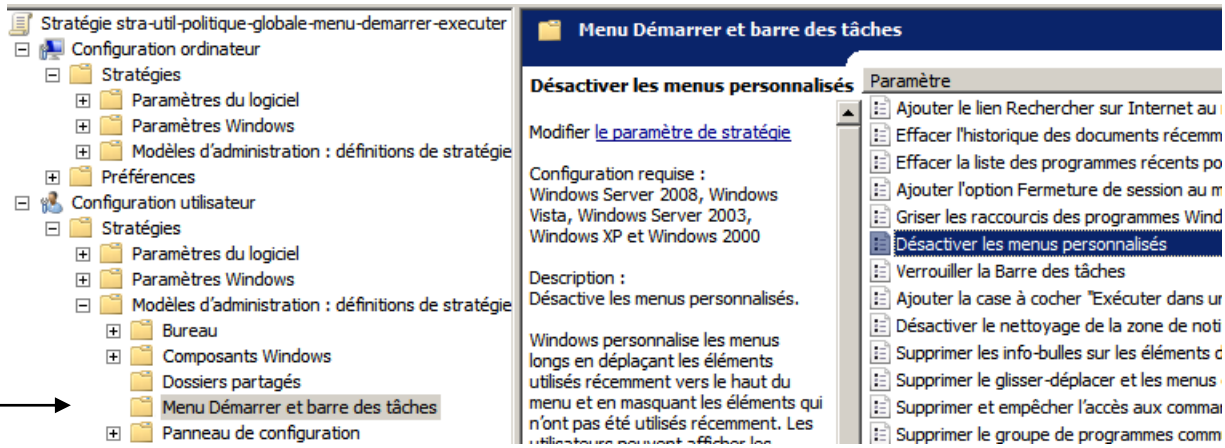
stra-util-politique-globale-menu-demarrer-executer



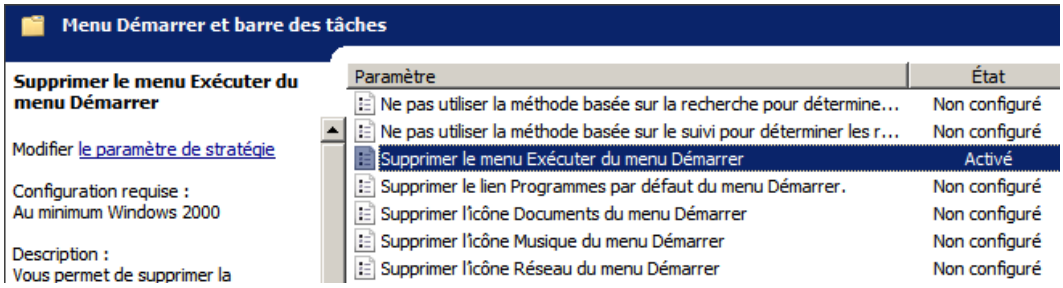
Qui contient donc

Configuration utilisateur / Stratégies / Modèles d'administration/ Menu Démarrer & barre des tâches

- Désactiver les menus personnalisés



- Désactiver le menu Executer



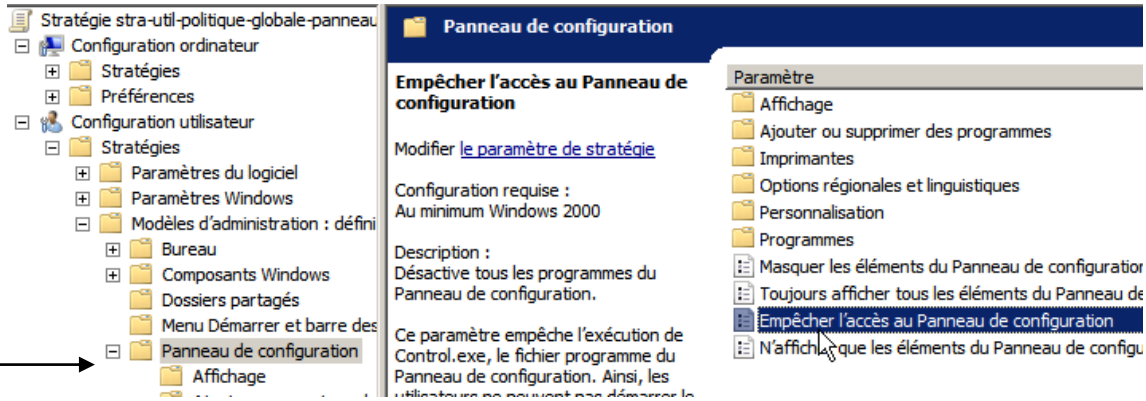
Interdire le panneau de configuration

stra-util-politique-globale-panneau-conf

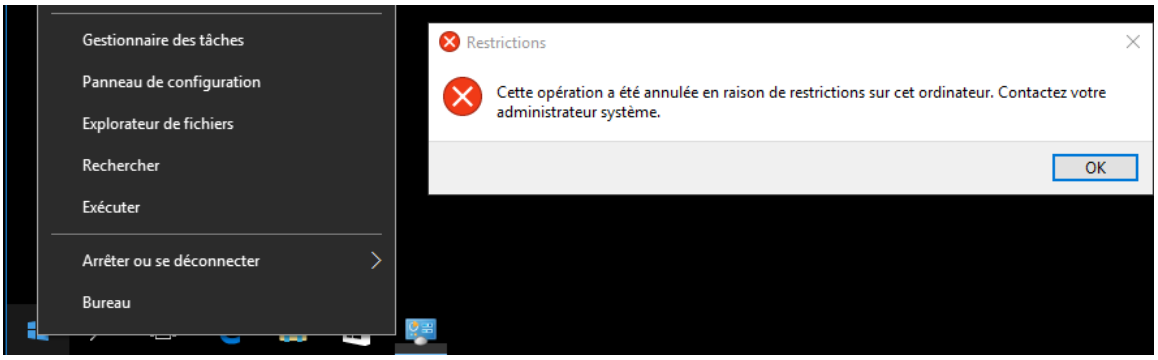
Qui contient donc

Configuration utilisateur / Strategies / Modèles d'administration,/ Panneau de configuration

Désactiver l'accès au Panneau configuration

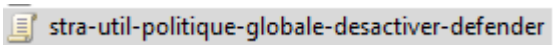


Si on essaye d'aller dans le panneau de configuration, ou les paramètres Windows 10, on obtiendra



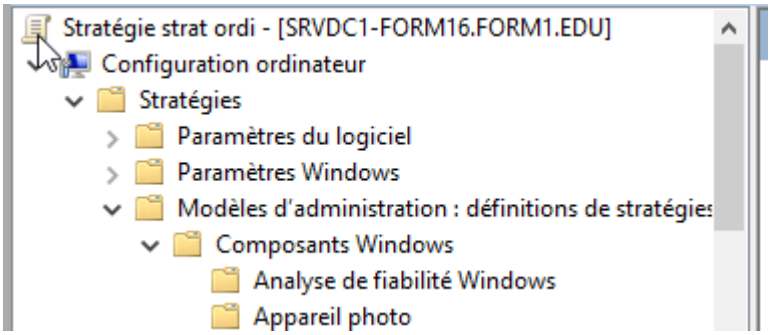
Désactiver Windows Defender

stra-util-politique-globale-desactiver-defender

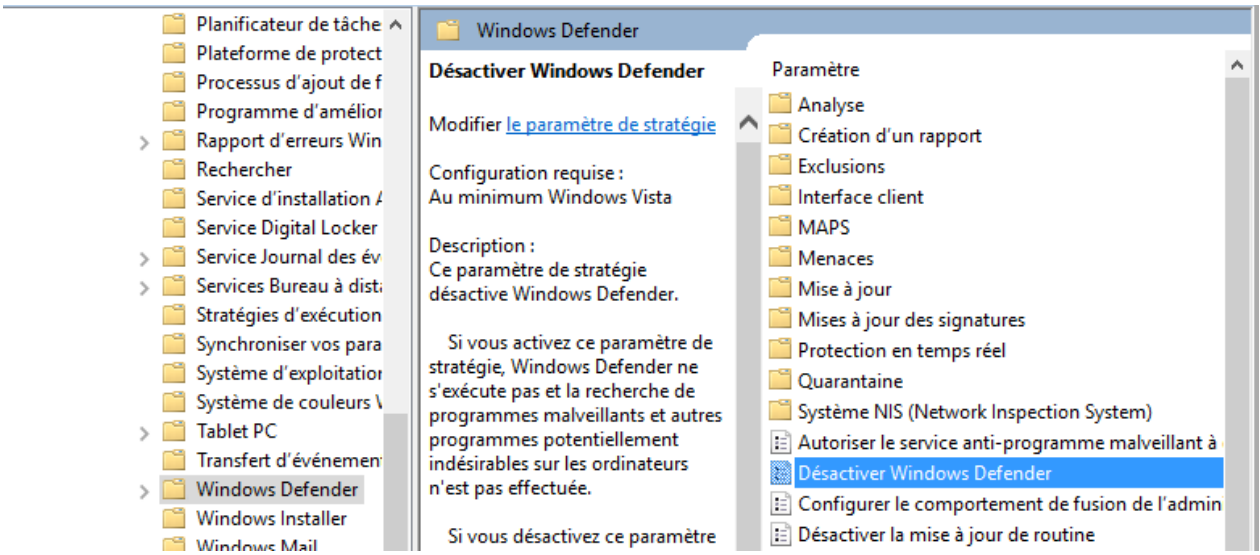


Qui contient donc

Configuration ordinateur / Modèles d'administration,/ Composant Windows / Windows defender



Et dans le composant windows defender on choisit Désactiver Windows Defender



GPO - SCRIPTS

Scripts de démarrage – arrêt – fin de session :

Lorsque l'on met en œuvre des scripts via les **GPO**, il est possible de placer trois nouveaux types de scripts

- Script de démarrage : s'exécute lors de l'allumage du poste
- Script de fermeture de session : s'exécute lors d'une fermeture de session
- Script d'arrêt : s'exécute lors d'un arrêt de la machine

Mais on peut aussi placer un script de type classique

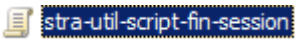
- Script d'ouverture de session : s'exécute lors d'une ouverture de session

Par défaut chaque script est réalisé avant la fin de l'autre (on parle de traitement synchrone). Les scripts **GPO** sont traités avant les scripts utilisateurs classiques.

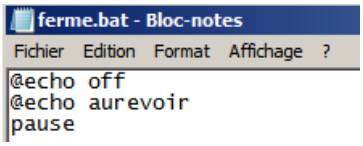
N.B : Par défaut les scripts de démarrage sont masqués.

Scripts de fin de session :

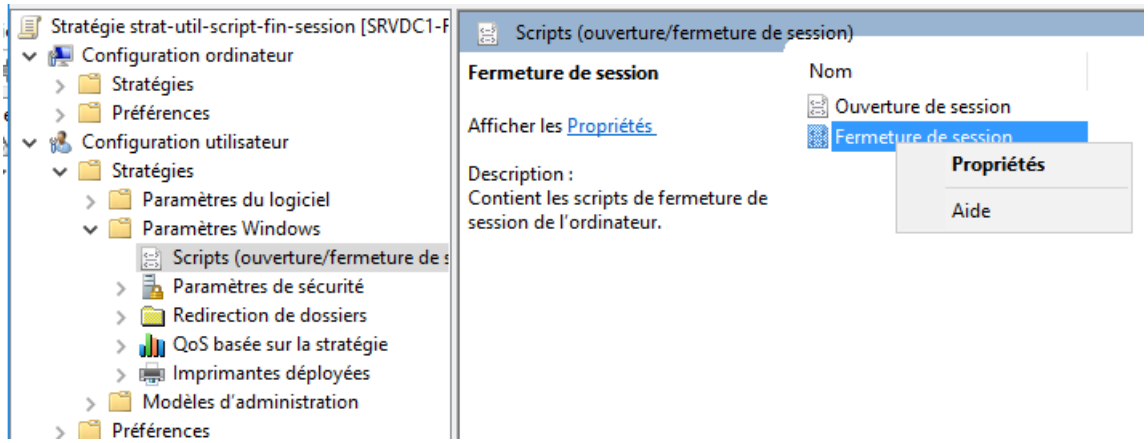
Créons nous une stratégie au nom parlant :

stra-util-script-fin-session 

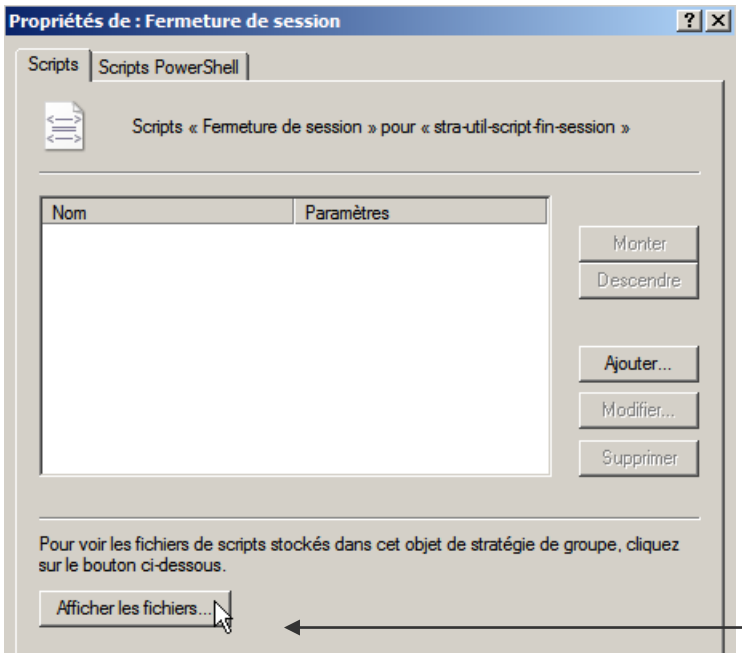
Pour utiliser un script de fin de session dans une **GPO**, (le script étant déjà écrit dans un fichier **.bat** ou **.vbs**, ou en **powershell,** par exemple « ferme.bat »…



Il faut demander les propriétés de Configuration Utilisateur / Stratégies / Paramètres Windows / Scripts / Fermeture de session



Pour avoir

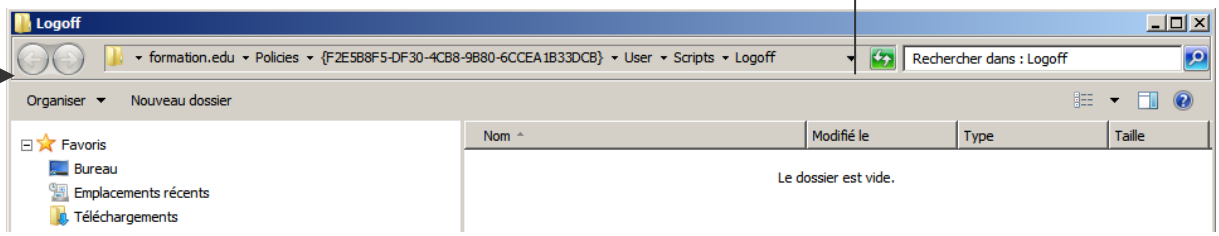


Il faut effectuer une manœuvre en deux temps :

