Cours 6 : Les Stratégies de sécurités de groupe (GPO)

Table des matières

1. Qu'est-ce qu'une GPO?

Les ***stratégies de groupe*** (Group Policy Objects ou ***GPO***) définissent des ensembles de paramètres reliés à la sécurité et aux fonctionnalités des ordinateurs et des utilisateurs d'un domaine Active Directory.

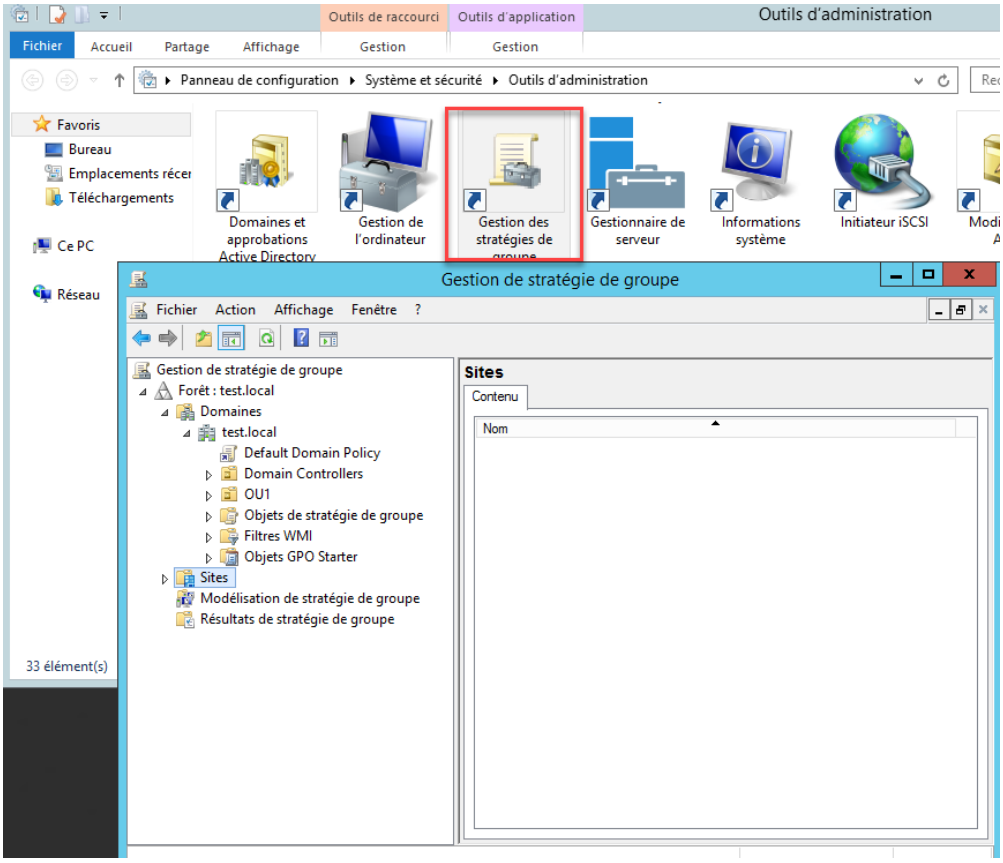
Grâce aux GPOs, un administrateur peut configurer et personnaliser des centaines de ordinateurs et de configurer les comptes utilisateurs en quelques clics

Remarque:

Un poste de travail ne faisant partie d'aucun domaine a aussi une GPO locale, mais nous ne parlerons pas de ce type de GPO ici

2. La console GPMC

La console qui permet d'éditer et de configurer les GPO est la console de **Gestion des stratégies de groupe** ou **GPMC** (*Group Policy Management Console*)



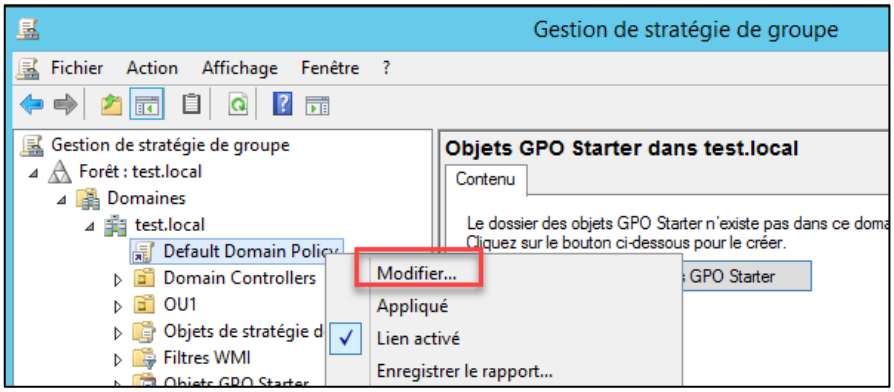
- Il est possible de lier une GPO au:
  - Domaine: dans ce cas, la GPO s'applique sur tous les ordinateurs et les utilisateurs du domaine

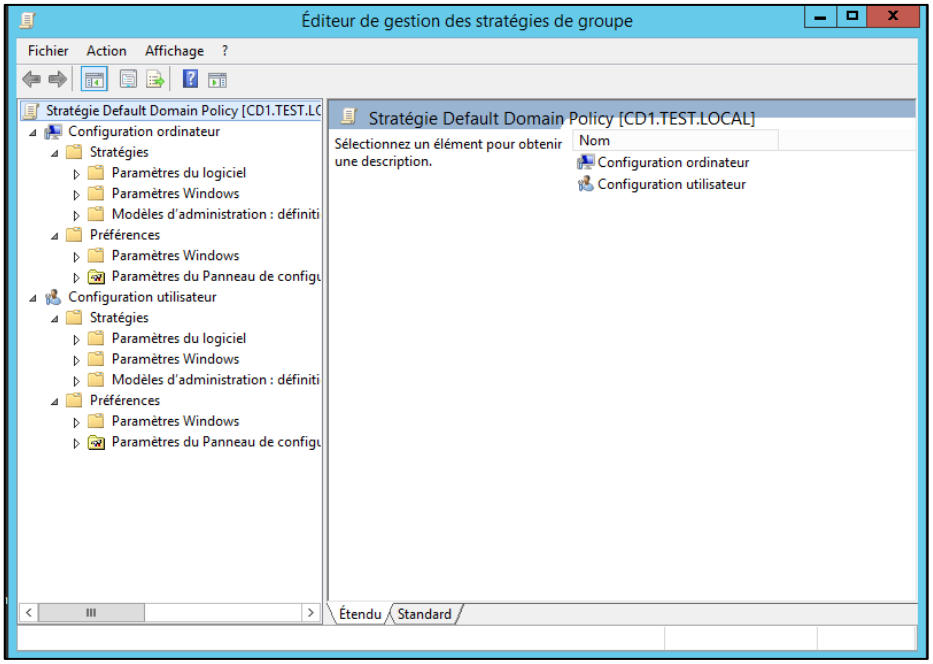
- Unité d'organisation: dans ce cas, la GPO s'applique sur tous les ordinateurs se trouvant dans cette OU et dans les unités d'organisation enfants
- Site: un site représente est un regroupement d'un ou plusieurs sous-réseaux connectés par un réseau haut-débit. En liant une GPO à un site, elle s'appliquera à tous les ordinateurs de ce site (ordinateurs se trouvant dans un de ses sous réseaux)

Remarque:

Les conteneurs *Users* et *Computers* qui apparaissent dans la **console Utilisateurs et ordinateurs Active Directory** ne sont pas des unités d'organisation. On ne peut pas donc y lier une GPO et ils n'apparaissent pas dans la console ***GPMC***

- Par défaut, une GPO est liée au domaine: **Default Domain Policy.** On peut accéder à son contenu en faisant un clic droit dessus **à Modifier**





Une deuxième GPO nommée Default Domain Controllers Policy est liée à l'OU Domain Controllers. Elle s'applique uniquement sur les contrôleurs de domaine.

Comprendre les paramètres d'une stratégie de groupes

- Une stratégie de groupes comprend deux parties:
  - **Configuration utilisateur** la GPO affecte tous les utilisateurs membres du conteneur associé à la GPO, peu importe l'ordinateur utilisé. Les paramètres sont téléchargés au moment de l'ouverture de session.
  - **Configuration Ordinateur** la GPO affecte tous les ordinateurs membres du conteneur associé à la GPO, peu importe qui se connecte. Les paramètres sont téléchargés lorsque l'ordinateur se connecte au domaine, au moment du démarrage.

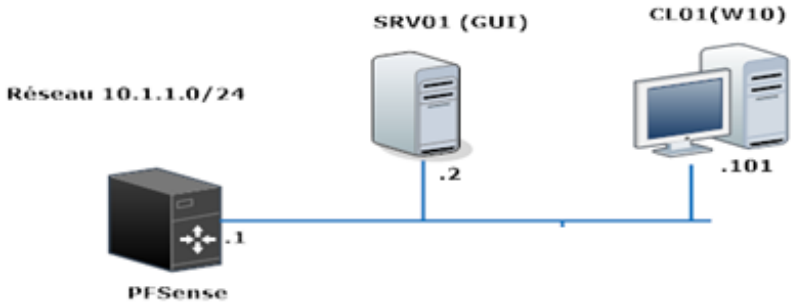
- Une stratégie de groupe qu'on vient de lier (appliquer) ou de modifier ne s'applique pas immédiatement. Il faut attendre après une période déterminée (par défaut 1h30) pour qu'elle soit téléchargée et appliquée par les clients. Pour appliquer immédiatement les modifications de GPO, on peut lancer sur le client la commande suivante:

  gpupdate /force

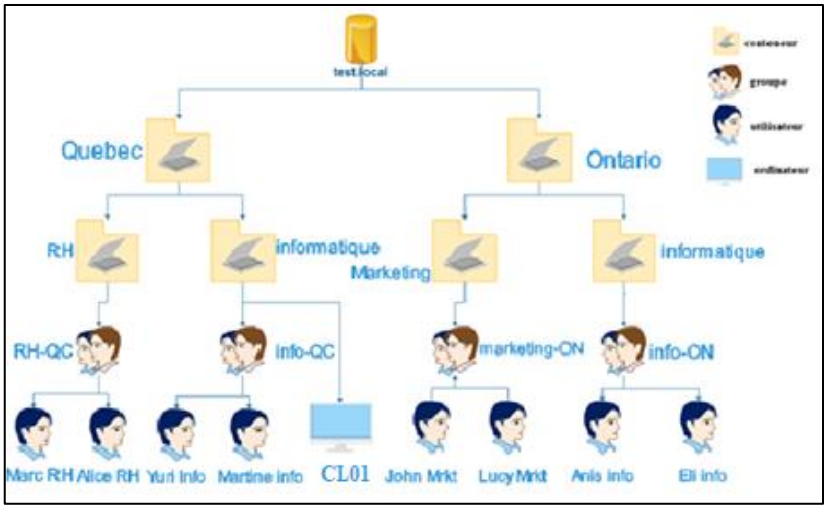
3. Démos de créations de GPO

a. Créer une première GPO

On prend toujours le réseau qu'on déjà crée auparavant:
Réseau Physique:
SRV01: contrôleur de domaine
CL01 (ou TP1): membres du domaine



Organisation logique des objets Active Directory:

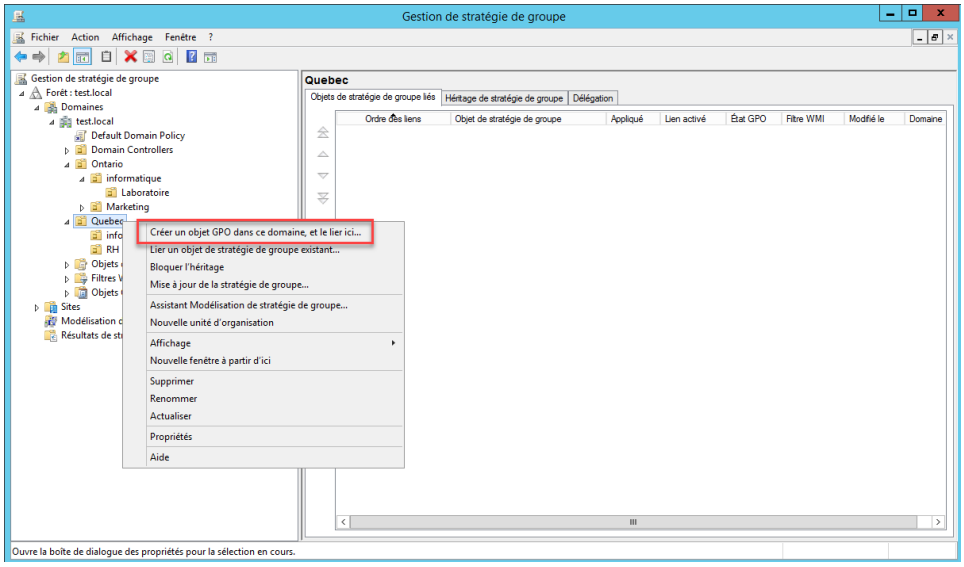


Remarque:

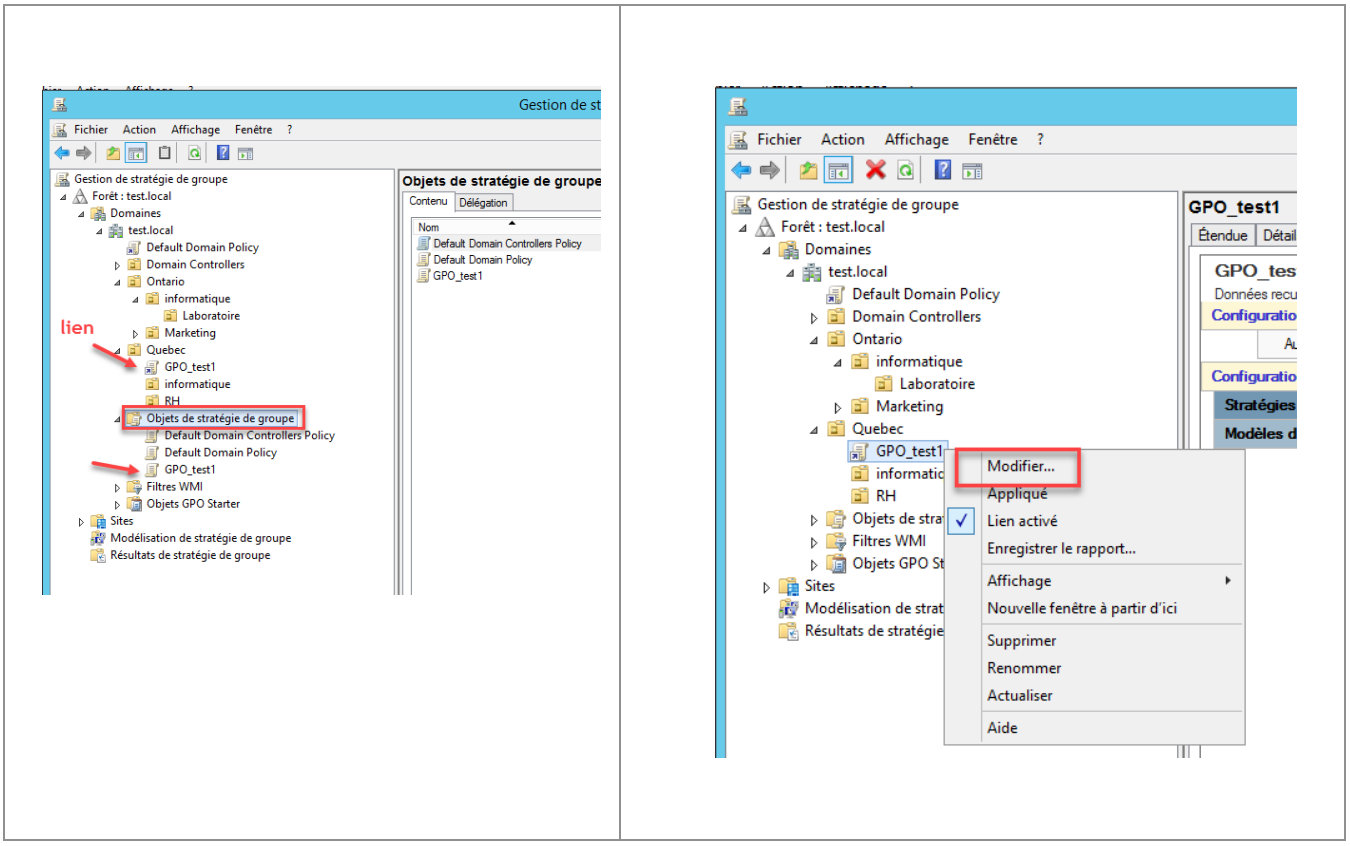
Exécutez le script PowerShell ci-dessous sur le contrôleur de domaine pour créer cette arborescence.

Nous allons Créer une GPO nommée ***GPO_test1*** pour désactiver l'affichage de la corbeille pour les **utilisateurs de Quebec**: cette GPO sera donc liée à l'OU **Quebec**

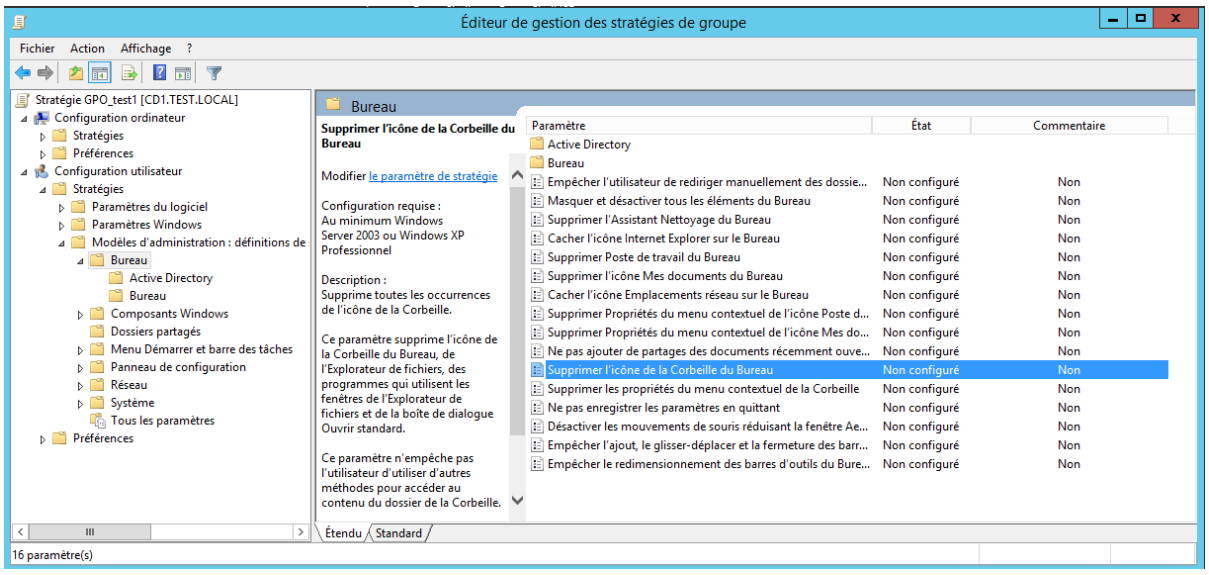
1- Dans la **GPMC**, clic droit sur l'OU **Quebec à Créer un objet GPO dans ce domaine, et le lier ici..**



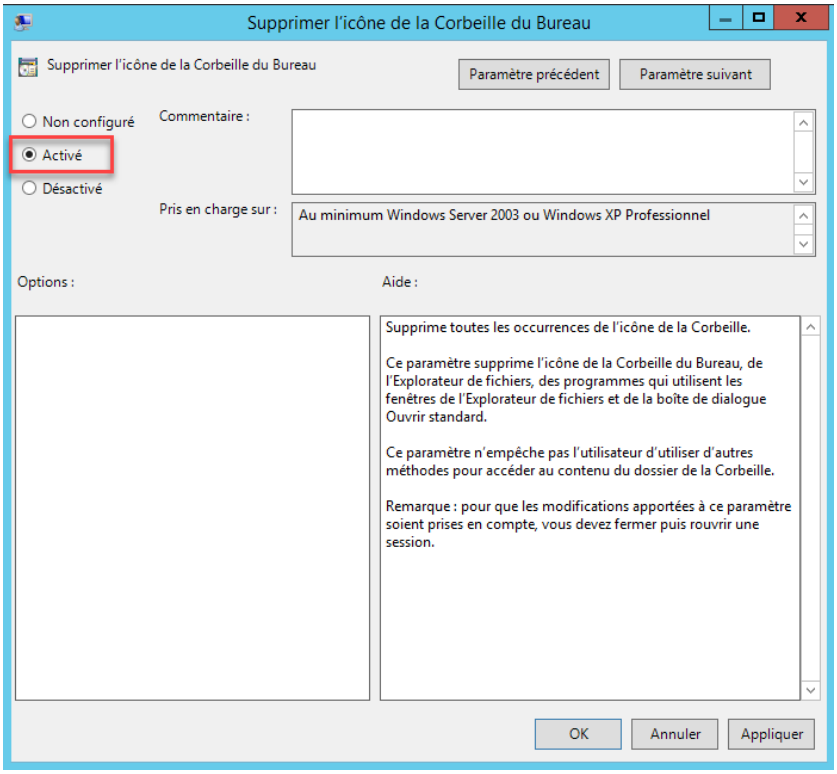
2- Toute GPO créée sera se trouve sous ***Objets de stratégie de groupe*** . Un lien est créé au niveau de l'OU **Quebec** indique qu'elle s'appliquera sur les utilisateurs et ordinateurs de cette OU. Faire un clic droit sur le lien **à modifier**



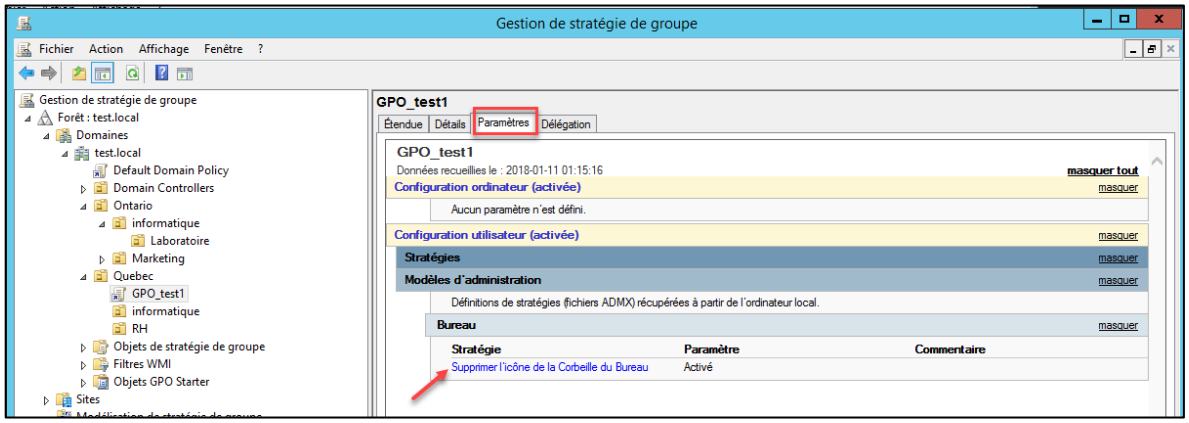
3- L'éditeur de gestion de stratégie de groupe apparait. Nous cherchons à supprimer l'icône Corbeille pour les utilisateurs de Quebec. On repére donc le paramétre ***Configuration utilisateur à Modèle d'administration àBureau à Supprimer l'icônede la corbeille du Bureau*** et on fait double clic dessus



4- On active le paramètre et on ferme la fenêtre et l'éditeur

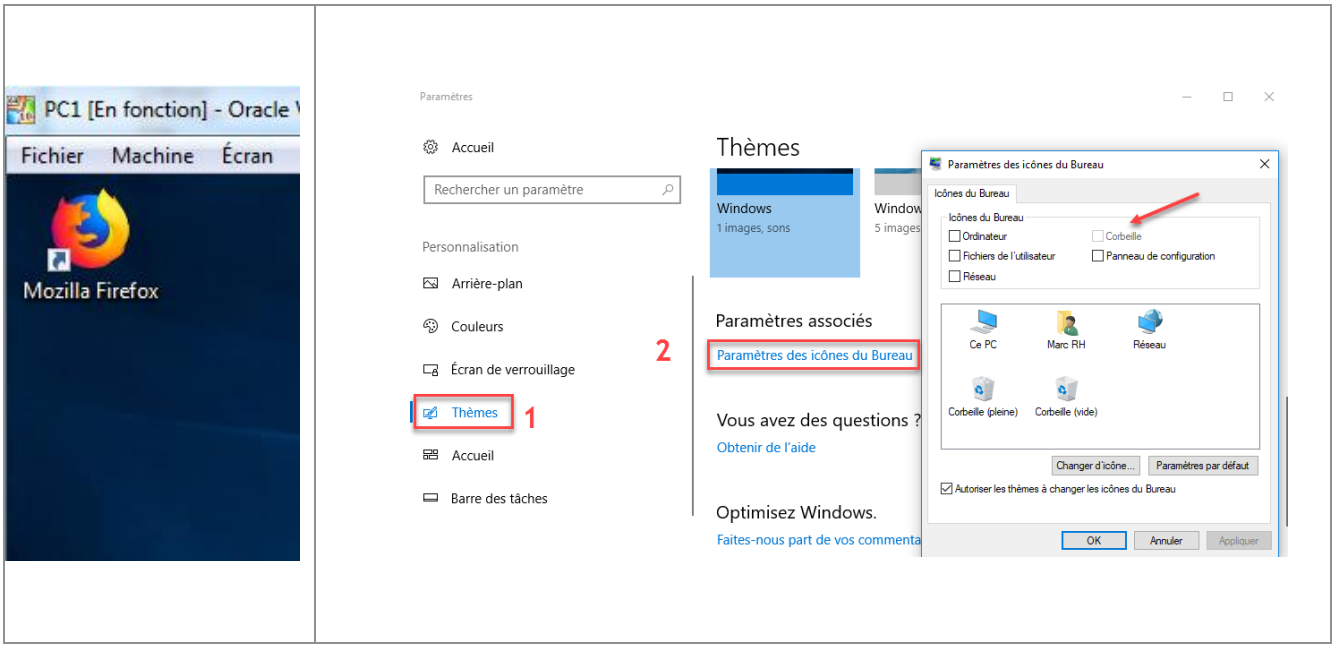


5- Remarquez que l'onglet ***Paramètres*** de chaque GPO affiche les paramètres configurés de cette GPO (pour la **partie ordinateur** et la partie utilisateur)