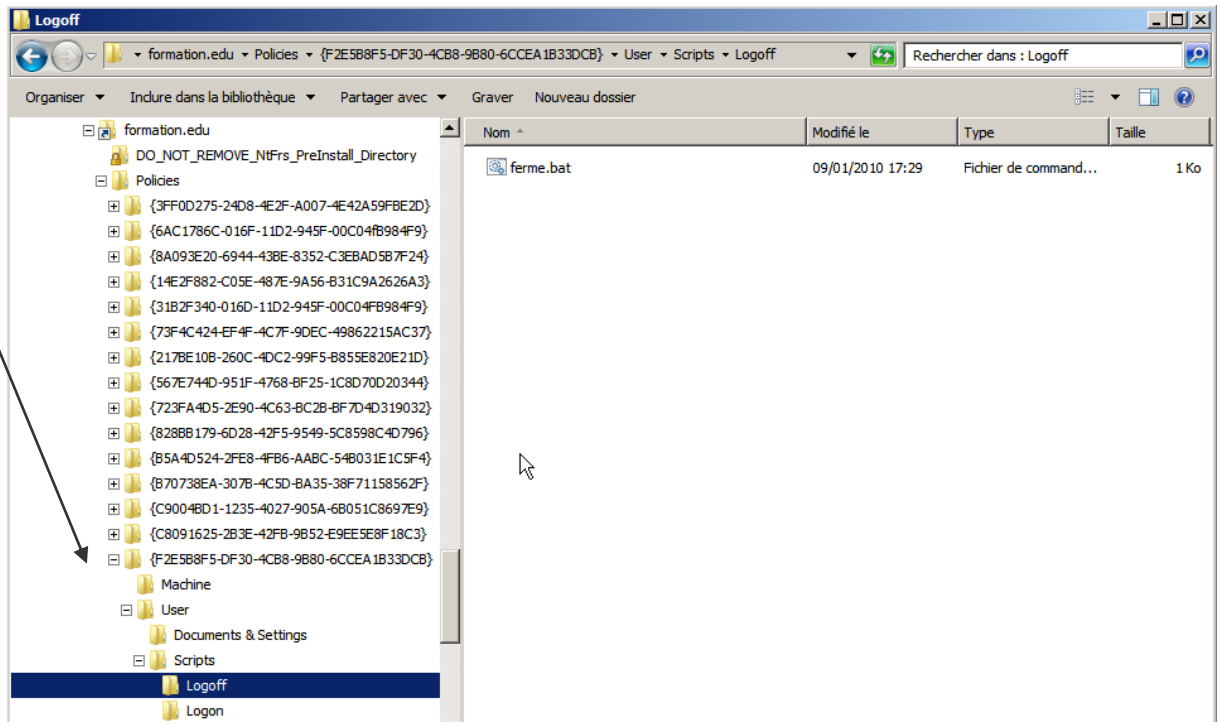
- D'abords il faut copier le script dans la **GPO**
- Puis il faut dire à la **GPO** d'utiliser ce script…

Copier le script dans la GPO : (Afficher…)

depuis la GPO, on demande le bouton **Afficher les fichiers…**



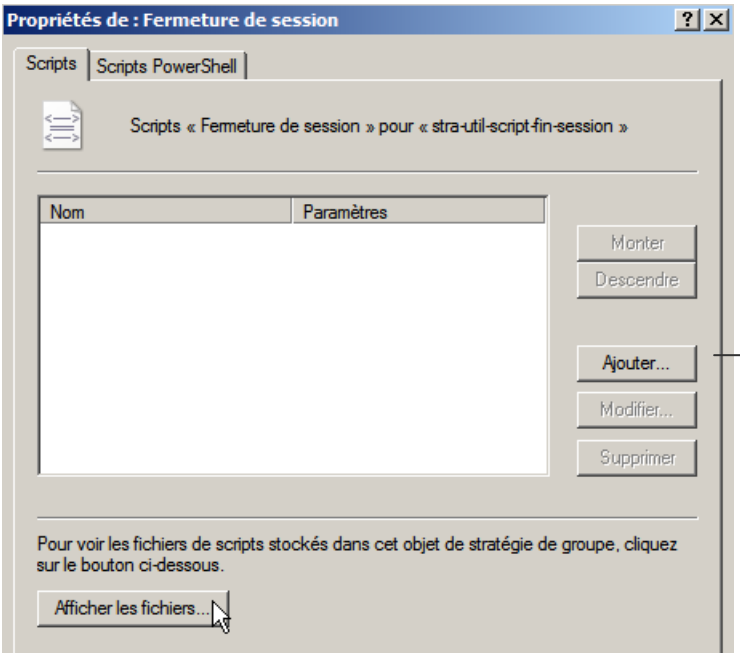
Une fenêtre s 'ouvre dans laquelle il faut copier notre script (donc ici **ferme.bat**)

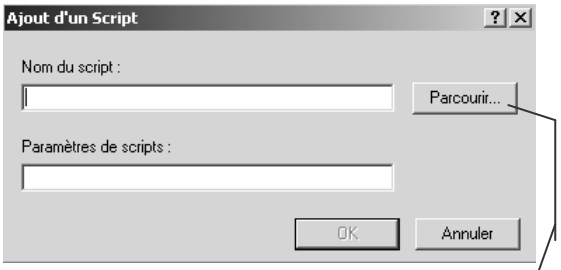


N.B : cette opération a simplement pour but de stocker dans notre **GPO** une copie du script, qui physiquement se trouve dans la stratégie **{F2E588F-DF30**…}

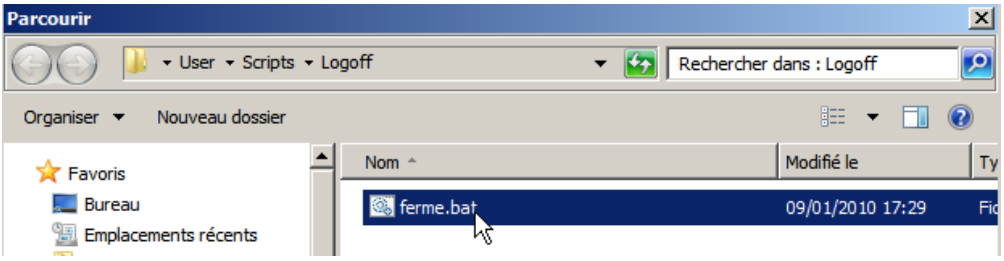
Utiliser le script dans la GPO (Ajouter…)

Pour utiliser le script dans la GPO, depuis la GPO, maintenant on demande le bouton **Ajouter**

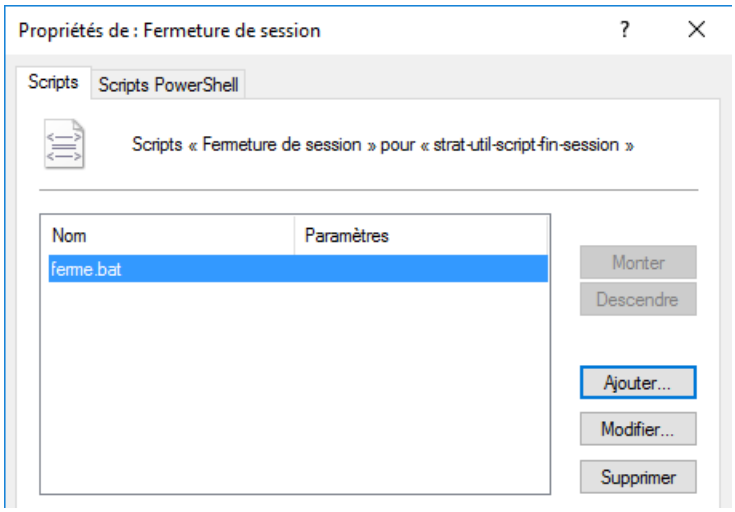




Et via **Parcourir** on prend un script parmi ceux existant dans la GPO (donc parmi ceux précédemment copiés)



Maintenant on a un script de déconnexion….



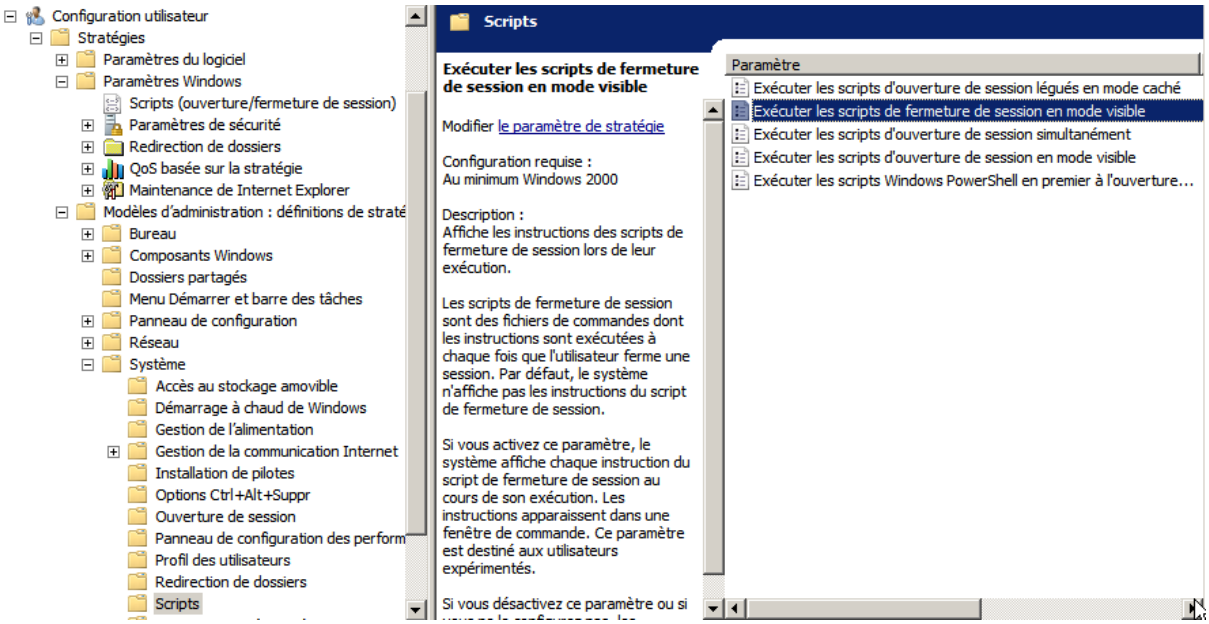
Parametrage execution du script :

Sachant que

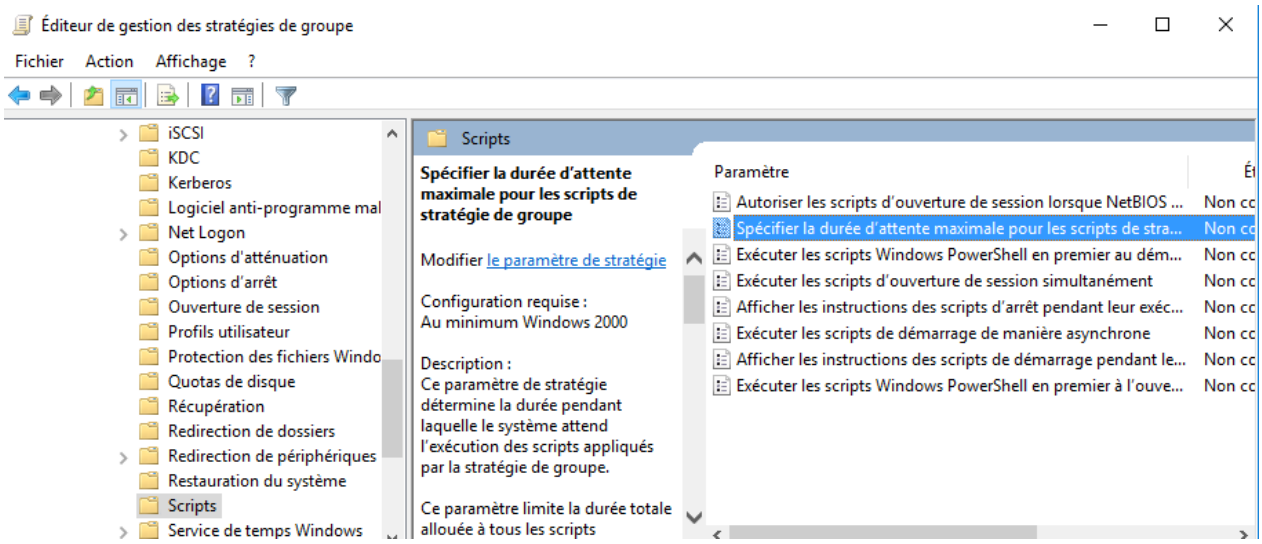
- les scripts de déconnexion s'exécutent par défaut en **mode caché**…
- les scripts disposent de **10 minutes** pour se réaliser, avant d'être interrompus.

Ainsi, une commande **pause**, dans un script de déconnexion, provoque le blocage pendant 10mn, puisque personne ne peut appuyer sur la touche …

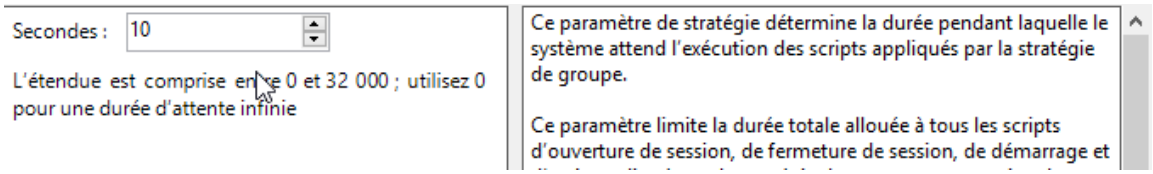
Il existe dans les stratégies utilisateur / Modèle d'administration / Système / Script, un réglage permettant d'exécuter les scripts de fermeture de session en mode visible…



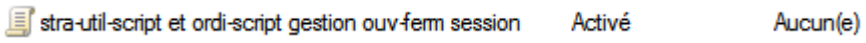
Il existe dans les de stratégies ordinateur / Modèle d'administration / Système / Script, un réglage pour paramétrer le délai d'attente maximal pour les scripts (tous les scripts)



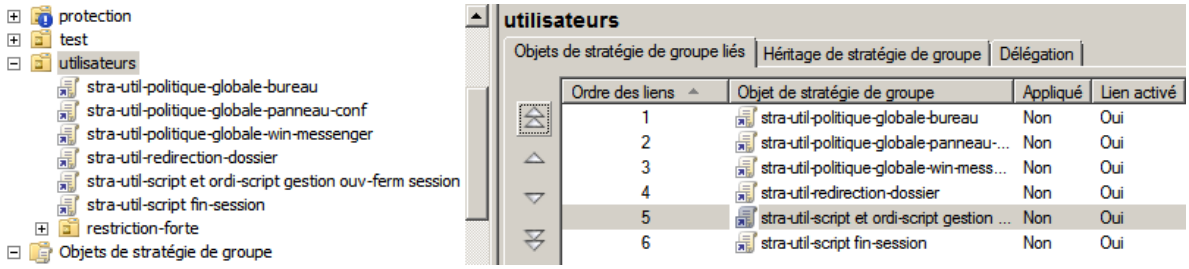
10 seconde cela suffira !



On pourrait faire une **stratégie ordinateur *ET* utilisateur** pour ces deux réglages…

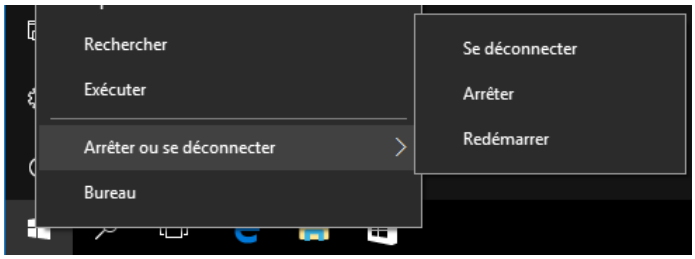


Du coup, il faut penser à appliquer non seulement notre stratégie de script, mais aussi notre stratégie de réglage… et dans le bon ordre !

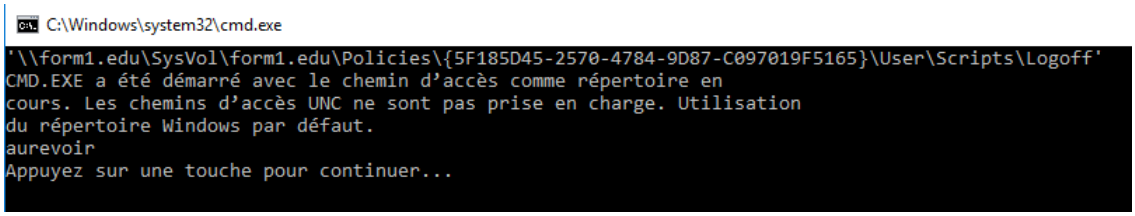


Test et visualisation :

Au moment de la deconnexion,



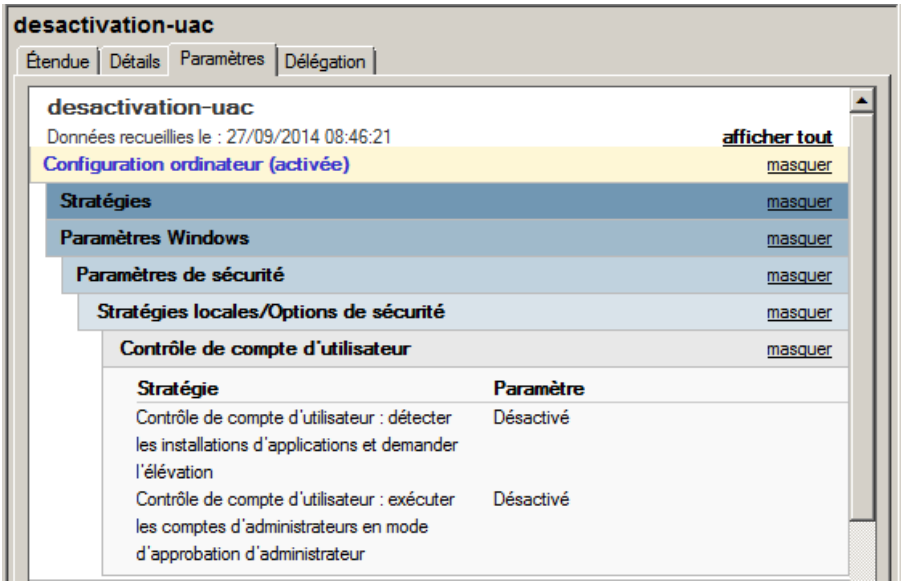
on devrait voir apparaître



Et si on ne fait rien, au bout de 10S le script est interrompu !