6- Pour tester cette GPO, on ouvre PC1 et on se connecte avec le compte **TEST\marcRH**

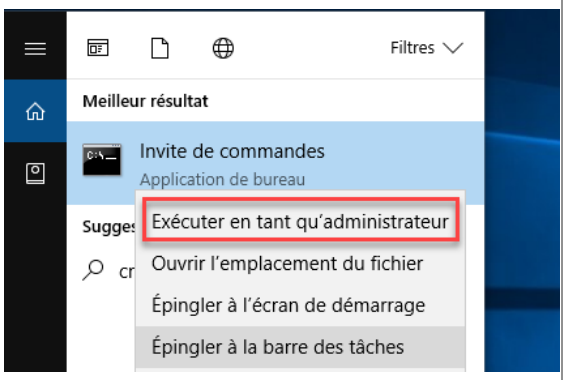
7- On remarquera que l'icône corbeille a disparu, d'ailleurs en accédant aux paramètres des icônes du bureau, on voit que *Corbeille* devient grisée (on ne peut plus l'afficher sur le bureau)

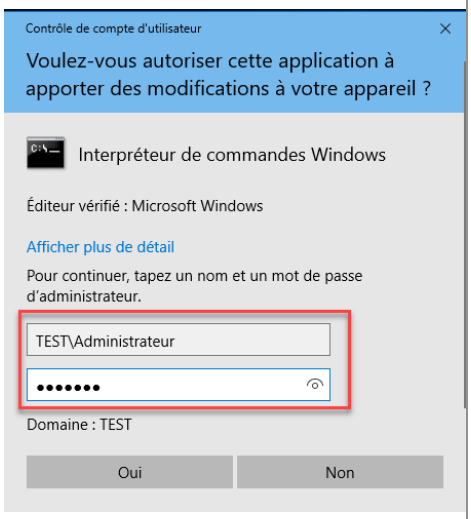


Remarque:

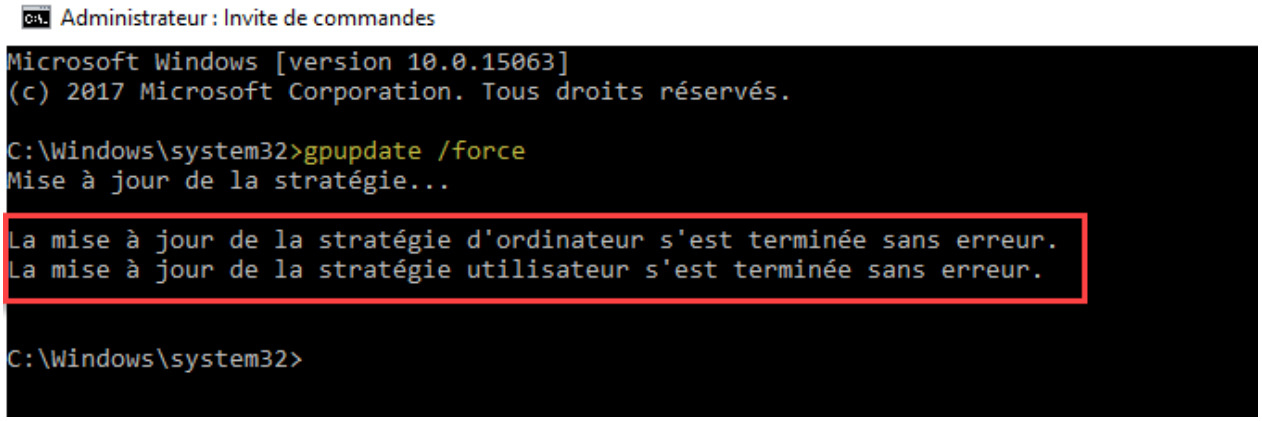
Si cette GPO n'a pas encore été appliquée on peut:

- Soit attendre un certain temps pour que la GPO soit téléchargée par CL01 (par défaut tous les 90 minutes)
- Soit:
  - Ouvrir une *invite de commandes* en tant qu'administrateur (nécessite l'utilisation d'un compte administrateur du domaine)



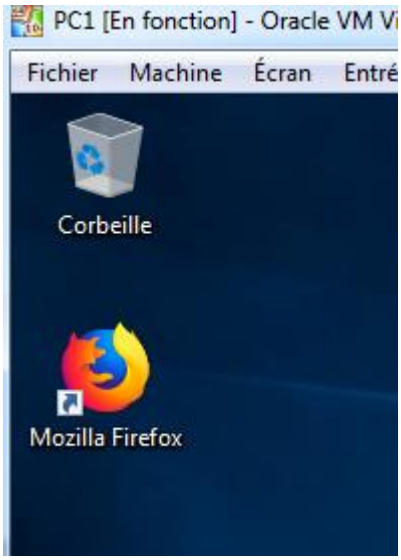


- Lancer la commande ***gpupdate /force***



Se déconnecter et reconnecter sur la machine **PC1**

8- On peut aussi vérifier que lorsqu'on se connecte avec le compte **TEST\johnMrkt** qui ne fait pas partie de l'OU ***Quebec*** (donc ***GPO_test1*** ne s'applique pas dessus), la corbeille reste toujours disponible.

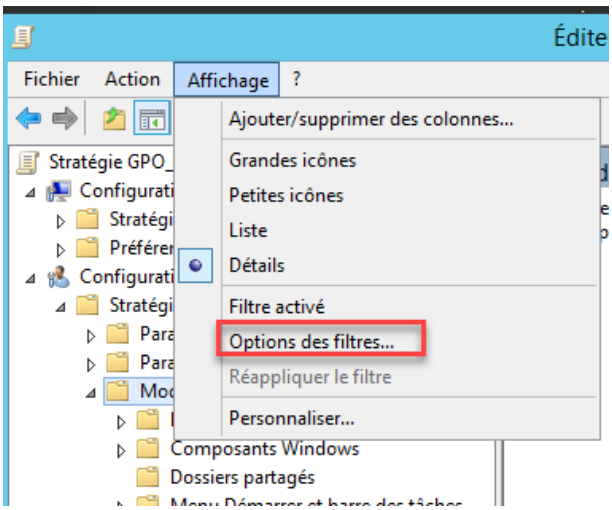


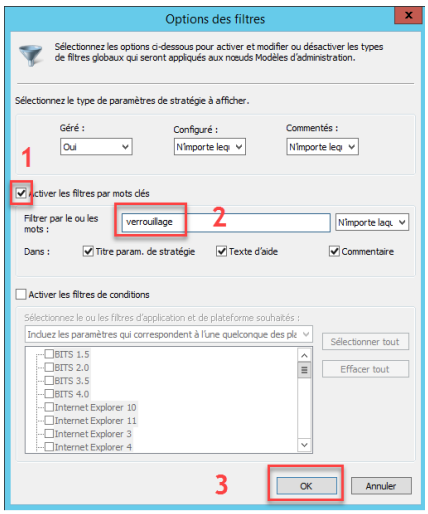
b. Deuxième exemple: Modifier la GPO

Modifier ***GPO_test1*** pour empêcher le verrouillage de la machine.

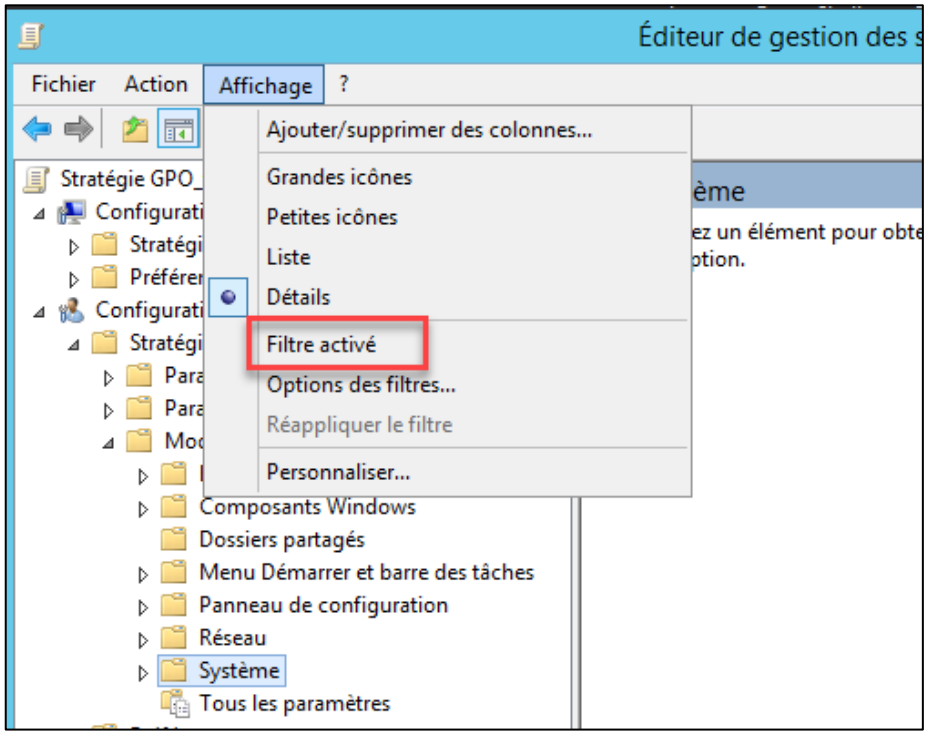
1- On fait clic droit sur ***GPO_test1*** **à modifier**

2- Puisqu'on ne connait pas encore le nom exact du paramètre, nous allons le chercher: accéder à **Affichage à Options de filtres**, activer les filtres par mots clé et insérer le mot **"verrouillage"**

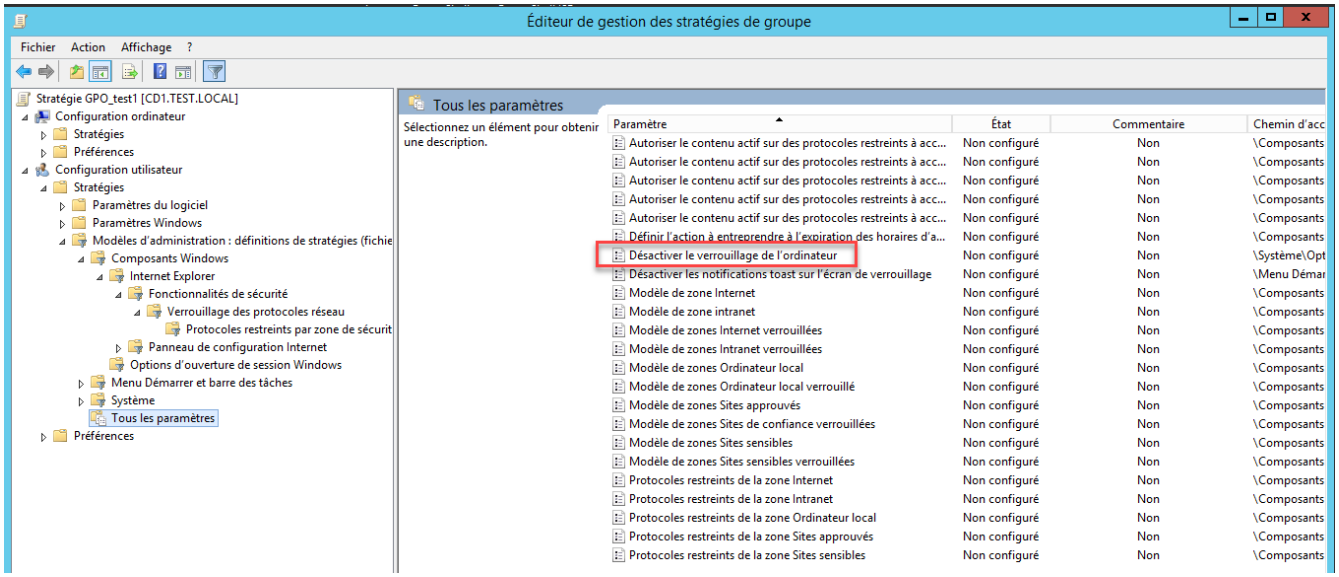


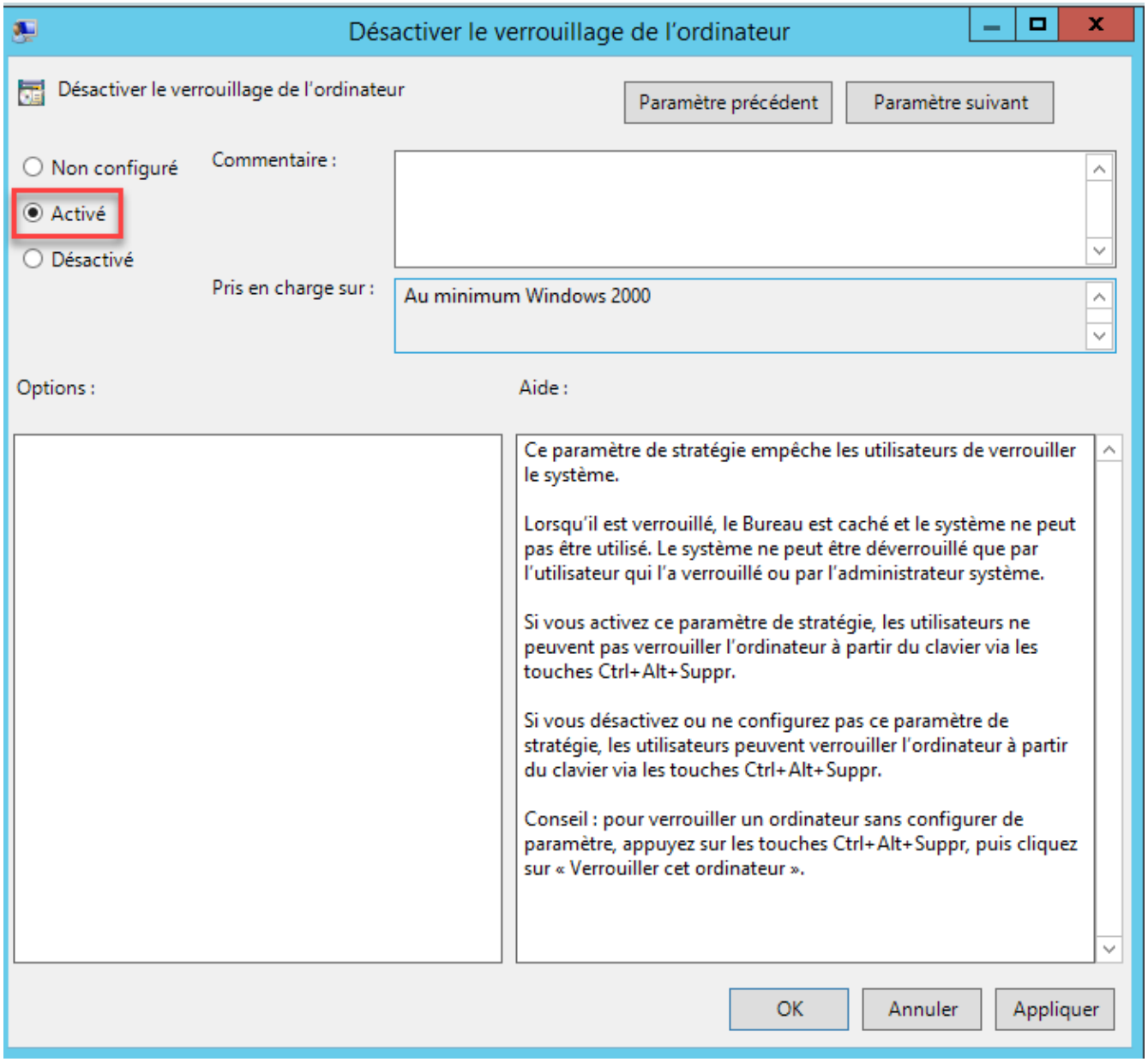


3- Activer le filtre par **Affichage à Filtre Activé**

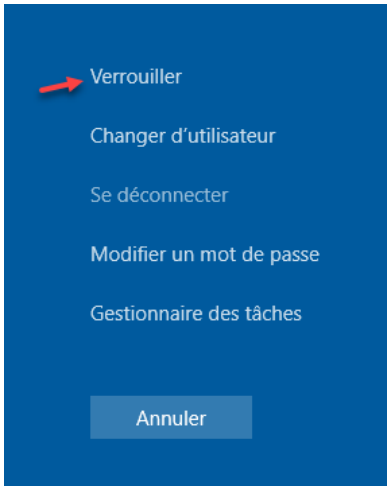


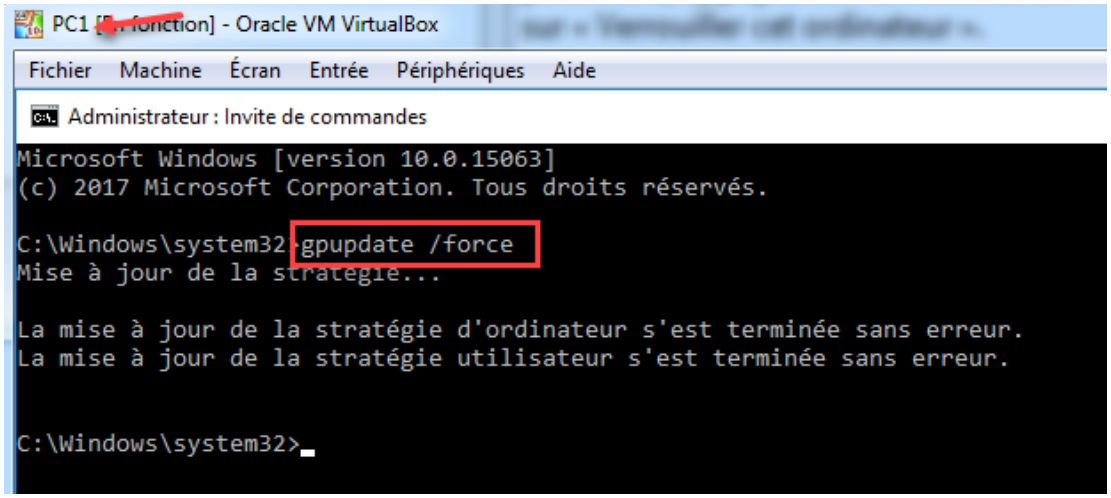
4- Dans *Tous les paramètres* de *configuration utilisateur*, on trouve tous les paramètres contenant ce mot clé (*verrouillage*) soit dans son nom soit dans sa description. Le nombre est réduit ce qui nous permet de les parcourir un à un pour trouver le bon paramètre (qui est **Désactiver le verrouillage de l'ordinateur**). On active donc le paramètre

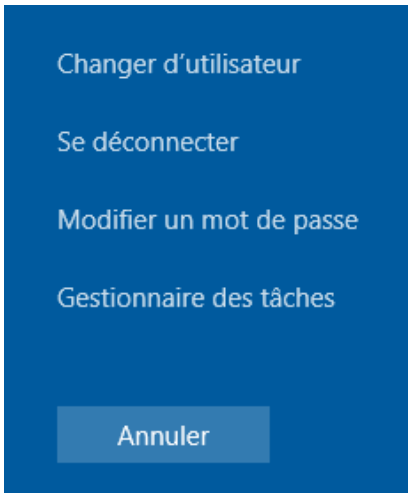




5- En se revenant sur la machine PC1 (avec le compte **TEST\marcRH**), on peut voir qu'on est toujours capable de verrouiller la machine quand on lance **ALT+CTRL+SUPPR** car la GPO n'a pas encore téléchargé par PC1. On lance donc la commande ***gpupdate /force***, on se déconnecte on se reconnecte. L'option de verrouillage n'est maintenant plus disponible.

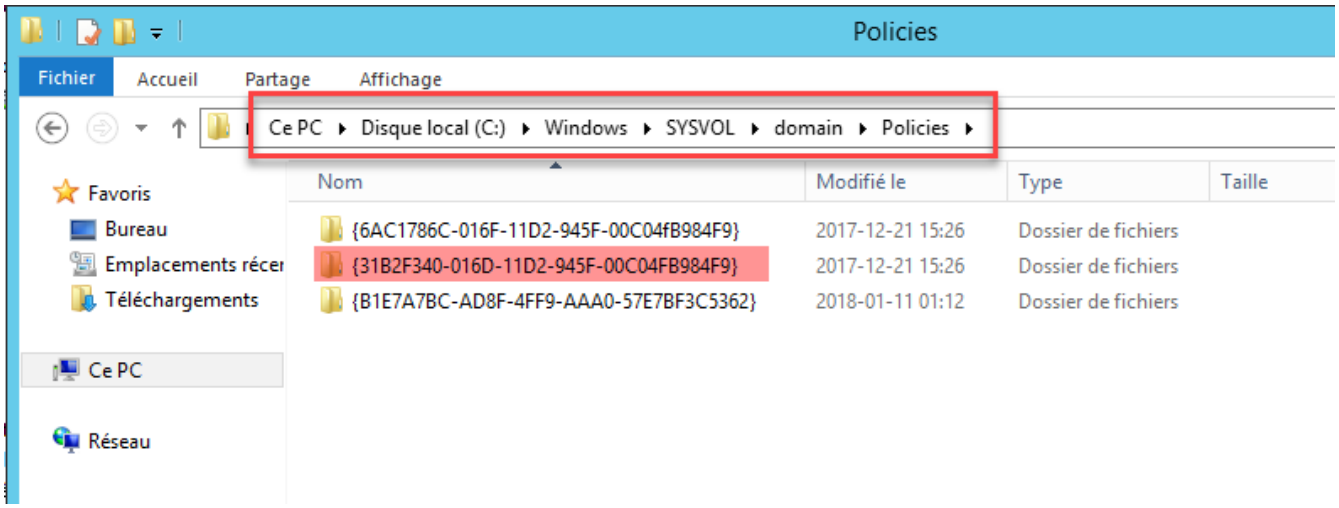

Verrouiller
Changer d'utilisateur
Se déconnecter
Modifier un mot de passe
Gestionnaire des tâches
Annuler

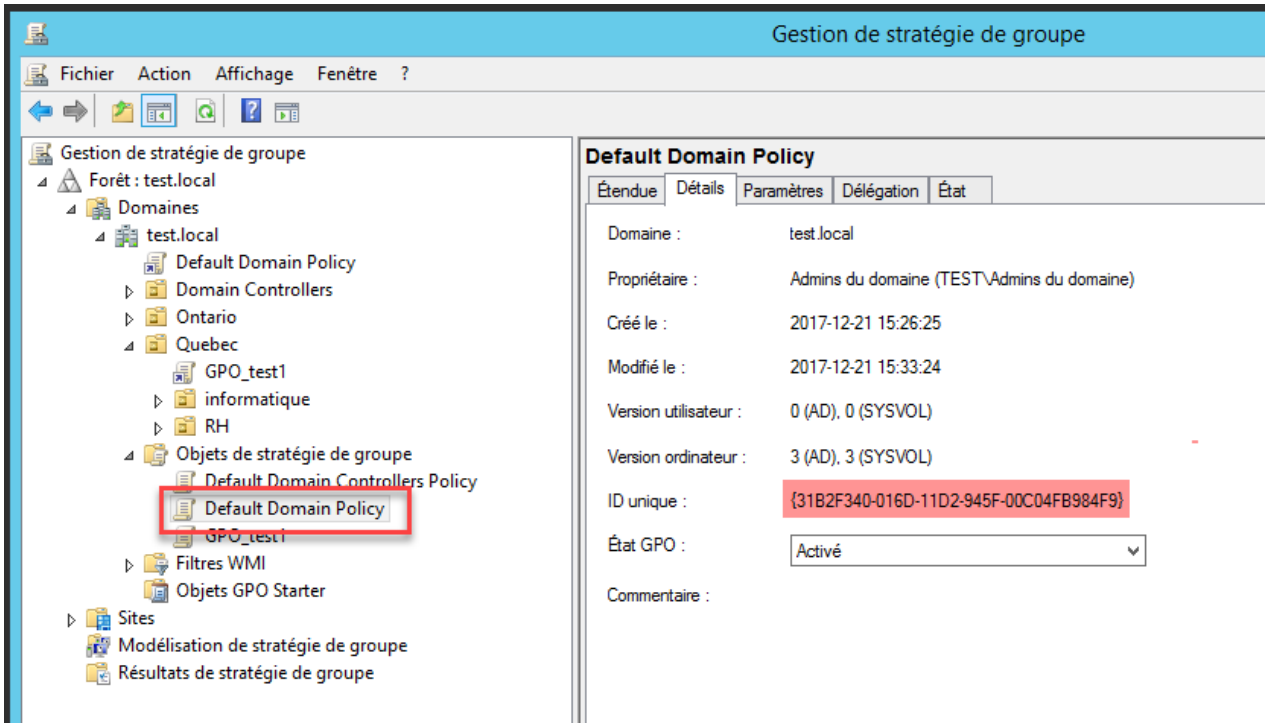

PC1 [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Administrateur : Invite de commandes
Microsoft Windows [version 10.0.15063]
(c) 2017 Microsoft Corporation. Tous droits réservés.
C:\Windows\system32>gpupdate /force
Mise à jour de la stratégie...
La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.
C:\Windows\system32>