Désactivation UAC:

Pour l'exécution de certains scripts il peut être nécessaire de désactiver l'UAC



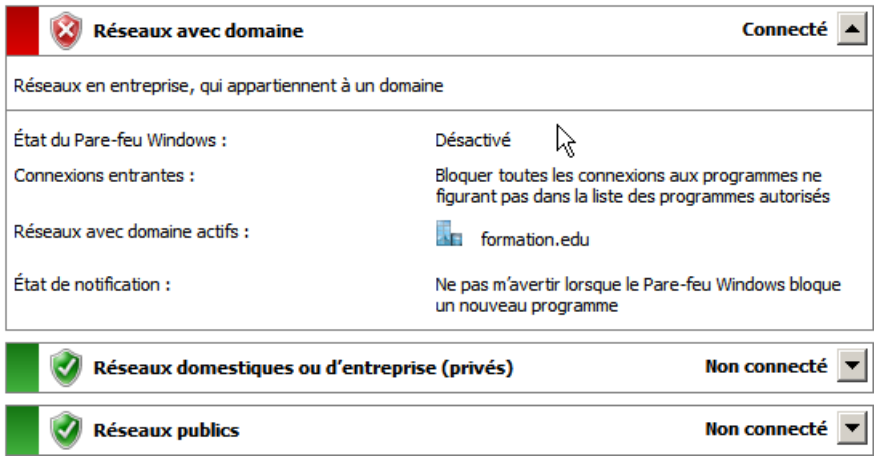
GPO – SCRIPTS - NETSH

Paramétrage via fichier wfw:

On peut utiliser la possibilité d'exploiter un fichier de paramétrage **.wfw** (cf chapitre Stratégie Locale Pare-feu Seven) via la commande **netsh** dans une stratégie de script.

On veut globalement que le pare-feu soit

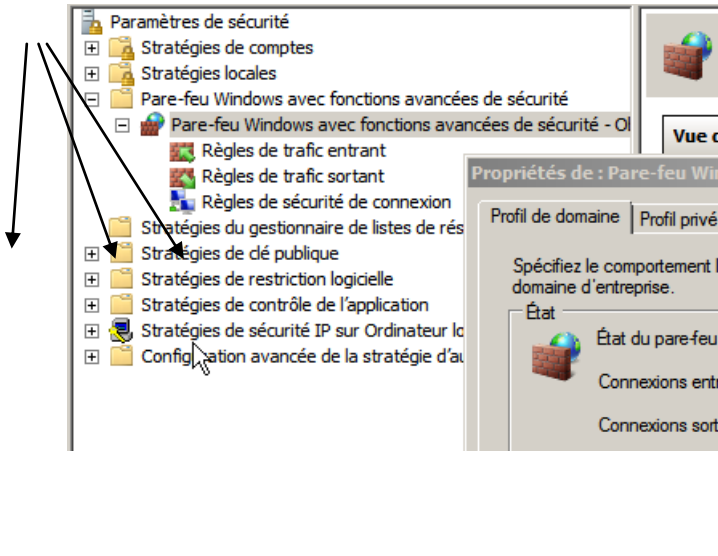
- Désactivé pour le profil de domaine
- Activé par défaut sur les profils Privé et Public



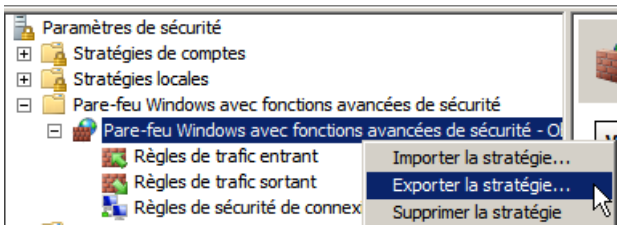
La séquence serait :

1. Création d'une stratégie locale effectuant le réglage (sur une machine tierce, sinon penser à la supprimer ensuite)
2. Génération du fichier de paramétrage **.wfw**
3. Création du script avec la commande **netsh** mettant en place ce fichier **.wfw**
4. Incorporation dans une GPO de script utilisateur
5. Test

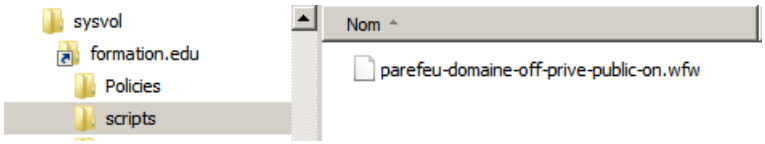
Création d'une stratégie locale avec nos réglages



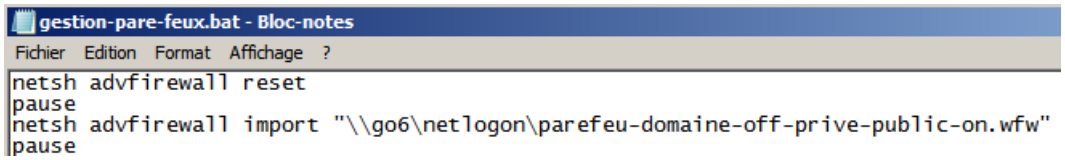
Génération du fichier de paramétrage .wfw



Mise à disposition du fichier de configuration **.wfw** dans **netlogon** (par exemple)

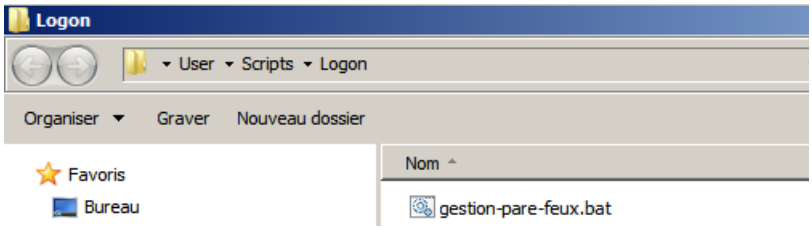


Et Création du script avec la commande **netsh** mettant en place ce fichier **.wfw**

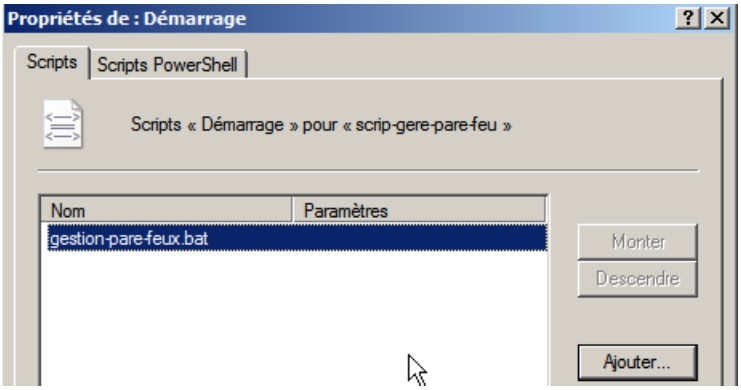


Incorporation dans une GPO de script utilisateur

Dans la GPO il faut incorporer le batch



et on indique le script a utiliser



Paramétrage via commande netsh directe:

Une variante serait d'utiliser **netsh** sans passer par un fichier de configuration…

```
netsh advfirewall reset
netsh advfirewall set domainprofile state off
netsh advfirewall set publicprofile state on
netsh advfirewall set privateprofile state on
```

GPO VS SCRIPTS ARRET PC

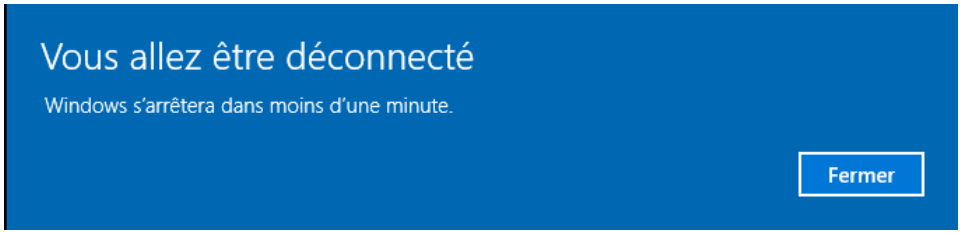
Windows commande Shutdown:

La commande shutdown est disponible désormais nativement sur les postes Windows 10

Syntaxe de base shutdown –s –f –m\\@IP ou shutdown –s –f –m\\nomhôte

Comme par exemple dans

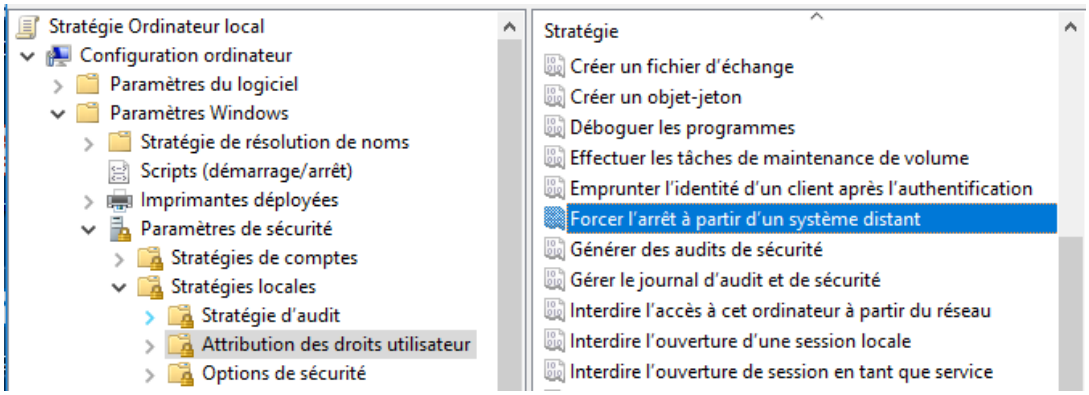
```
D:\gpo>shutdown -s -f -m \\192.168.1.171
```

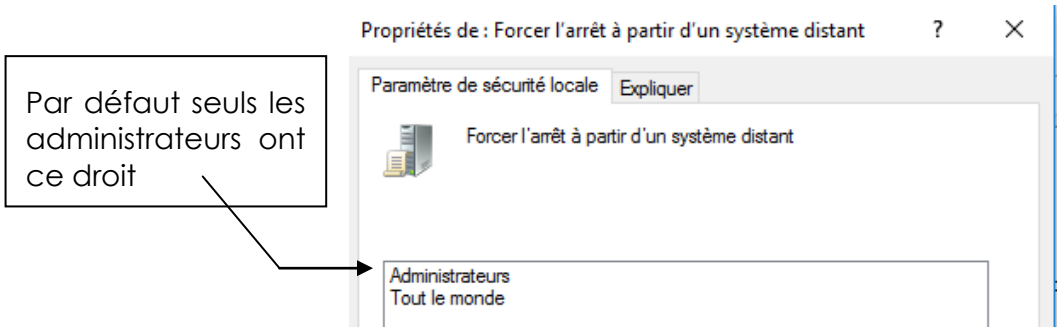


N.B : il peut y avoir un problème d'accès

```
D:\gpo>shutdown -s -f -m \\192.168.1.171
192.168.1.171: Accès refusé.(5)
```

Stratégie de Sécurité Locale / Attribution des droits utilisateurs et Forcer l'arrêt à partir d'un système distant





Il n'y a plus qu'à se construire une **GPO** pour gérer les droits d'arrêt via un accès distant stra-ordi-autorisation-arret-acces-distant

N.B : Attention a qui l'on ajoute (ici **Tout le monde**), et verifier par **RSOP** les droits finaux, car cette **GPO** existe au niveau de la **default Domain policy**

On peut affiner un peu la commande, avec une tempo et un message explicatif pour l'utilisateur

```
D:\gpo>shutdown /s /f /t 60 /c "arrêt pc fin de journée ! " /m \\192.168.1.171
```

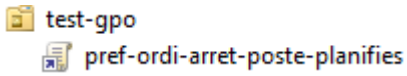
Il n'y a plus qu'a faire un script avec l'ensemble des postes à eteindre, puis lancer le script , soit manuellement, soit par le planificateur de tâches

---

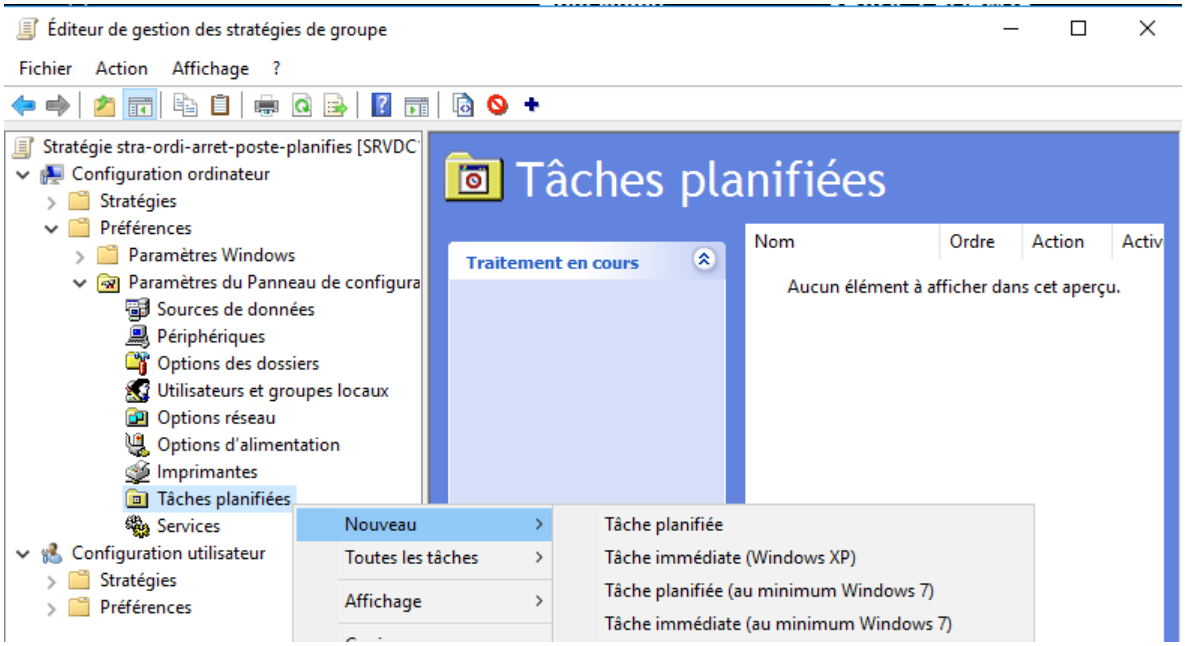
GPO – Préférence planification arrêt shutdown des postes:

La commande **shutdown** étant disponible désormais nativement sur les postes Windows on va se construire une GPO Tâche planifiée

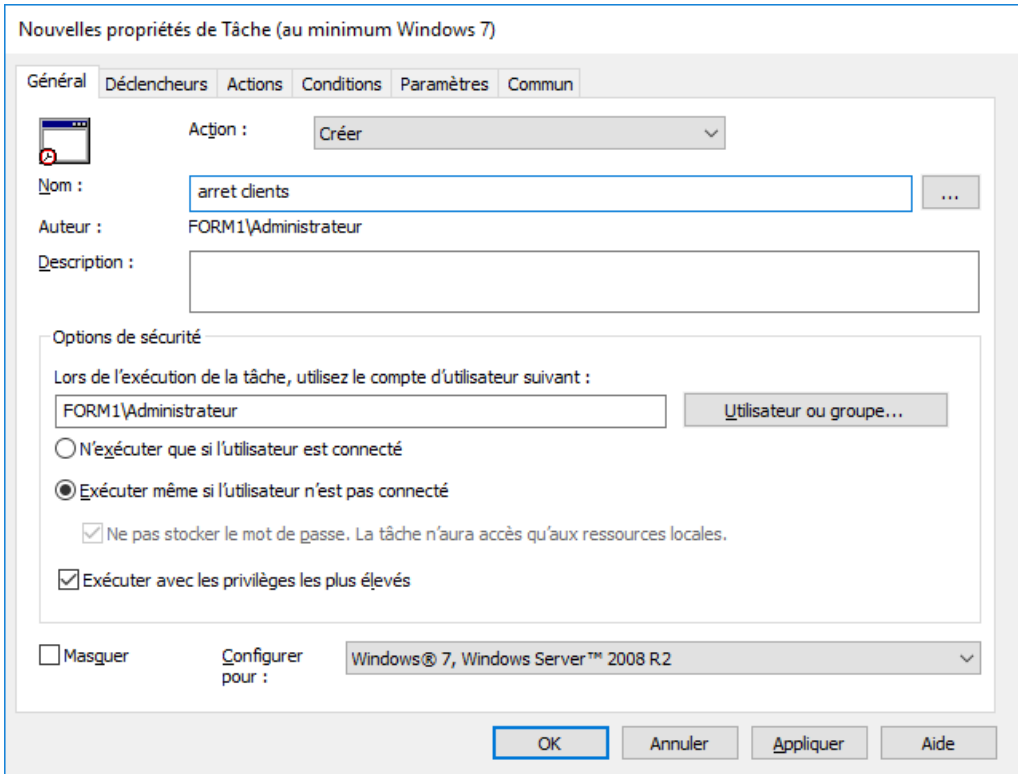
Cette GPO va créer un tache planifiée sur chaque machine ciblée, avec comme invocation la commande shutdown. C'est donc chaque machine qui lance sa propre tâche d'arrêt…



Configuration ordinateur / Préférences / Paramètres panneau de configuration / Tâches planifiées. Puis Nouveau / tâche planifiée (au minimum Windows 7)

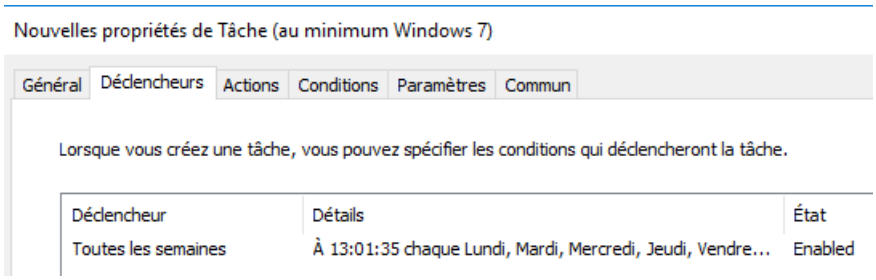


Onglet **Général**:

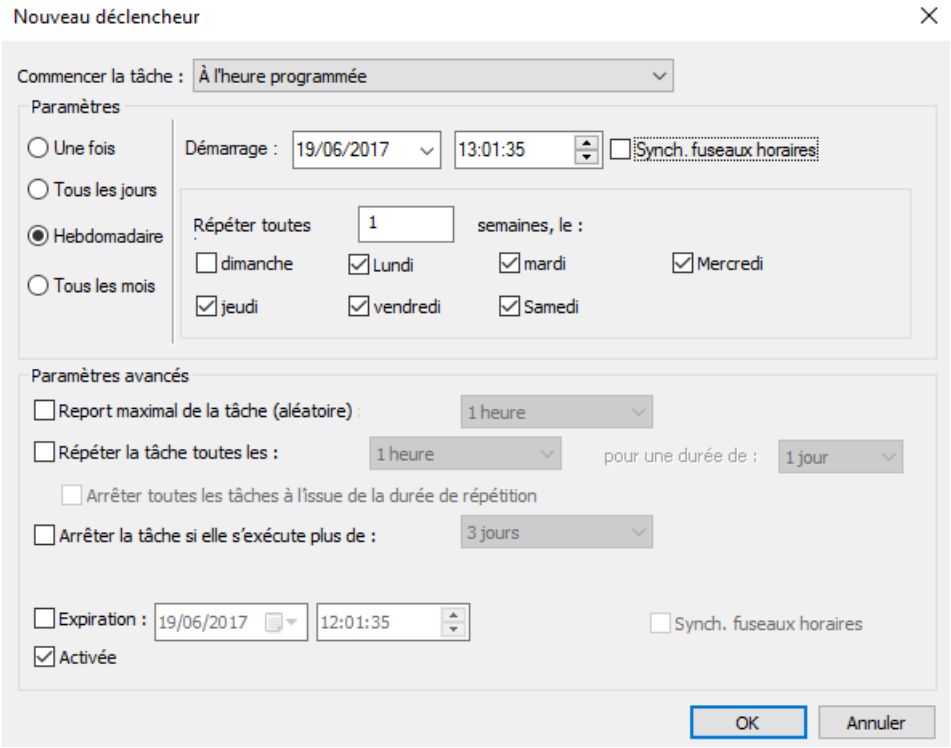


- Action : Remplacer (ou créer)
- Compte administratif avec droits admin domaine et membre admins locaux. -« Executer même si l'utilisateur n'est pas connecté » coché

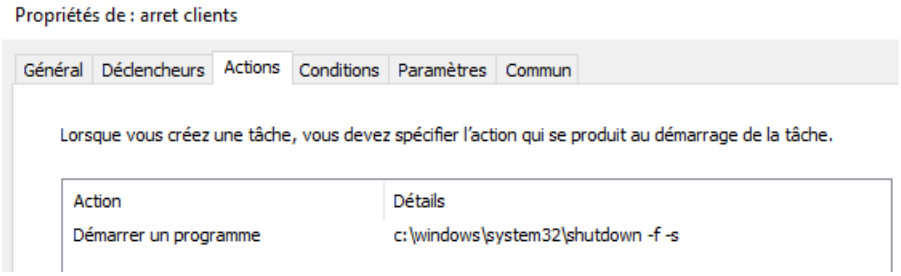
Onglet Déclencheurs :



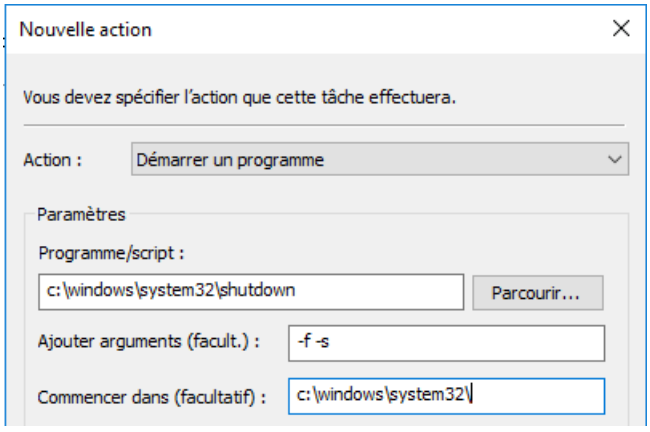
- A l'heure programmée /Hebdomadaire / du lundi au samedi / à 22h00 / Paramtres avancés : Activée



Onglet **Actions** :

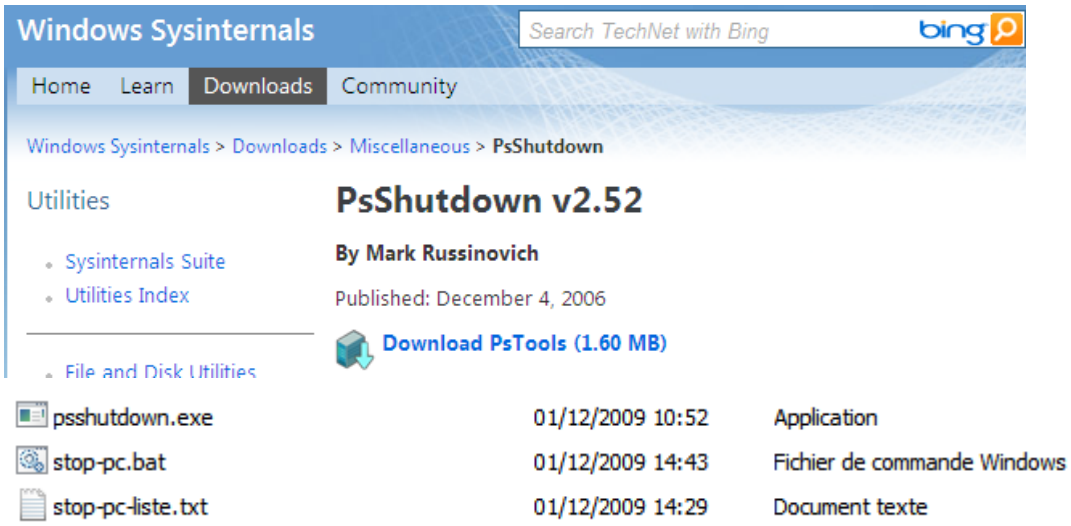


Avec Démarrer un programme / C:\Windows\System32\shutdown.exe / Arguments : -f –s



Utilitaires Psshutdown:

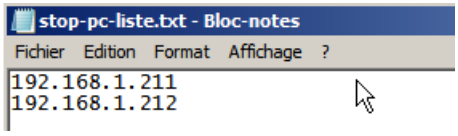
L'utilitaire **PsShutdown** de **sysinternal** peut être lancé depuis un batch…



La commande de base serait

psshutdown ***@****stop-pc-liste.txt* ***-u*** *formation.edu\admin* ***-p*** *Domaine2008* ***-k***

avec un fichier *texte stop-pc-lste.txt* de la forme



N.B: en commande en ligne, on ne peut pas donner une addresse ip, mais seulement un nom machine sous la forme \\non

Les options pour une commande un peu moins violente pourraient être

- c

permettre à l'utilisateur d'interrompre l'arrêt s'il est sur sa machine

-t pour attendre 5min avant la mise en arrêt de la machine

- **m**

pour mettre un petit message.

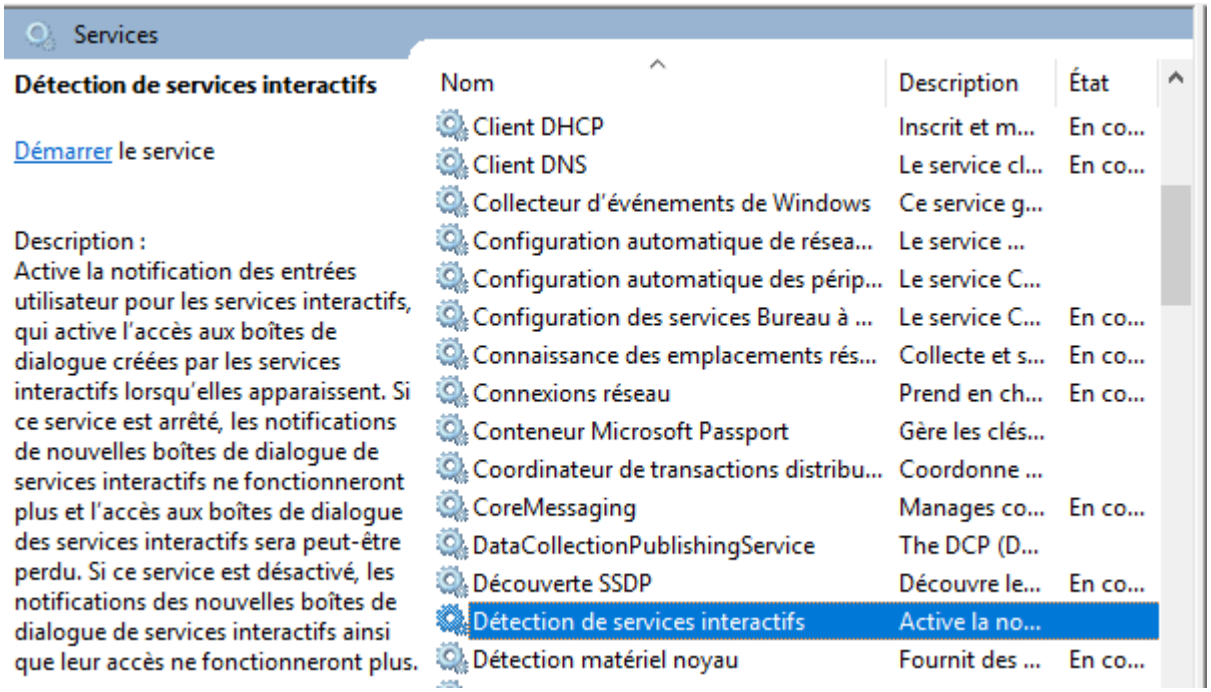
Comme dans

psshutdown *@stop-pc-liste.txt* **-u** formation.edu\admin -p Domaine2008 **-c -k -t** 120 **-m** « Extinction ordinateur ! Pour interrompre cliquez sur CANCEL »

stop-pc.bat - Bloc-notes

Fichier Edition Format Affichage ?

```
rem psshutdown \\* -u formation.edu\admin -p Domaine2008 -k -t
rem pour toutes les machines du domaine
rem tempo de 20s

rem psshutdown @stop-pc-liste.txt -u formation.edu\admin -p Domaine2008 -c -k -t 120
rem pour les machines specifiees dans un fichier texte nommé stop-pc-liste.txt, ayant
rem un compte administrateur "admin" et mot de passe Domaine2008
rem tempo de 2 min et une possibilité d'interrompre

rem psshutdown @stop-pc-liste.txt -u formation.edu\admin -p Domaine2008 -c -k -t 120 -m "Extinction ordi
rem idem ci dessus avec un message

rem psshutdown @stop-pc-liste.txt -u formation.edu\admin -p Domaine2008 -k
rem immediat

rem psshutdown \\pcxp -u pcxp\administrateur -p local -c -t 30 -m "arret"
rem pour une machine en workgroup, nommée pcxp avec un compte administrateur, mdp local

psshutdown \\pc7 -u pc7\administrateur -p local -c -k -t 30 -m "arret"
rem pour une machine en workgroup, nommée pc7 avec un compte administrateur, mdp local
```



GPO - INSTALLATION DE LOGICIELS

Les 3 éléments Winstaller – GPO - AD

Une nouveauté de windows 2000-2003 , et maintenue avec 2008 consiste en un système d'installation et de maintenance de logiciel, utilisant **AD** (Active Directory), les **GPO** (stratégies de groupe), et **Windows installer**

L'ordre logique dans lequel ces fonctionnalités vont jouer est le suivant :

1. **Windows Installer** est utilisé pour l'installation administrative d'un logiciel
2. Les **GPO** sont utilisées pour définir une stratégie quant à cette installation
3. **Active Directory** est là pour déployer cette stratégie

Windows installer et fichiers msi

Le service **Windows installer** est un service client automatisant entièrement la procédure d'installation et de désinstallation de logiciel, à condition d'avoir un « package windows installer » correspondant à l'application à installer. Ce package est plus connu sous l'appellation du **fichier MSI** (**Microsoft installer**)

Le fichier **MSI** est donc en fait un package contenant :

- Un fichier de réponse automatisé
- tous les fichiers nécessaires à l'installation de l'application…

Les fichiers **MSI** font aussi des installations **classiques locales** de tout logiciel, grâce à la présence dans l'OS du composant Windows Installer.

- Si l'OS n'a pas **Windows Installer**, une **mise à niveau du système sera nécessaire**
  C'est pour cette raison que certaines installations demandent un redémarrage du poste, car d'abords en fait elles installent **Windows installer**, puis elles font « lire » le fichier **msi** par le **Windows installer** pour installer l'application proprement dite.
- Si l'on **veut une installation réseau**, type installation administrative d'office, les fichiers msi et windows installer **ne savent pas faire**

La présence de **Windows installer** est vérifiable par la présence du fichier **msiexec.exe,** présent en général dans le dossier système.

Aujourd'hui toutes les applications récentes sont livrées avec un fichier **MSI** destiné à être interprété par un Windows installer

Si on n'a pas de fichier **Msi,** il est impossible de se créer une stratégie d'installation automatisée. Il existe des outils professionnels permettant de créer des fichier msi, notamment ***Installshield***, et ***Wyse installer***

Procédure d'installation et de maintenance logiciels

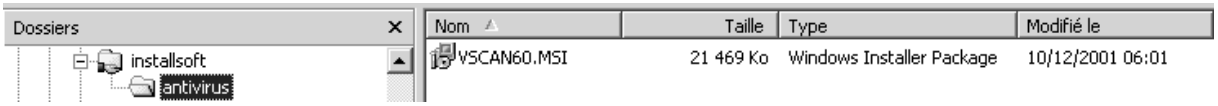
Il va falloir exécuter les étapes suivantes :

1. Il faut créer une GPO qui installe le logiciel sur l'ordinateur, soit lors du démarrage du poste, soit lors du « lancement » de l'application (qui paraît comme disponible) de la part de l'utilisateur.
   cette phase peut être qualifiée de **déploiement** .
2. Le logiciel déployé peut être mis automatiquement à niveau, ou redéployé au démarrage du poste ou lorsqu'un utilisateur lance sa session.
   cette phase peut être qualifiée de **maintenance** .
3. Le logiciel peut être automatiquement supprimé au démarrage du poste ou lorsqu'un utilisateur lance sa session.