Changer d'utilisateur
Se déconnecter
Modifier un mot de passe
Gestionnaire des tâches
Annuler

4. Les politiques de groupes et le dossier SYSVOL

- Stockée par défaut dans "**C:\Windows\SYSVOL**" de chaque contrôleur de domaine, "SYSVOL" (System Volume) et il sert à stocker certaines données qui doivent être répliquées entre les contrôleurs de domaine ou accessibles par les ordinateurs clients (entre autres, les politiques de groupes GPO)
- Le dossier SYSVOL est répliqué entre les différents contrôleurs de domaine, pour que le contenu soit identique, et que les clients bénéficient tous des mêmes données (à jour)
- Le répertoire "**C:\Windows\SYSVOL**" est composé de plusieurs sous-dossiers :
    - **domain**: ce répertoire contient toutes les données à jour (GPO et scripts), réparties en deux sous dossiers : "*Policies*" et "*scripts*". Policies contient toutes les GPOs du domaine, que l'on crée avec la console GPMC. Un sous-dossier par GPO est créé où le nom du dossier correspond au GUID de l'objet GPO.



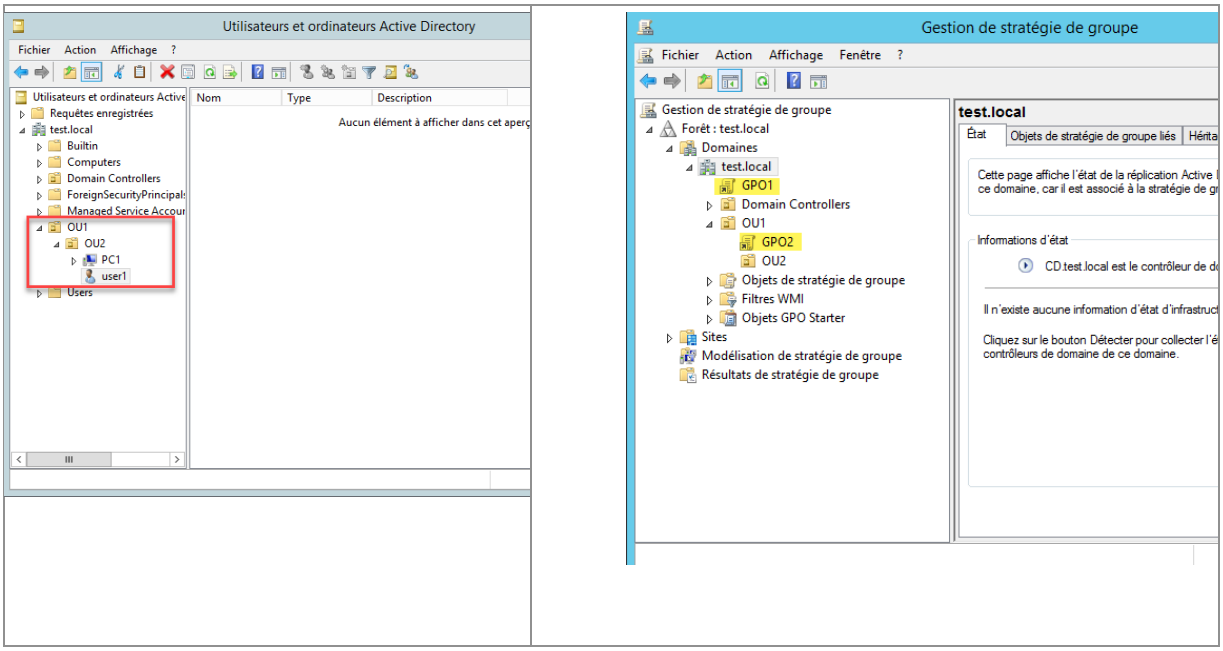


- **scripts:** contient les différents scripts, notamment les scripts de connexion.
- **staging:** ce répertoire est utilisé pour créer une file d'attente (queue) des données en attente de réplication à destination des autres contrôleurs de domaine.

a. Résultante et Ordre d'exécution de GPO

Considérons l'exemple suivant:

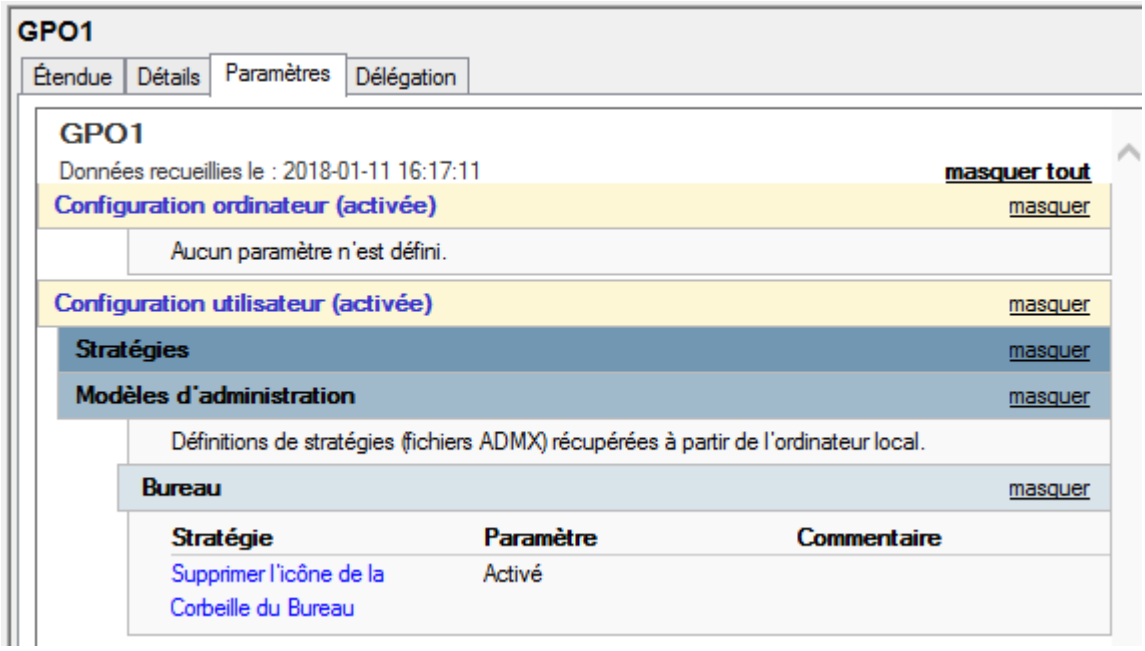
Ce résultat, on doit comprendre comment *Active Directory* définit la priorité entre GPO est définie comme suit: ***OU***, ***Domaine***, ***Site***, ***Local***	



b. Cas 1:

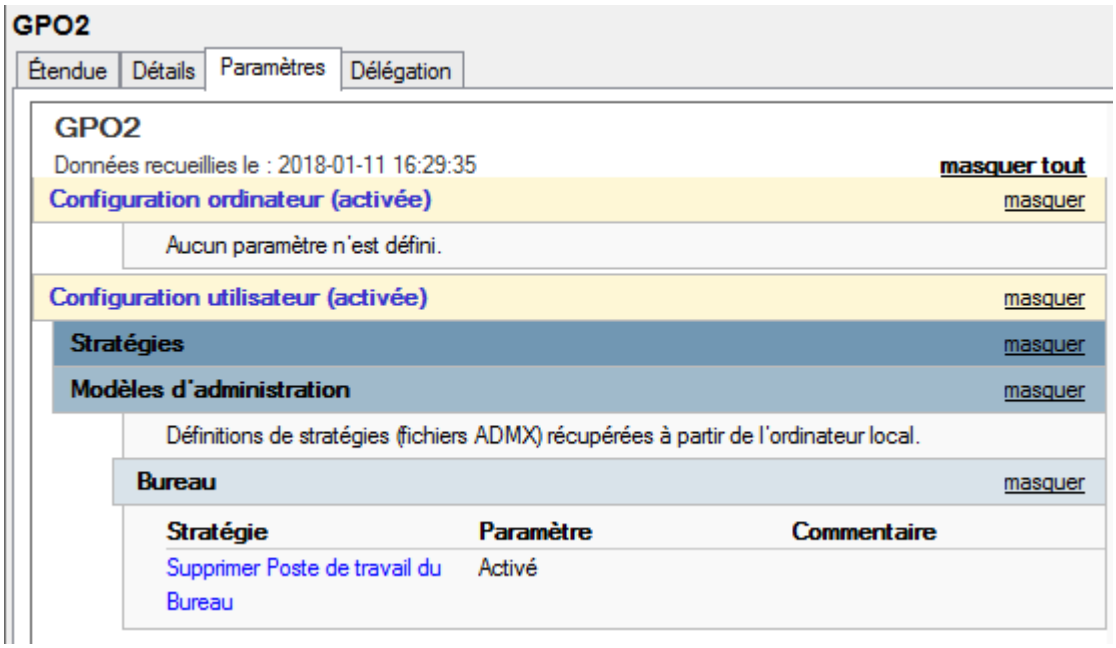
- **GPO1** a un seul paramètre activé:

Configuration utilisateur à Stratégies à Modèles d'administration à Bureau à Supprimer l'icône de la Corbeille du Bureau (Activé)

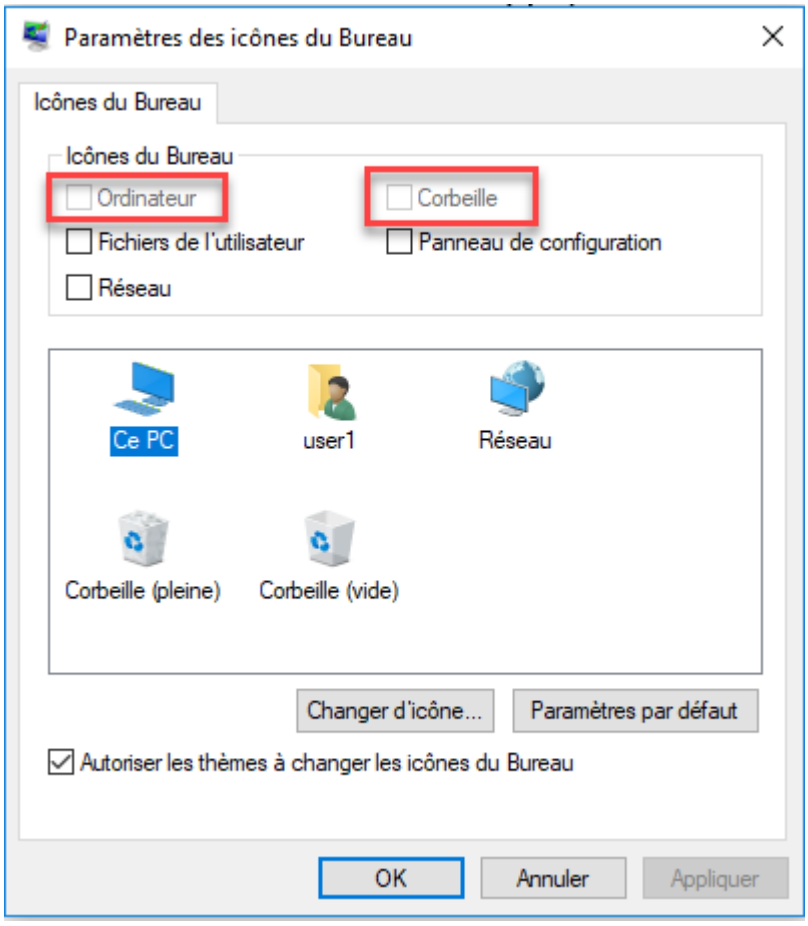


- **GPO2** a un seul paramètre activé:

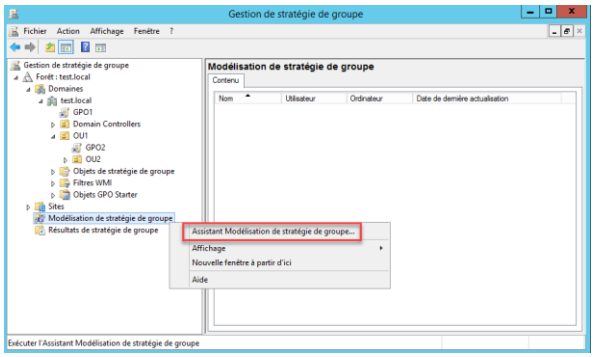
Configuration utilisateur à Stratégies à Modèles d'administration à Bureau à Supprimer poste de travail du Bureau (Activé)

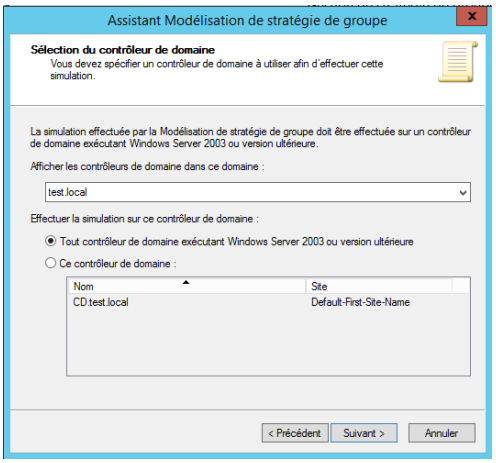


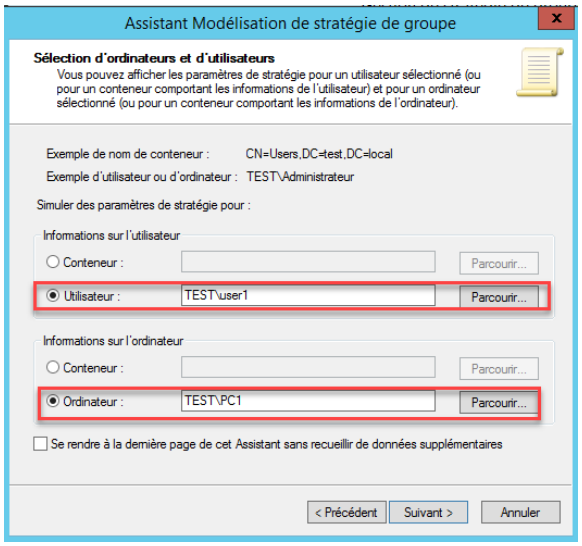
Lorsque **user1** se connecte sur **PC1**, les 2 GPOs sont applicables. Du coup, les deux icônes ***Corbeille*** et ***Mes documents*** ne sont pas disponibles.

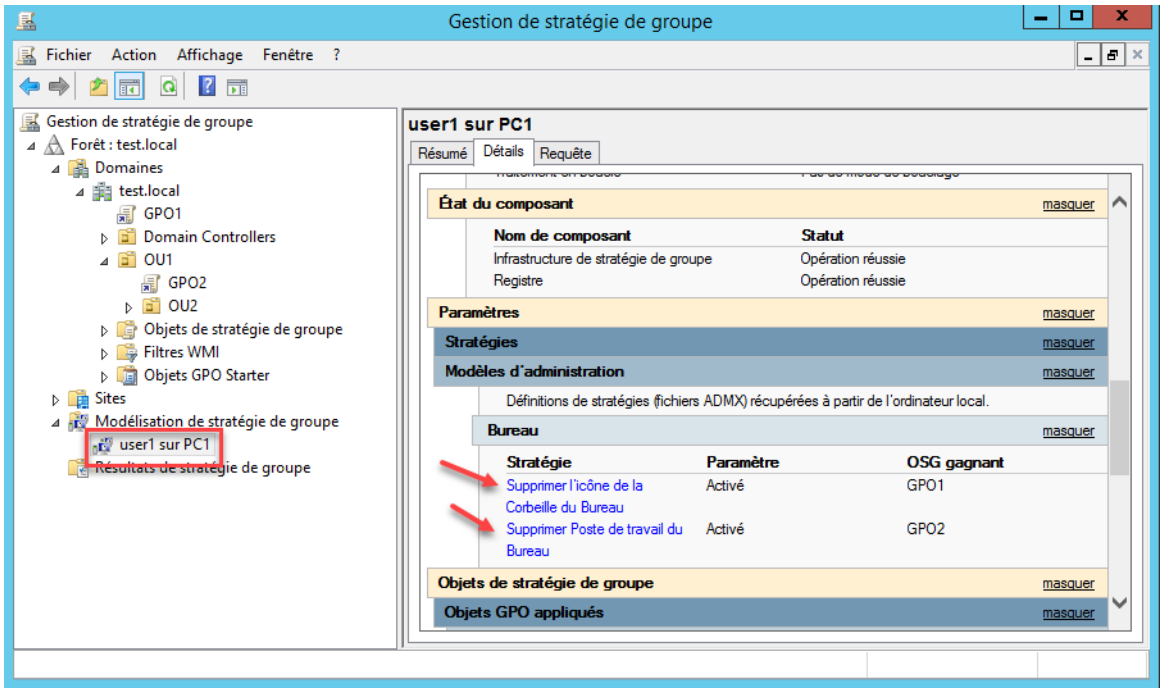


On peut afficher la résultante de superposition des GPO applicables avec l'assistant de Modélisation de stratégie de groupe









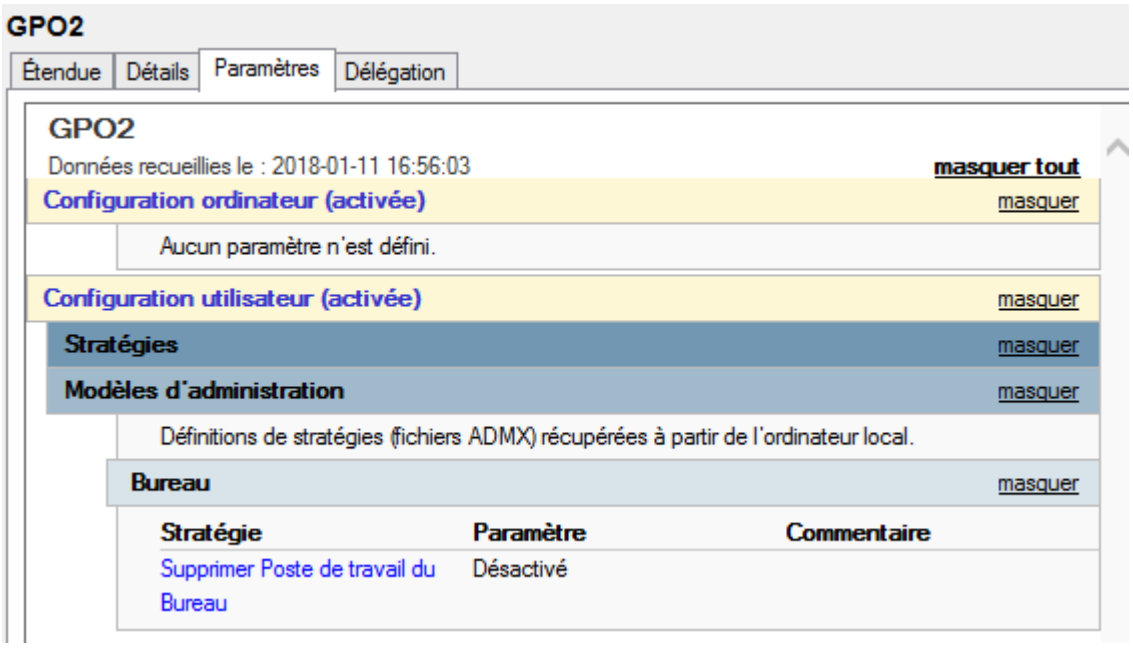
Cas 2

GPO1 a un seul paramètre configuré:

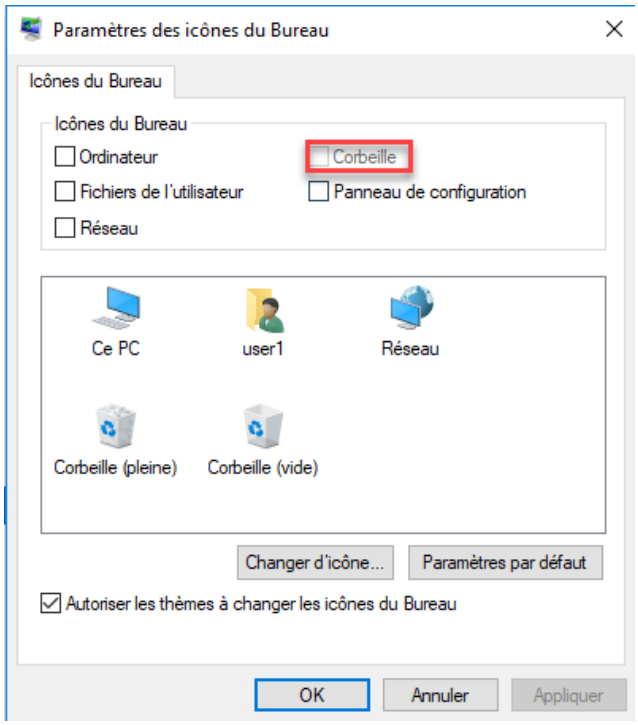
- **Configuration utilisateur** à **Stratégies** à **Modèles d'administration** à **Bureau** à **Supprimer l'icône de la Corbeille du Bureau (Activé)**

- **GPO2** a un seul paramètre configuré:

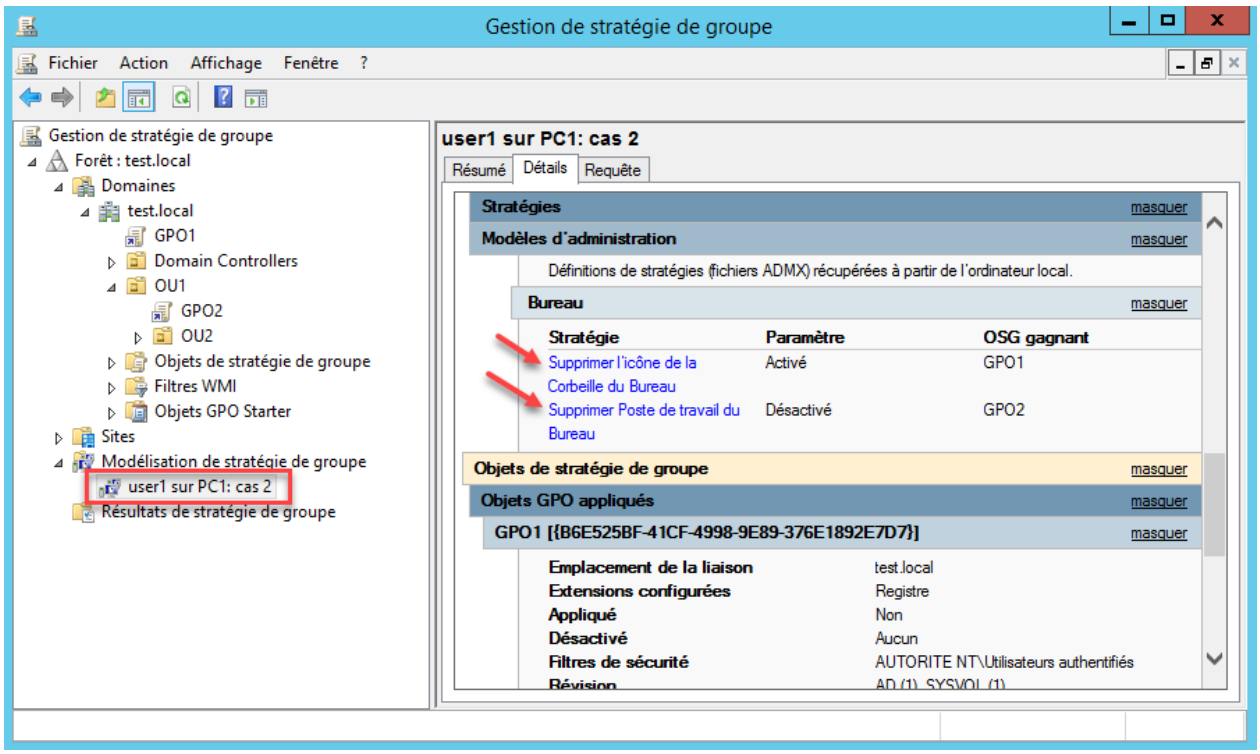
Configuration utilisateur à Stratégies à Modèles d'administration à Bureau à Supprimer poste de travail du Bureau (Désactivé)