Création du point d'installation de logiciel

Il faut copier les package Windows installer, c'est à dire le fichier **msi** vers un **point de distribution** du logiciel.

Par exemple



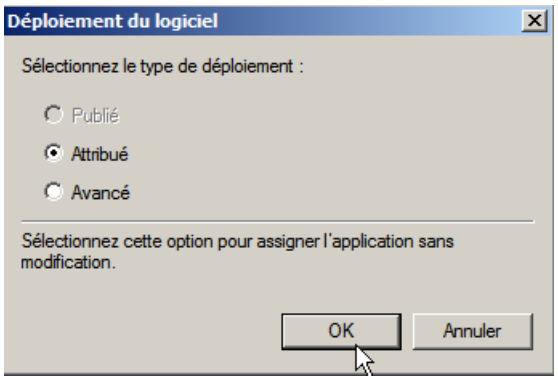
Ce **point de distribution** est généralement un dossier partagé sur le serveur, mais cela peut être un emplacement réseau quelconque…

C'est en fait simplement un dossier sur lequel on peut si on veut donner des permissions en lecture seule…, partager le dossier de manière administrative ($), pour le rendre invisible…

N.B : il faut impérativement donner un **point de distribution réseau**, et non pas un chemin local !

Attribution - Publication de logiciel

L'attribution ou la **Publication** sont les deux options de distribution de logiciel possibles



L'attribution permet d'être sûr que le logiciel est présent sur l'ordinateur voulu. Avec une attribution on peut affecter les logiciels à des **utilisateurs**, ou a des **ordinateurs**.

- Si on les affectent à des **ordinateurs** : il n'y a pas d'annonce, le logiciel est automatiquement installé lors de l'allumage du poste. (sauf pour les CD)

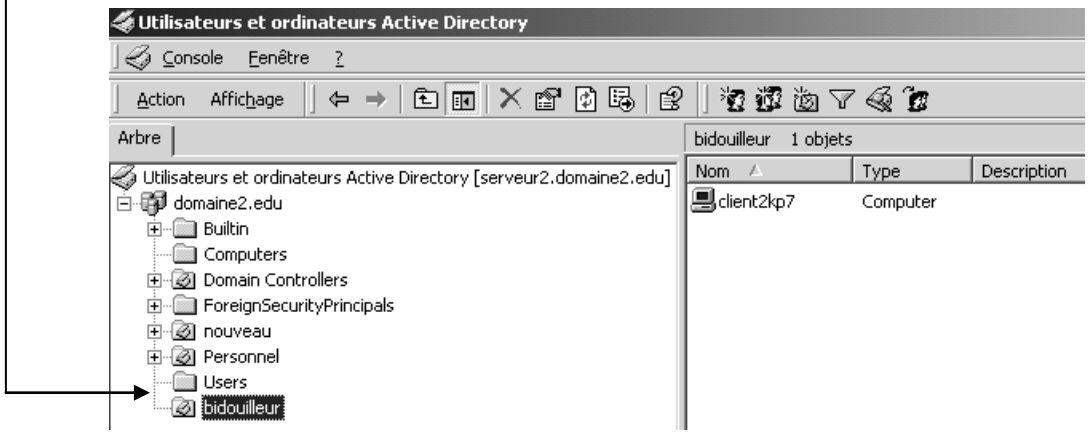
- Si on les affectent à des **utilisateurs** : lorsque l'utilisateur ouvre un session, le logiciel est annoncé (raccourcis présents) , mais l'installation ne débute réellement que si l'utilisateur clique sur l'application ou double-clique sur un fichier associé.

La Publication permet que le logiciel soit installable sur l'ordinateur voulu. Avec une publication on peut affecter les logiciels uniquement pour des **utilisateurs**, mais pas pour des ordinateurs.

En effet lors de la publication de logiciels, il n'y a pas d'annonce. L'utilisateur peut/doit installer l'application en passant par **ajout/suppression programme**, ou l'installation se fait automatiquement via un double clic sur un fichier associé

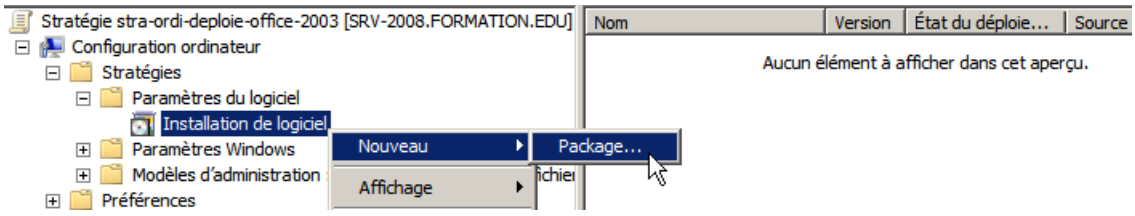
Stratégie de déploiement de logiciel

On va créer une **GPO** sur une **OU** contenant les machines des **bidouilleurs**, et leur installer un antivirus dès le démarrage du poste



Sur cette OU on va poser une GPO que l'on nomme de manière explicite

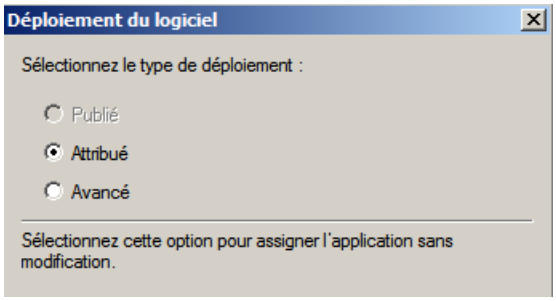
Cette GPO contient une définition de **Paramètres logiciel** dans **Configuration d'ordinateurs (ou utilisateurs)**



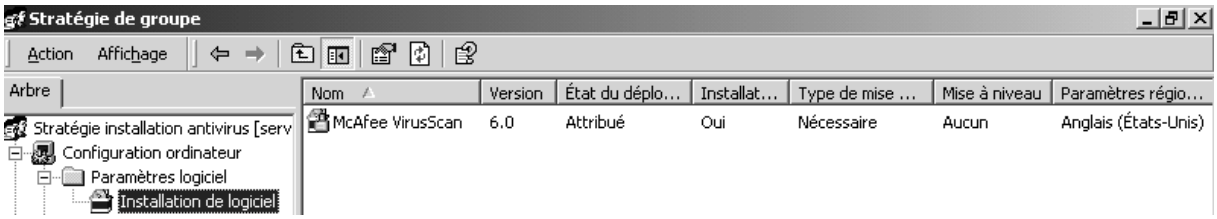
Pour laquelle on demande via un clic droit **Nouveau / Package…**

et on va

1. chercher le chemin du dossier de distribution (via le réseau bien sûr)
2. indiquer le type de déploiement

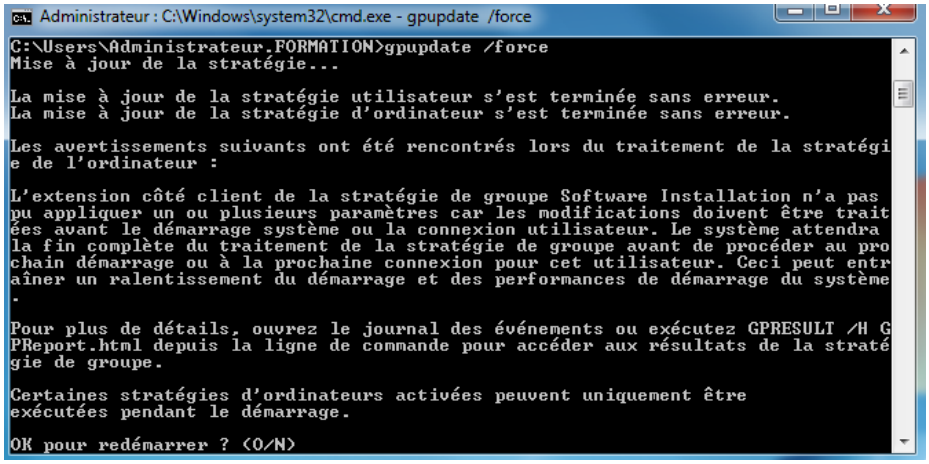


pour obtenir finalement



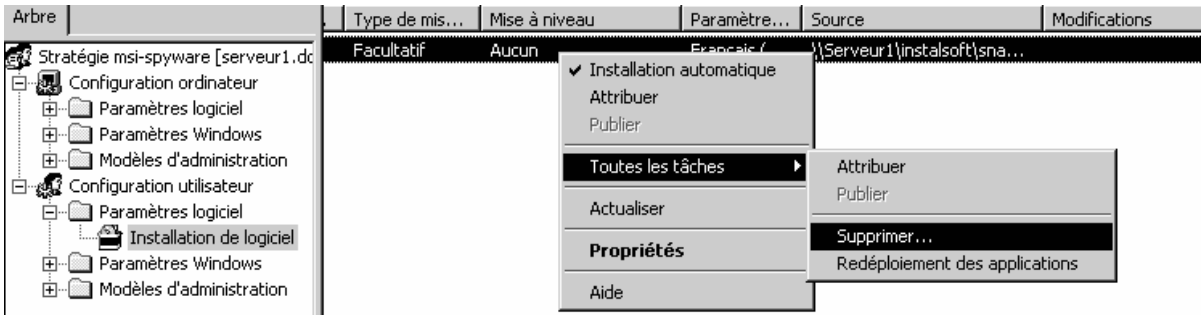
NB: si on travaille au niveau de la configuration d'utilisateur, à l'ouverture de session on récupère le MSI

NB: si on travaille au niveau de la configuration d'ordinateur, il faut arrêter et re-démarrer le poste pour récupérer le MSI

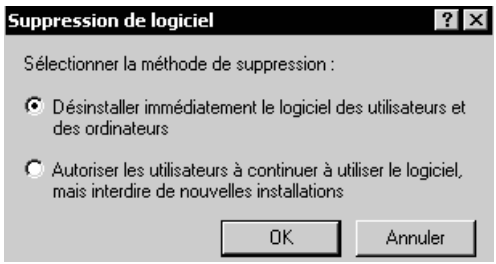


Stratégie de re-déploiement / désinstallation

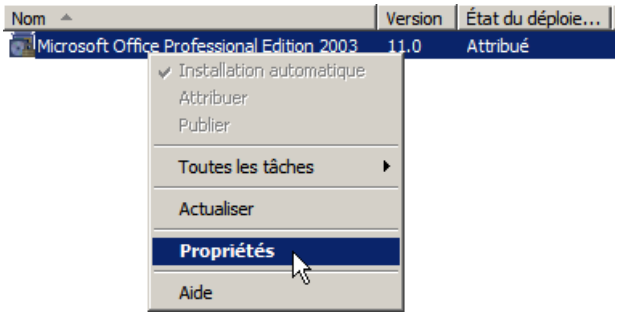
En se plaçant sur la stratégie, on demande **toutes les tâches / supprimer**



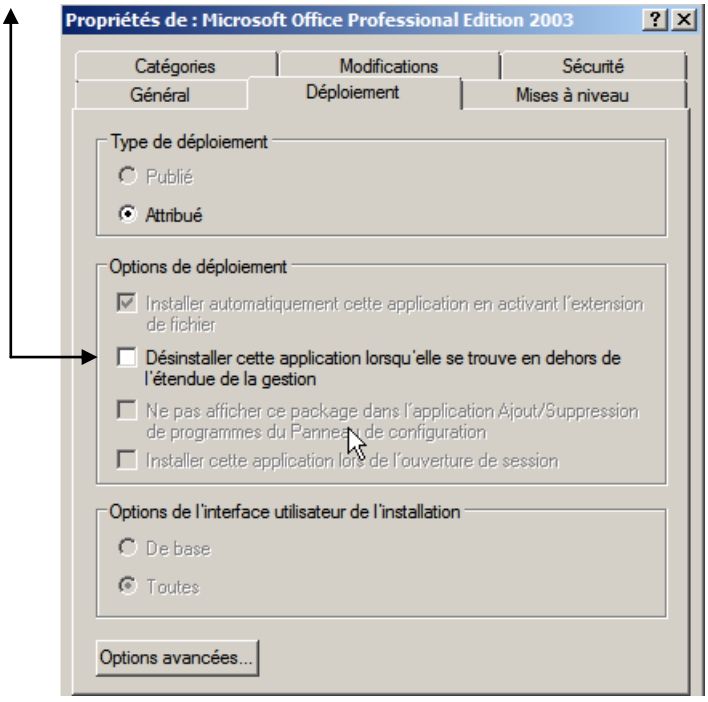
et là on peut choisir **Supprimer** ou **redéploiement des applications**, avec



Propriétés de déploiement de logiciel



Donnant

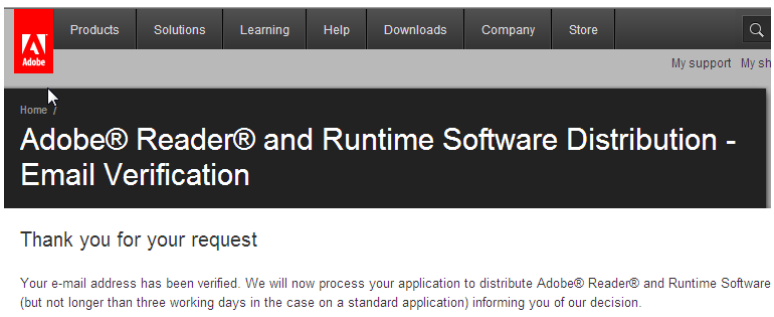


DEPLOYER ADOBE READER PAR MSI

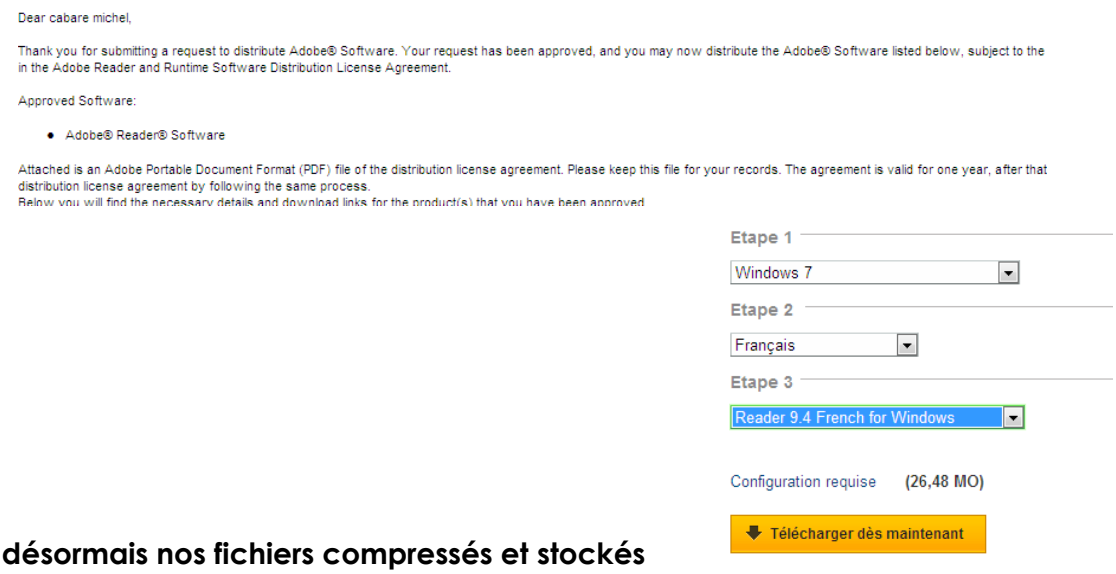
Récupération Fichier Adobe :

Il faut d'abord demander sur le site de adobe une autorisation de distribution, et non pas un téléchargement du logiciel pour usage local…

Ceci afin de récupérer un source ne demandant pas d'interaction lors de son installation (nom, licence…)(il faut un compte adobe, et un échange d'emails…)



On reçoit un mail avec un lien… Permettant de télécharger les sources



Dear cabare michel,

Thank you for submitting a request to distribute Adobe® Software. Your request has been approved, and you may now distribute the Adobe® Software listed below, subject to the in the Adobe Reader and Runtime Software Distribution License Agreement.

Approved Software:

- Adobe® Reader® Software

Attached is an Adobe Portable Document Format (PDF) file of the distribution license agreement. Please keep this file for your records. The agreement is valid for one year, after that distribution license agreement by following the same process.
Below you will find the necessary details and download links for the product(s) that you have been approved.

On a désormais nos fichiers compressés et stockés localement…

AdbeRdr1001_fr_FR.exe	10/03/2011 16:27	Application	46 806 Ko
AdbeRdr940_fr_FR.exe	10/03/2011 16:19	Application	27 120 Ko
AcroRdrDC1700920044_fr_FR.exe	21/06/2017 07:34	Application	107 614 Ko

Décompression Fichier Adobe :

On veut décompresser une version… La syntaxe est particulière à adobe,

The general form of the command to convert a Nosso-compressed file to an MSI package is:

```
<path to>\AdbeRdr90_en_US.exe [<switches>...]
```

where: `<switches>` can consist of either Nosso or Adobe switches.

The values for the `NOS-Switches` are shown in Table A.1.

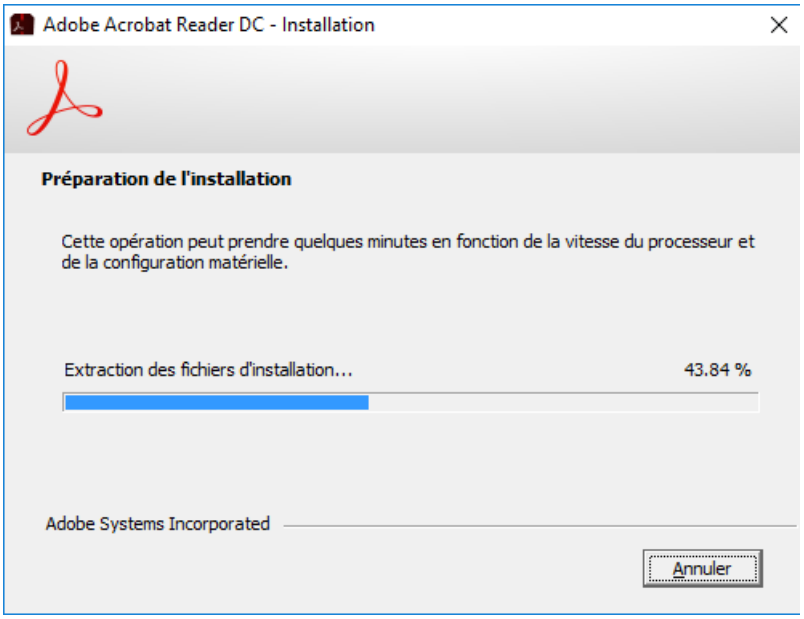
TABLE A.1 Switches for Expanding Nosso Installer

Argument	Description
`-nos_ne`	Do not execute any file after installation (overrides the `-e` switch) This switch should be used if user only wants to extract the installer contents and not run the installer.
`-nos_nd`	Do not delete files after installation (overrides the `-r` switch) The `-r` switch uses the existing folder and overwrites the extraction files to the same folder without creating an additional extraction folder.
`-nos_o`	Specifies the name of folder where the contents of the expanded package are to be placed. The folder name should be enclosed in quotation marks. It is best i f you do not use an existing folder, and there should be no space following the "-nos_o". For example: <path to>\AdbeRdr90_en_US.exe -nos_o"TestFolder" -nos_ne
`/sAll`	This switch specifies that installation will be run in silent mode.

Pour nous cela se traduirait par exemple par

```
AcroRdrDC1700920044_fr_FR.exe -nos_o"c:\readerdc2017" -nos_ne
```

AcroRdrDC1700920044_fr_FR.exe –nos_o"c:\readerdc2017" –nos_ne



Pour désarchiver le fichier dans un dossier nommé « readerdc2017 »…

abcpy.ini	05/04/2017 04:14	Paramètres de co...	1 Ko
AcroRdrDCUpd1700920044.msp	05/04/2017 04:14	Correctif Window...	90 340 Ko
AcroRead.msi	17/03/2015 09:41	Package Windows...	2 740 Ko
Data1.cab	17/03/2015 09:35	Fichier CAB	175 026 Ko
setup.exe	05/04/2017 04:14	Application	453 Ko
setup.ini	05/04/2017 04:14	Paramètres de co...	1 Ko

AdbeRdr1001_fr_FR.exe –nos_o"c:\reader10" –nos_ne

Pour désarchiver le fichier dans un dossier nommé « reader10 »…

ABCPY.INI	10/11/2010 21:49	Paramètres de co...	2 Ko
AcroRead.msi	10/11/2010 22:03	Package Windows...	2 267 Ko
AdbeRdrUpd1001_Tier1.msp	30/01/2011 21:44	Correctif Window...	12 135 Ko
Data1.cab	10/11/2010 22:03	Fichier CAB	118 953 Ko
setup.exe	30/01/2011 21:44	Application	330 Ko
Setup.ini	30/01/2011 21:44	Paramètres de co...	1 Ko

AdbeRdr940_fr_FR.exe –nos_o »reader9-4 » –nos_ne

Pour désarchiver le fichier dans un dossier nommé « reader9-4 »…

abcpy.ini	11/12/2007 22:29	Paramètres de co...	2 Ko
AcroRead.msi	23/09/2010 15:09	Package Windows...	3 908 Ko
Data1.cab	23/09/2010 15:07	Fichier CAB	122 634 Ko
Setup.exe	23/09/2010 06:28	Application	338 Ko
setup.ini	25/08/2006 19:01	Paramètres de co...	1 Ko

Msiexe /a - Création d'un AIP Administration Installation point :

La commande **msi.exe** est dotée de paramètres que l'on peut utiliser selon les cas

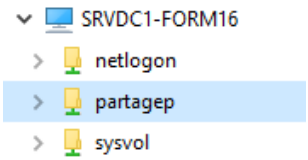
/a	*Package*	Administrative installation option. Installs a product on the network.

Administrative Installation

The Windows Installer can perform an administrative installation of an application or product to a network for use by a workgroup. An administrative installation installs a source image of the application onto the network that is similar to a source image on a CD-ROM. Users in a workgroup who have access to this administrative image can then install the product from this source. A user must first install the product from the network to run the application. The user can choose to run-from-source when he installs and the installer uses most of the product's file directly from the network.

Administrators can run an administrative installation from the command line by using the /a **command line option**.

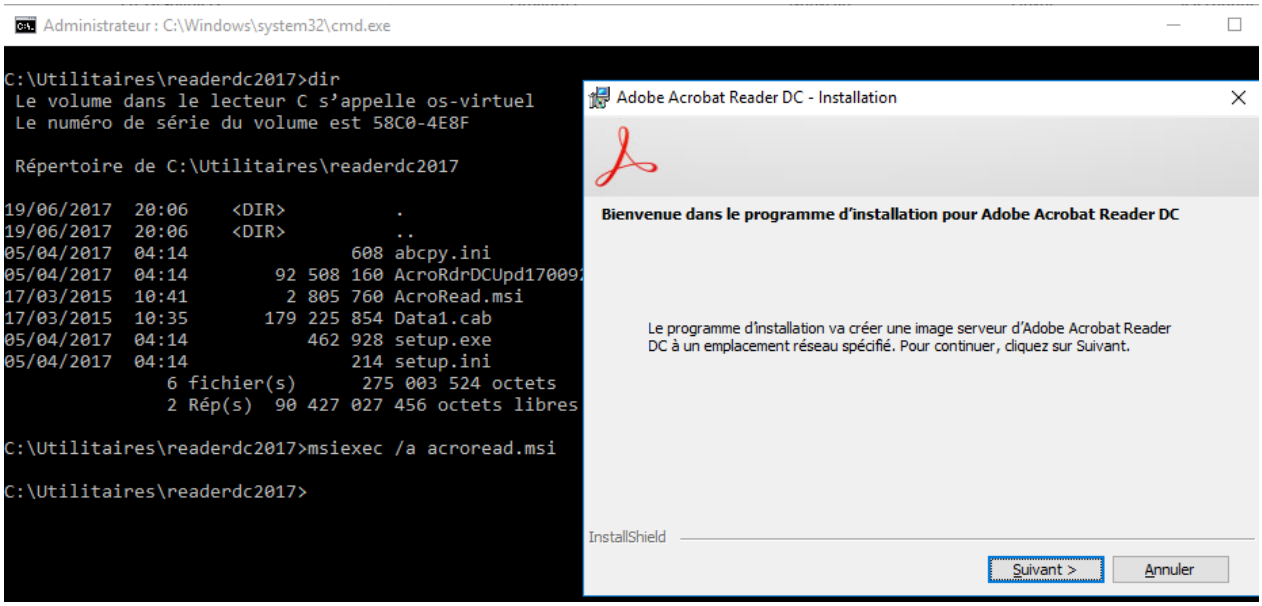
Il faut créer un dossier partagé sur le serveur, futur point de **distribution administrative**…



Et vérifier que l'on y a accès depuis un client via un chemin classique \\srv\partagep, par exemple sur un serveur dans le dossier ***acrobat-dc*** on souhaite donc installer un AIP d'acrobat reader …

On se place dans le dossier dans lequel on à désarchivé précédemment notre distribution, donc par exemple readerdc2017, et on execute

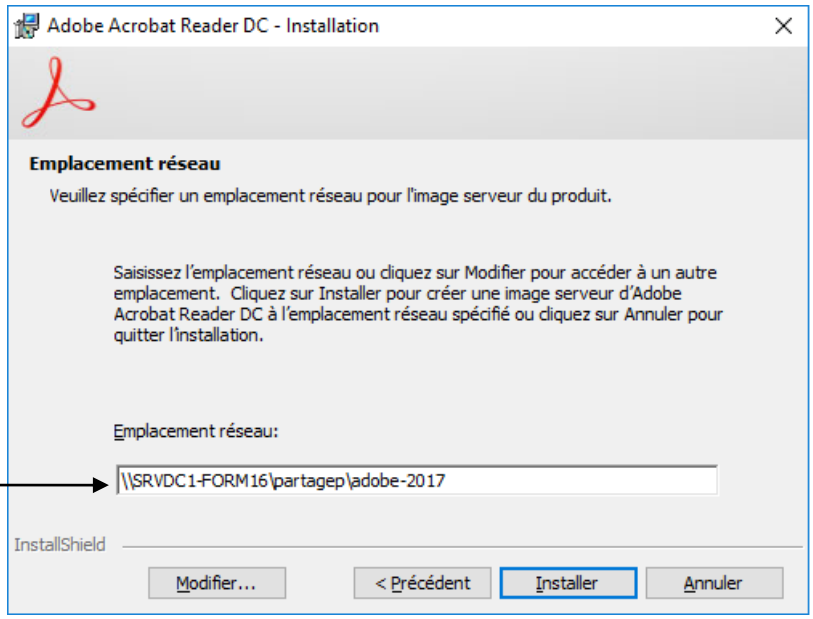
msiexec /a acroread.msi



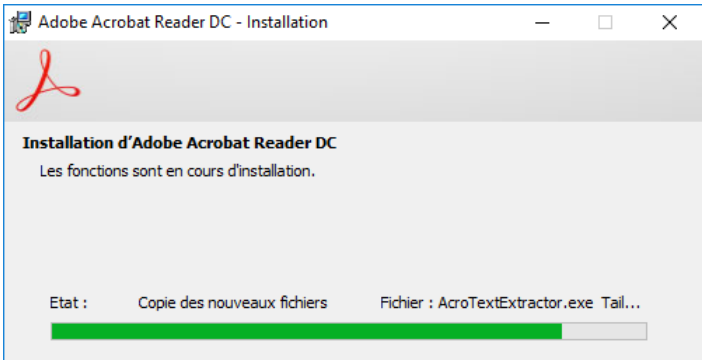
La création du point **AIP** commence,

il faut indiquer le chemin réseau **\\xxxx** le **dossier de stockage** de notre futur point de distribution administrative

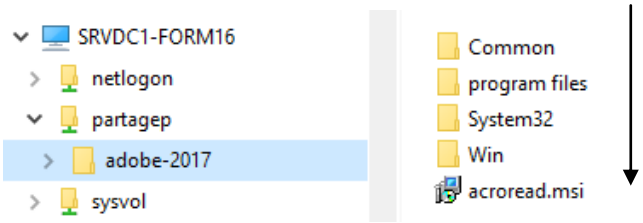
...



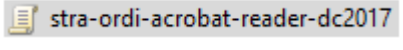
Et la copie des fichiers s'effectue donnant à terme



Lorsque le transfert est terminé, on aura à disposition une installation administrative de acrobat reader disponible…avec notre **.msi !**

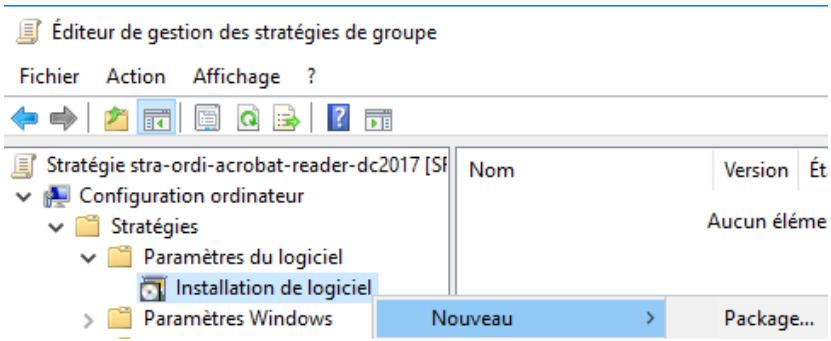


GPO de dépliement MSI :

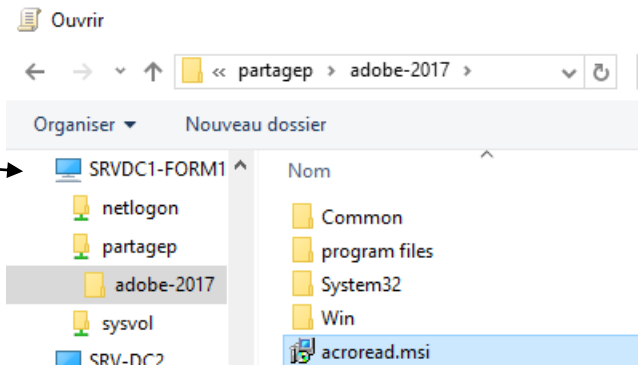
Il ne reste plus qu'à se créer une **stratégie ordinateur**, nommée par exemple ***stra-ordi-acrobat-reader-dc2017*** 

allant chercher notre point AIP de adobe

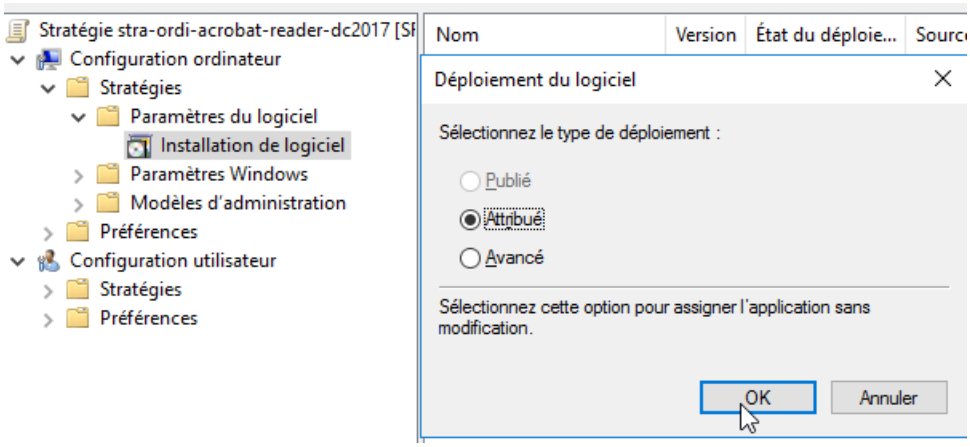
On demande dans **Installation de logiciel** un **Nouveau/ Package…**



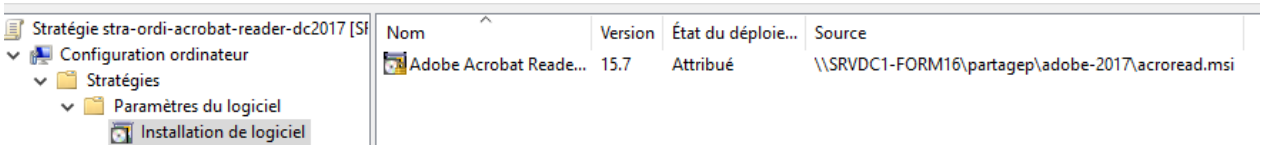
N.B: dans la boite de dialogue « ouvrir » il faut absolument indiquer le chemin réseau… même si ce chemin n'est pas proposé.