Lorsque **user1** se connecte sur **PC1**, seul l'icône de la corbeille sera désactivée puisque le paramètre **supprimer Poste de travail du Bureau** est désactivé



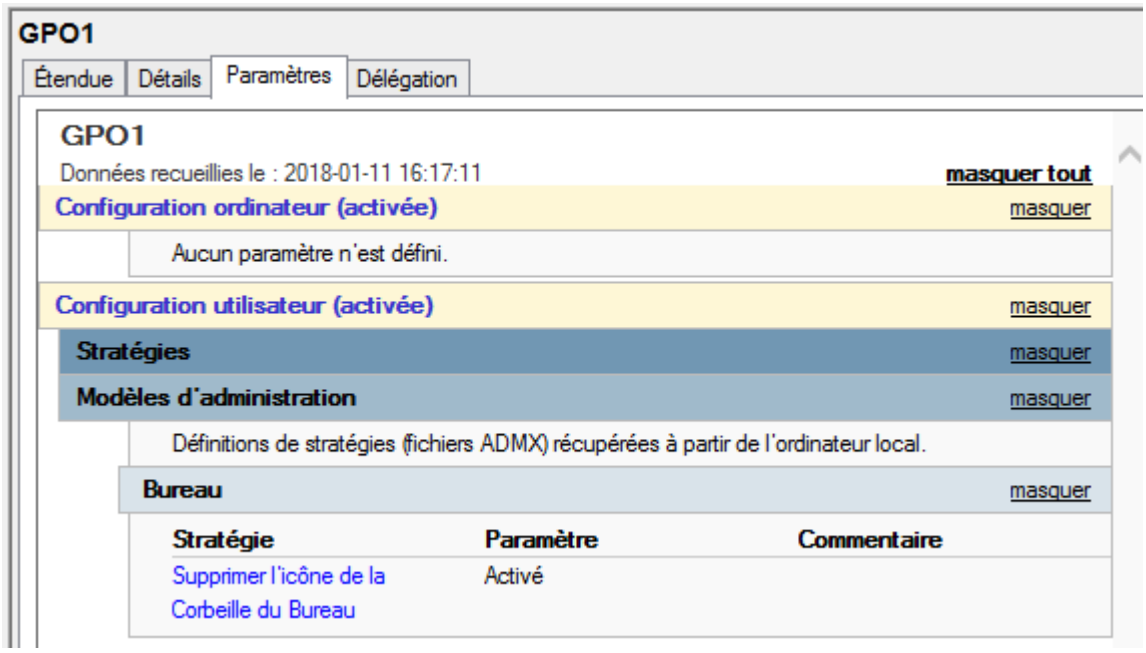
D'ailleurs, si on utilise l'outil de modélisation de stratégie de groupe on aura le résultat suivant:



c. Cas 3

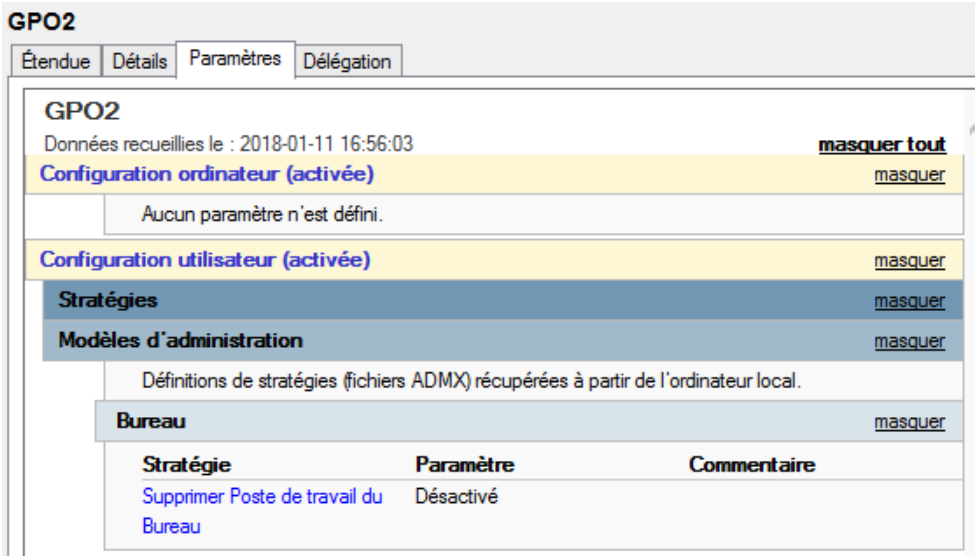
GPO1 a un seul paramètre configuré:

- **Configuration utilisateur** à **Stratégies** à **Modèles d'administration** à **Bureau** à **Supprimer l'icône de la Corbeille du Bureau (Activé)**



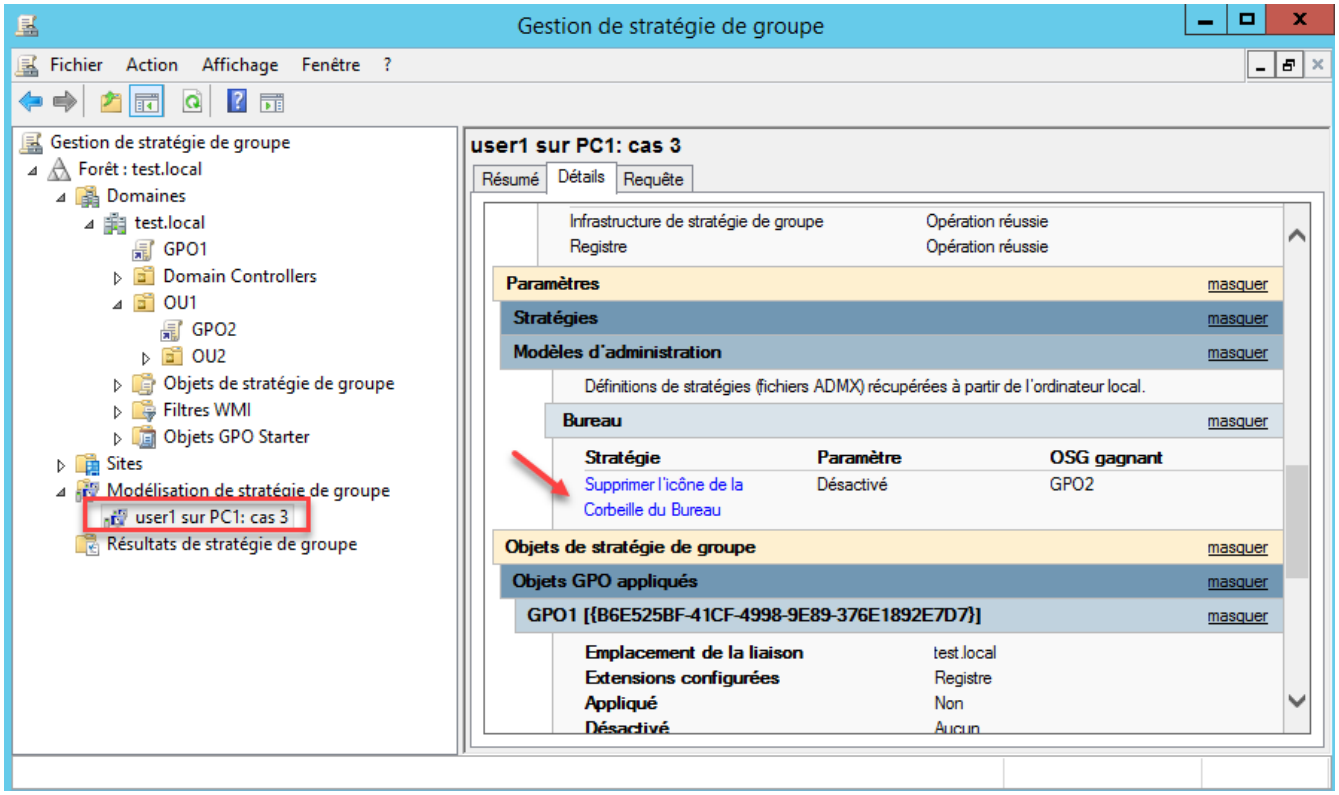
GPO2 a un seul paramètre configuré:

- **Configuration utilisateur** à **Stratégies** à **Modèles d'administration** à **Bureau** à **Supprimer l'icône de la Corbeille du Bureau (Désactivé)**



Le même paramètre est *activé* dans **GPO1** et *désactivé* dans **GPO2**. Quel sera donc le résultat de superposition des 2 GPOs ?

En utilisant la modélisation, le résultat affiché est le suivant:



5. Exemples de paramètres dans GPOs

a. Restreindre accès au panneau de configuration

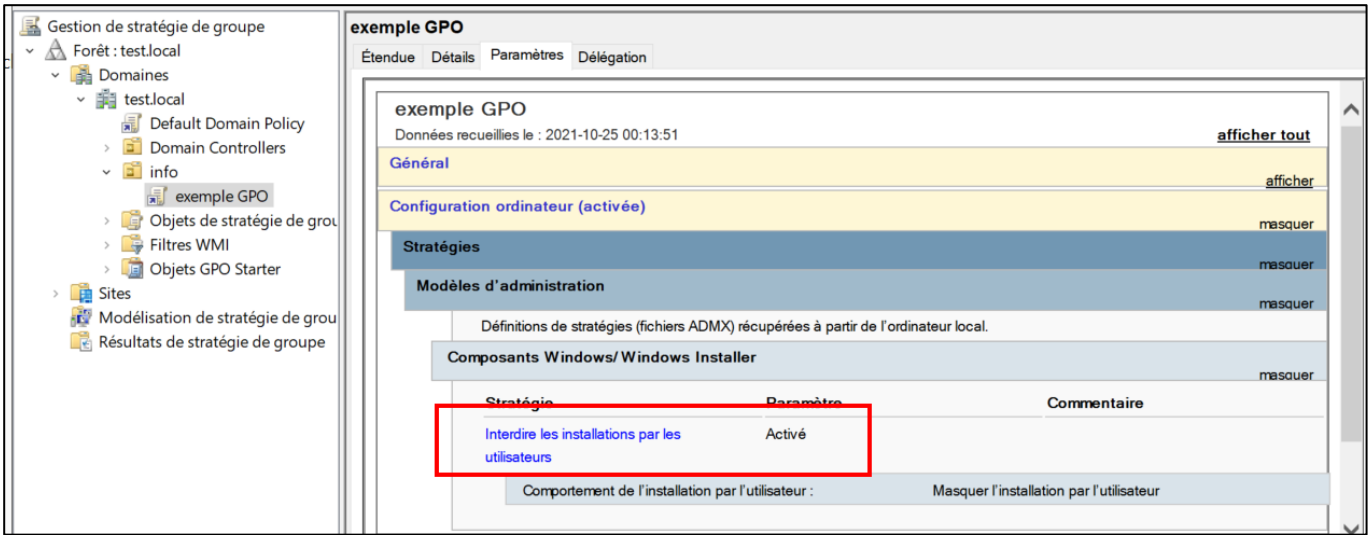
Configuration Utilisateur →·Modèles d'administration →·Panneau de configuration →·Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC → activé

b. Restreindre accès au appareils amovibles (clé USB…)

Configuration Utilisateur →·Modèles d'administration →·Système →·Accès au stockage amovible →·Toutes les classes de stockage amovible: refuser tous les accès → activé