Puis on demande **Attribué**

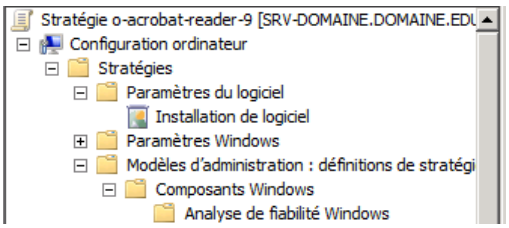


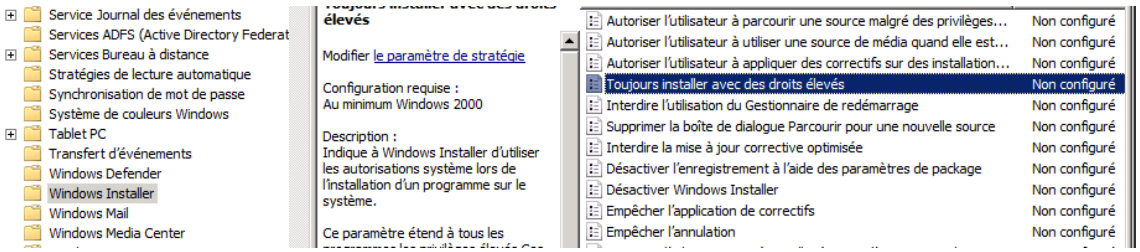
De manière à obtenir



N.B: il est conseillé de coupler cette GPO avec le réglage **Toujours installer avec des droits élevés**…

dans **Configuration ordinateurs / Modèles d'administration / Composants Windows / Windows Installer**





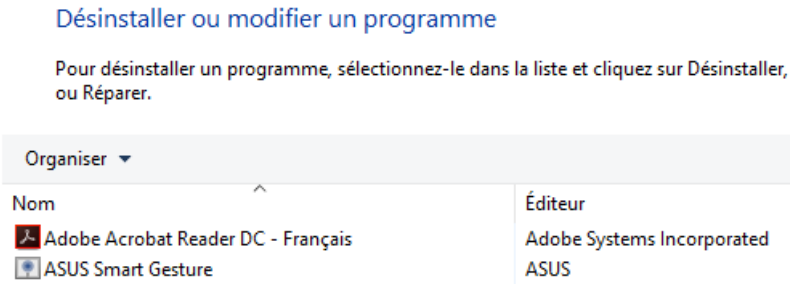
il n'y a plus qu'a lier la GPO sur une UO ayant un ordinateur sur lequel on souhaire déployer Adobe Acrobat

Lorsque l'on execute un **gpupdate /force** on peut avoir ce message, normal

```
C:\Users\Administrateur.FORM1>gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.

Les avertissements suivants ont été rencontrés lors du traitement de la stratégie de l'ordinateur :

L'extension côté client de la stratégie de groupe Software Installation n'a pas pu appliquer un ou plusieurs paramètres
car les modifications doivent être traitées avant le démarrage système ou la connexion utilisateur. Le système attendra
la fin complète du traitement de la stratégie de groupe avant de procéder au prochain démarrage ou à la prochaine connex
ion pour cet utilisateur. Ceci peut entraîner un ralentissement du démarrage et des performances de démarrage du système
.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

Pour plus de détails, ouvrez le journal des événements ou exécutez GPRESULT /H GPReport.html depuis la ligne de commande
 pour accéder aux résultats de la stratégie de groupe.

Certaines stratégies d'ordinateurs activées peuvent uniquement être
exécutées pendant le démarrage.

OK pour redémarrer ? (O/N)^P
```

Lors du redemarrage du poste, on verra un message permettant de comprendre que en arrière plan, le déploiement d'acrobat reader s'effectue

et effectivement on a bien



DEPLOIEMENT DE FIREFOX

FrontMotion - récupération d'un MSI Firefox :

Il existe des sites ou l'on peut récupérer des MSI opérationnels…

FrontMotion

HOME PRODUCTS SERVICES SUPPORT COMMUNITY

MSI FOR FIREFOX

Easily deploy the Firefox browser on your network to thousands of clients. *MSI for Mozilla Firefox*

FrontMotion FRONTMOTION

HOME PRODUCTS SERVICES SUPPORT COMMUNITY ABOUT CONTACT

HOW TO DEPLOY

- *About*
- *Features*
- *How to deploy*
- *Download*
- *Success Story*
- *Firefox Packager*

1. Save the installer to a network location accessible by client computers (e.g. a network share on a domain controller). If you need to change the INSTALLLEVEL property (such as setting the Default browser), first create an *administrative install* in a network location)
2. Next step depends on if this is a new or upgrade site install.
   1. *New site install:* Create a Group Policy Object (GPO). Right click on an Organizational Unit (OU) or your top level domain, then **Properties**. In the **Group Policy** tab, click **New** to create a new Group Policy.
   2. *Existing site install:* Edit an existing GPO that installs Firefox.
3. Edit the GPO and navigate to **Computer Configuration** -> **Software Settings** -> **Software Installation**
4. Next step depends on if this is a new or upgrade site install.
   1. *New site install:* Add the new package, specify the location of the Firefox MSI on a network share. (e.g. serverappinstallsfirefoxfirefox-x.x.x.x.msi). To include transformations (*.mst), choose 'Advanced' for the deployment method.am
   2. *Existing site install:* Add the new package and choose 'Advanced' to specify the older packages in the **Upgrades** tab in the new package's **properties**. Optionally add transformations (*.mst)

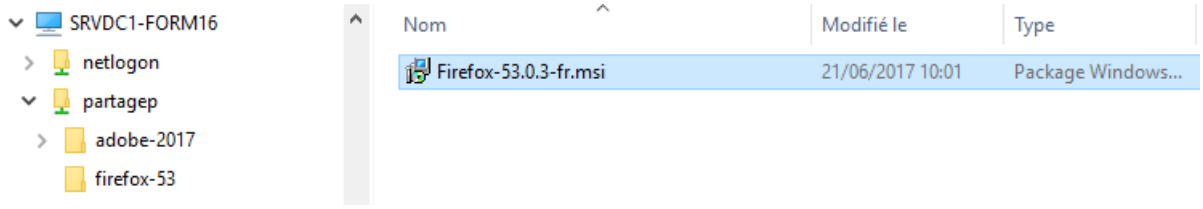
Dans le but d'effectuer un déploiement par GPO, il nous faut un fichier MSI adéquat…

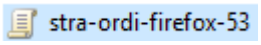
FIREFOX RELEASES

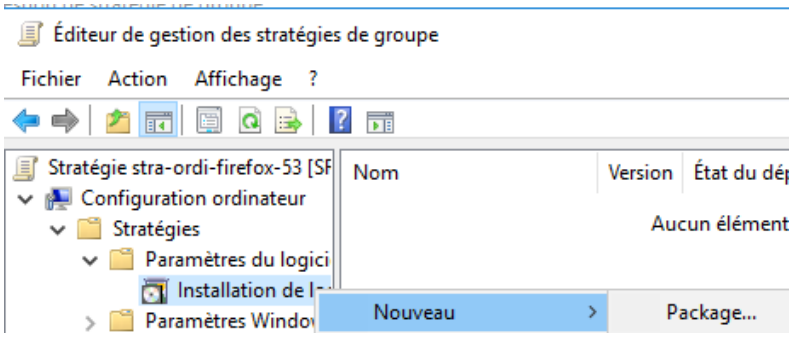
On récupère celui de la version 53.0 française…

- *Firefox-53.0.3*

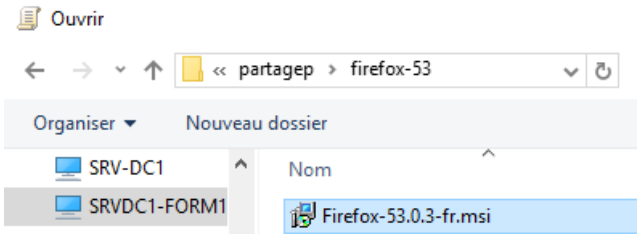
On crée un point d'installation par exemple ***firefox-53*** dans un dossier partagé sur le serveur, et on y copie notre fichier **msi**…



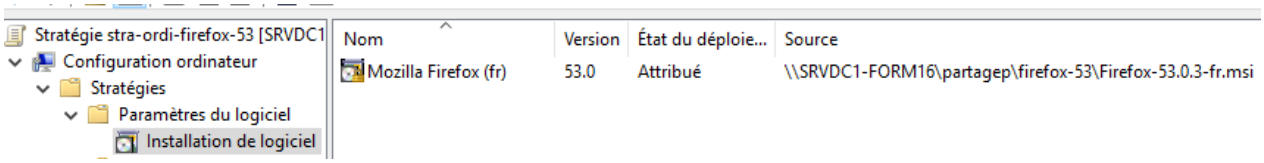
Il ne reste plus qu'à créer une **stratégie ordinateur**… 



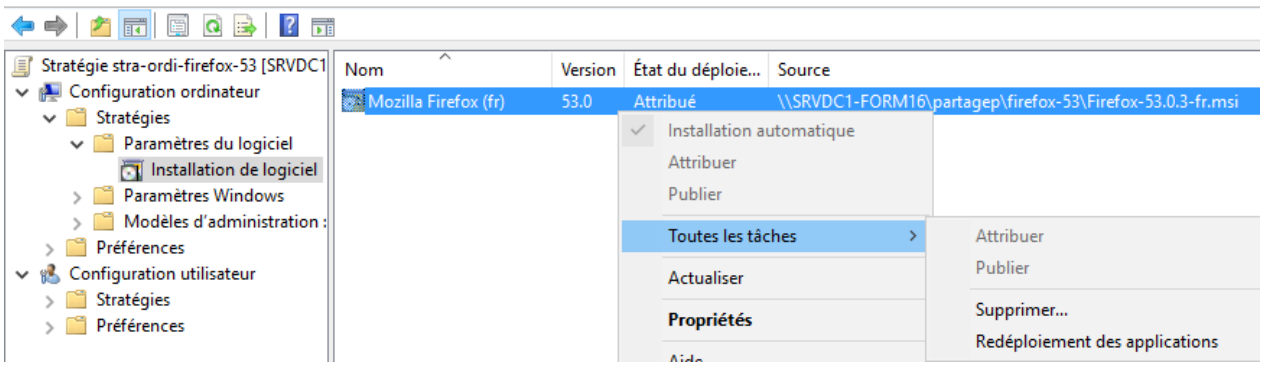
on indique bien un chemin réseau dans la boite de dialogue « ouvrir »



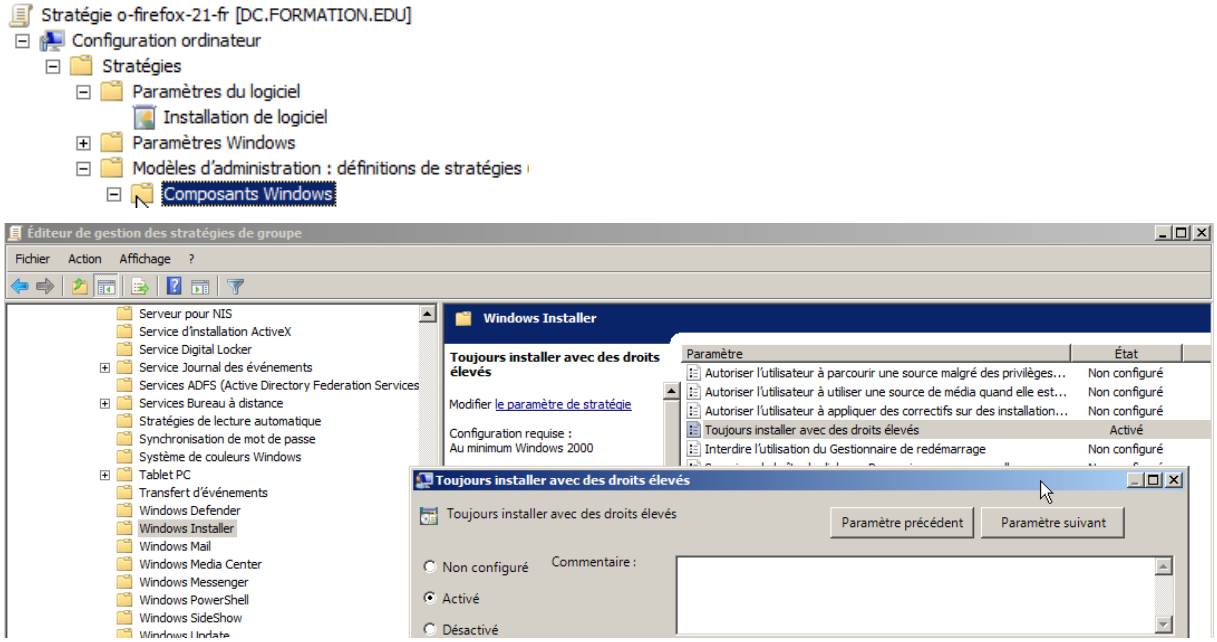
puis attribué pour obtenir



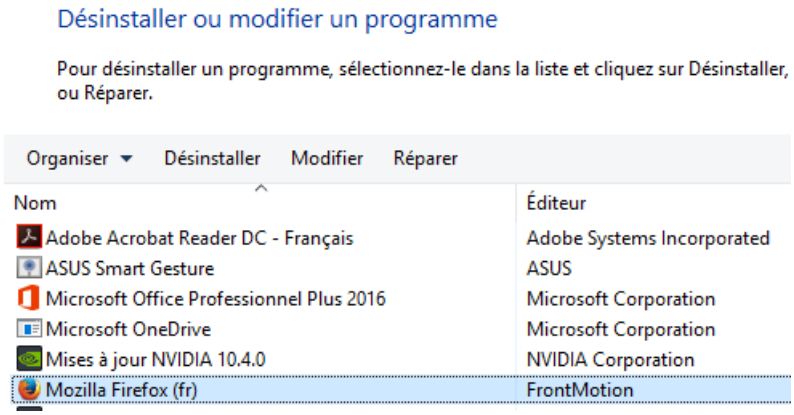
Eventuellement avec une notion de **re-déploiement**



et on demander d'exécuter Windows Installer avec des droits élevés



Après déploiement on aura bien

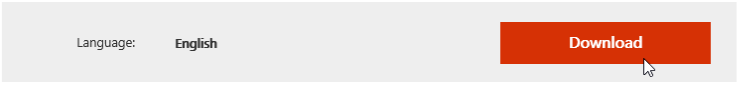


GPO – PARAMETRAGE OFFICE 2016

Récupération des GPo Templates office 2016

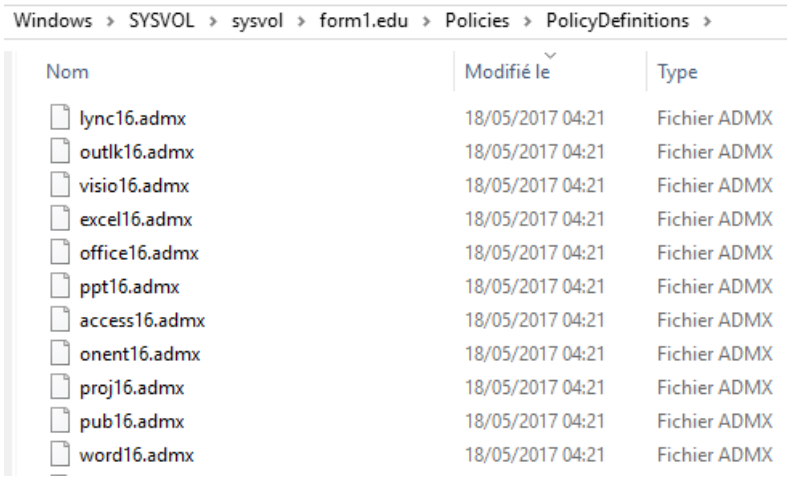
On récupère les modèles de templates pour Office 2016

Office 2016 Administrative Template files (ADMX/ADML) and Office Customization Tool