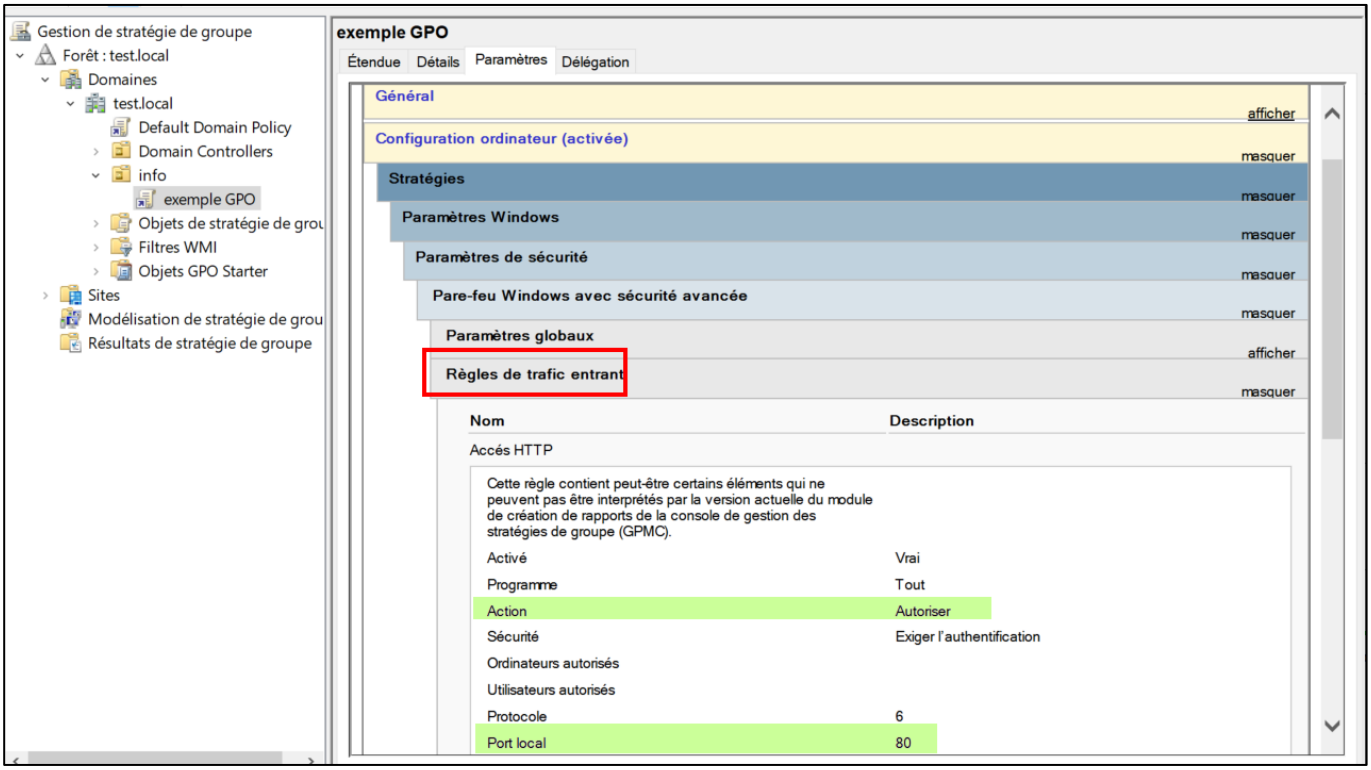
c. Désactiver installation de logiciel par les utilisateurs

Configuration ordinateur →·Modèles d'administration →·Composants Windows →·Windows Installer →·Interdire les installation par les utilisateurs → activé



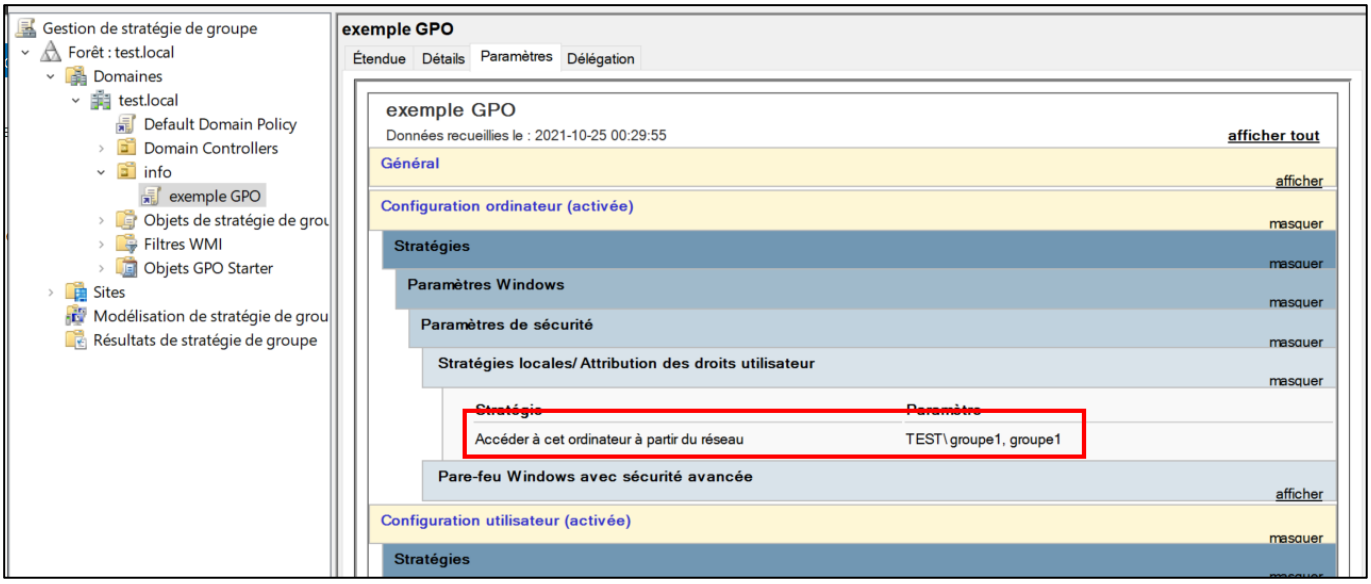
d. Ajouter des règles au pare-feu

Configuration ordinateur → Paramètres Windows → Paramètres de sécurité → Pare-feu Windows avec sécurité avancée → Règles de trafic entrant → ajouter le port à ouvrir (80 dans la capture ci-dessous)



e. Choisir quels comptes qui peuvent se connecter sur une machine

Configuration ordinateur →·Paramètres Windows →·Paramètres de sécurité →·Stratégies locales →·Attribution des droits d'utilisateur →·Accéder à cet ordinateur à partir du réseau (mettez les comptes et groupes autorisés à se connecter sur les ordinateurs appliquant la GPO)

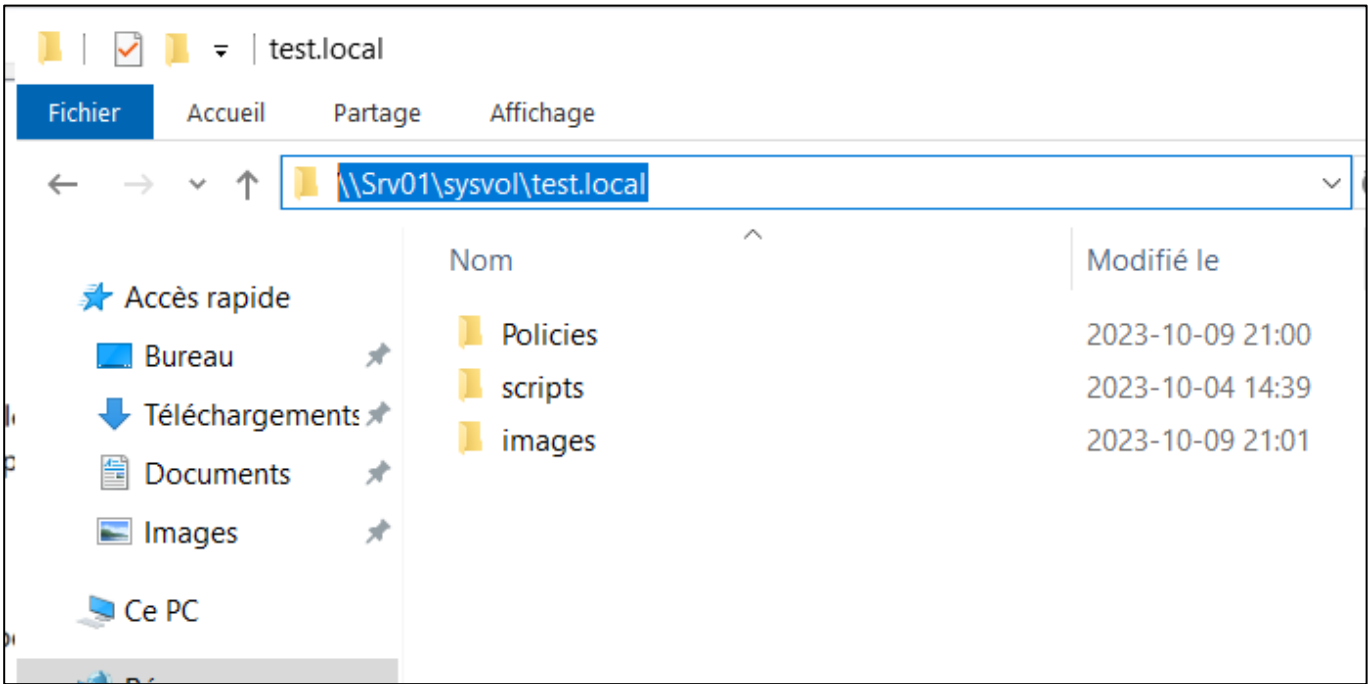


f. Configurer l'arrêt du disque dur après un heure d'inactivité

Configuration ordinateur → Modèles d'administration → Système à Gestion de l'alimentation → Paramètres de disque dur (sur secteur) → Arrêter le disque dur (sur secteur) →·activer avec valeur 3600 secondes (=1heure)

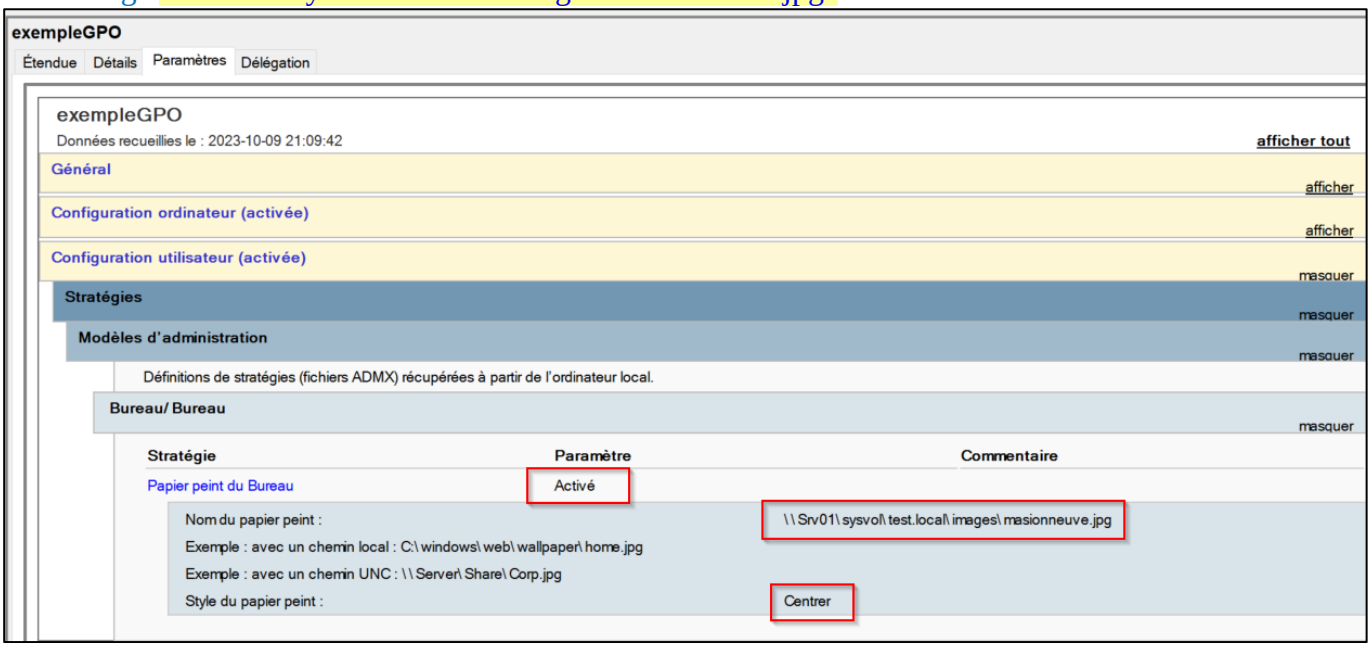
g. Changer l'arrière-plan des ordinateurs

- Commencer par créer un répertoire "images" dans le dossier réseau suivant: \\SRV01\sysvol\test.local



- Dans ce nouveau répertoire, mettez le fichier .jpg à utiliser comme arrière-plan. Dans mon exemple, ce fichier s'appelle **maisonneuve.jpg** donc le chemin d'accès de ce fichier est \\SRV01\sysvol\test.local\images\masionneuve.jpg

  Configuration utilisateur → Modèles d'administration →·Bureau → Bureau → Papier Peint du Bureau →·activer avec chemin d'accès de l'image "\\SRV01\sysvol\test.local\images\masionneuve.jpg"



h. Changer la taille minimale des mots de passes AD

Configuration ordinateur → Stratégies → Paramètres Windows → Paramètres de sécurité → Stratégies de comptes →·Stratégies de mots de pass →·activer avec valeur 7 caractères (ou plus)