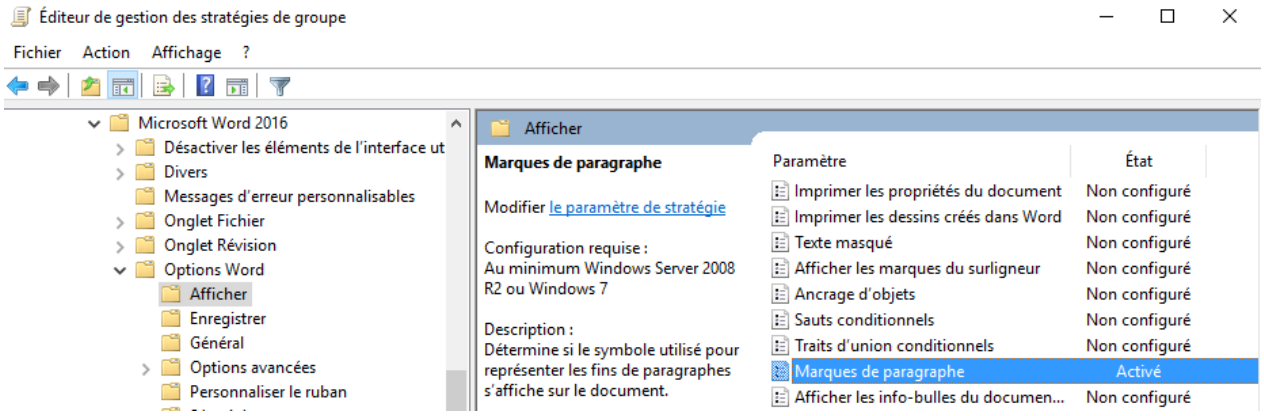


On les désarchive, admintemplates_x86_4549-1000_en-us.exe

et on les poses, dans notre magasin central sur notre DC



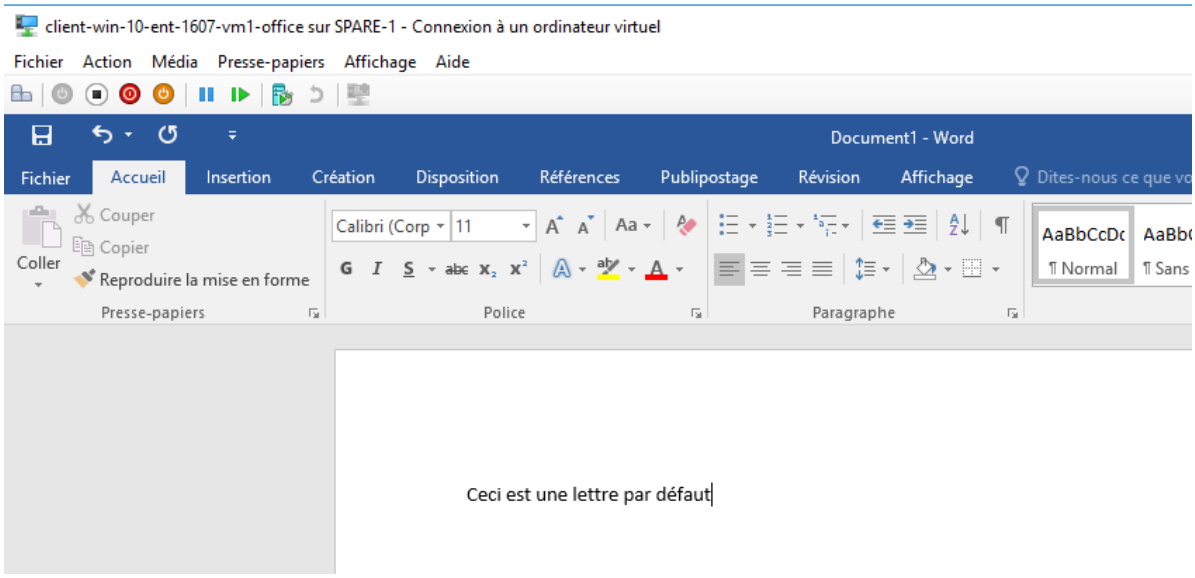
On se crée un GPO utilisateur, avec dans le template Microsoft Word 2016, **l'affichage de la marque de paragraphe**



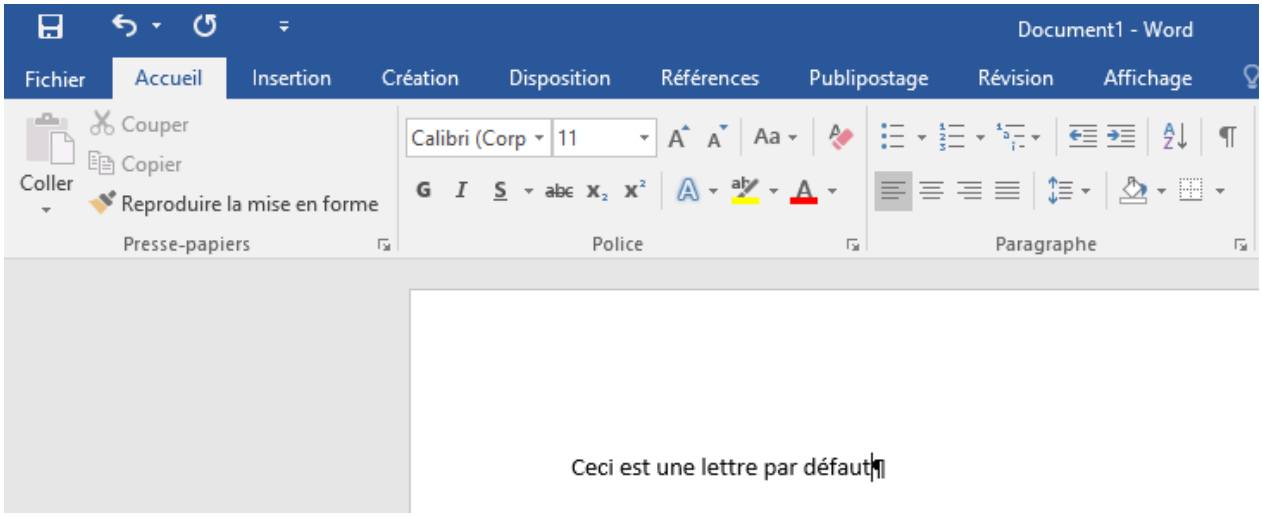
On sent bien que les paramétrages sont nombreux, on peut en trouver une idée dans le fichier Excel associé avec les templates de GPO. office2016grouppolicyandoctsettings.xlsx

Lancement Word 2016 par défaut

Sur le client, on observe que on ne fait pas appraître les marques de paragraphe, ni la règle…



Après application de la GPO sur notre machine, on aura bien la marque de fin de paragraphe qui s'affichera pas défaut !



GPO – FILTRE WMI

Selectionner un OS Windows – exemple WMI

Dans le cas d'un serveur, on peut utiliser la variable **ProductType** qui permet de différencier les serveurs contrôleurs de domaines ou non

ProductType= »2" pour les CD ProductType= »3" pour les autres.

Windows Clients :

Windows 7

select Version from Win32_OperatingSystem WHERE Version like "6.1%" AND ProductType="1" AND OSArchitecture = "64-bit"

select Version from Win32_OperatingSystem WHERE Version like "6.1%" AND ProductType="1" AND NOT OSArchitecture = "64-bit"

select Version from Win32_OperatingSystem WHERE Version like "6.1%" AND ProductType="1"

Windows 8

select Version from Win32_OperatingSystem WHERE Version like "6.2%" AND ProductType="1" AND OSArchitecture = "64-bit"

select Version from Win32_OperatingSystem WHERE Version like "6.2%" AND ProductType="1" AND NOT OSArchitecture = "64-bit"

select Version from Win32_OperatingSystem WHERE Version like "6.2%" AND ProductType="1"

Windows 8.1

select Version from Win32_OperatingSystem WHERE Version like "6.3%" AND ProductType="1" AND OSArchitecture = "64-bit"

select Version from Win32_OperatingSystem WHERE Version like "6.3%" AND ProductType="1" AND NOT OSArchitecture = "64-bit"

select Version from Win32_OperatingSystem WHERE Version like "6.3%" AND ProductType="1"

Windows 7, 8 and 8.1 (all versions before 10)

select Version from Win32_OperatingSystem WHERE Version like "6.%" AND ProductType="1" AND OSArchitecture = "64-bit"

select Version from Win32_OperatingSystem WHERE Version like "6.%" AND ProductType="1" AND NOT OSArchitecture = "64-bit"

select Version from Win32_OperatingSystem WHERE Version like "6.%" AND ProductType="1"

Windows 10 all builds

select Version from Win32_OperatingSystem WHERE Version like "10.%" AND ProductType="1" AND OSArchitecture = "64-bit"

select Version from Win32_OperatingSystem WHERE Version like "10.%" AND ProductType="1" AND NOT OSArchitecture = "64-bit"

select Version from Win32_OperatingSystem WHERE Version like "10.%" AND ProductType="1"

Windows 10 1507

select Version from Win32_OperatingSystem WHERE Version like "10.0.10240" AND ProductType="1" AND OSArchitecture = "64-bit"

select Version from Win32_OperatingSystem WHERE Version like "10.0.10240" AND ProductType="1" AND NOT OSArchitecture = "64-bit"

select Version from Win32_OperatingSystem WHERE Version like "10.0.10240" AND ProductType="1"

Windows 10 1511

select Version from Win32_OperatingSystem WHERE Version like "10.0.10586" AND ProductType="1" AND OSArchitecture = "64-bit"

select Version from Win32_OperatingSystem WHERE Version like "10.0.10586" AND ProductType="1" AND NOT OSArchitecture = "64-bit"

select Version from Win32_OperatingSystem WHERE Version like "10.0.10586" AND ProductType="1"

Windows 10 1607

select Version from Win32_OperatingSystem WHERE Version like "10.0.14393" AND ProductType="1" AND OSArchitecture = "64-bit"

select Version from Win32_OperatingSystem WHERE Version like "10.0.14393" AND ProductType="1" AND NOT OSArchitecture = "64-bit"

select Version from Win32_OperatingSystem WHERE Version like "10.0.14393" AND ProductType="1"

Windows Sever :

Windows Server 2003 R2

select Version from Win32_OperatingSystem WHERE Version LIKE "5.2%"

Windows Server 2008

select Version from Win32_OperatingSystem WHERE Version LIKE "6.0%" AND (ProductType = "2" or ProductType = "3")

Windows Server 2008 R2

select Version from Win32_OperatingSystem WHERE Version LIKE "6.1%" AND (ProductType = "2" or ProductType = "3")

select Version from Win32_OperatingSystem WHERE Version LIKE "6.2%" AND (ProductType = "2" or ProductType = "3")

Les clients Windows :

select ProductType FROM Win32_OperatingSystem WHERE ProductType = "1"

select ProductType FROM Win64_OperatingSystem WHERE ProductType = "1"

Les serveurs Windows :

select ProductType from Win32_OperatingSystem where (ProductType = « 2 ») OR (ProductType = « 3 »)

Les clients Windows posterieur ou égal au build 1803:

Soit en énumérant les build…

select Version,ProductType from Win32_OperatingSystem WHERE Version like "10.0.17134" OR Version like "10.0.17763" AND ProductType="1"

Soit en effectuant une comparaison (avec correction/convertion car on a une chaine de caractère, et la comparaison est numérique)

Select BuildNumber from Win32_OperatingSystem WHERE BuildNumber >= 17134 AND BuildNumber LIKE "%[123456789][0123456789][0123456789][0123456789][0123456789]%"

Test wmi via powershell

GPO WMI filters can get screwed up when edited. Quick way of testing a WMI filter is available using Powershell:

1.Grab the GPO WMI filter from GPMC and put it into clipboard

2.in Powershell console: gwmi -Query 'Paste your WMI filter here'

gwmi -Query 'SELECT ProductType, CSName FROM Win32_OperatingSystem WHERE (ProductType = "1") AND Not CSName = "CB002021")'

When any results are returned WMI filter evaluates to $true (GPO applies), else $false (GPO does not aplly)

Don't forget that you get the luxury to test against multiple computer just by adding the -Computername parameter:

gwmi -Query 'SELECT ProductType, CSName FROM Win32_OperatingSystem WHERE (ProductType = "1") AND Not CSName = "CB002021")' -Computername PC01,PC02

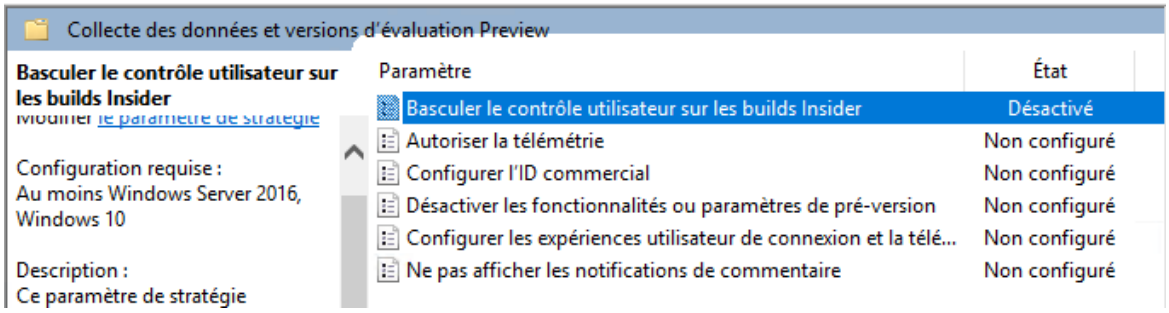
WINDOWS INSIDER PREVIEW

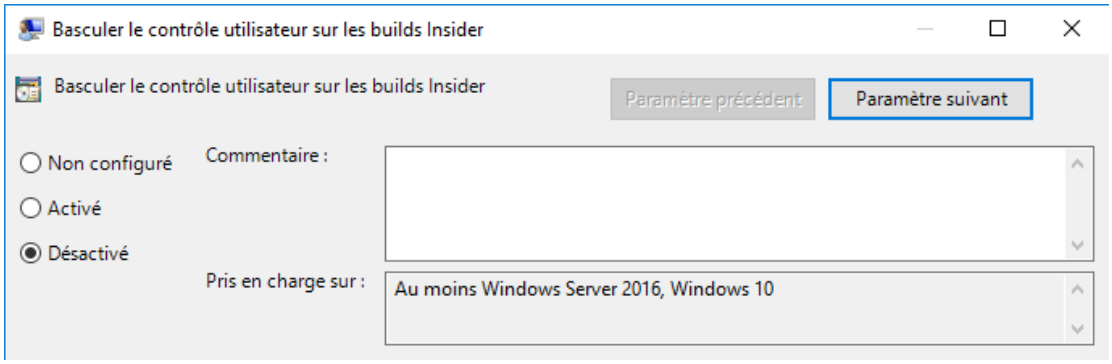
Gestion activation windows 10 insider preview :

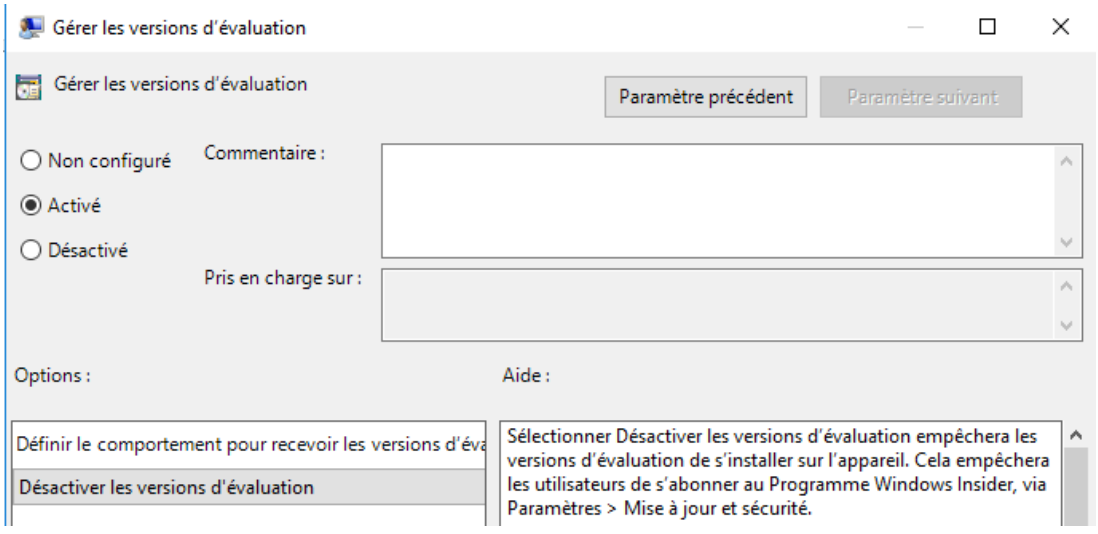
Il faut désactiver la possibilité de demander de récupérer les versions **windows insider**, dans un environnement professionnel

- Jusqu'à la version **10-1703**,

il faut utiliser désactiver la valeur **Basculer le contrôle utilisateur sur les builds insider**





- A partir de la version **10-1709**,

On peut utiliser dans le nouvel ADMX dan **Windows Update pour entreprises**, **Gérer les versions d'évaluation**, et **désactiver les versions d'évaluation**