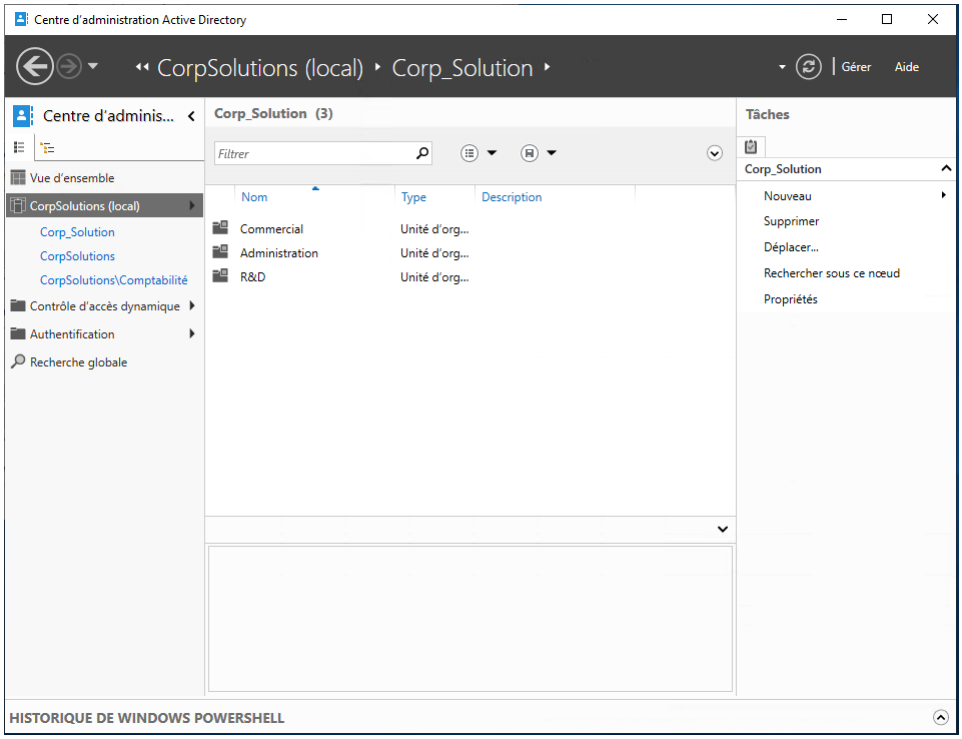
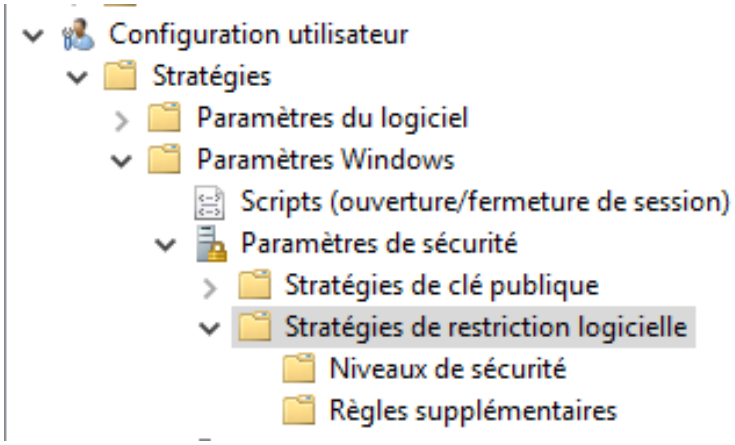
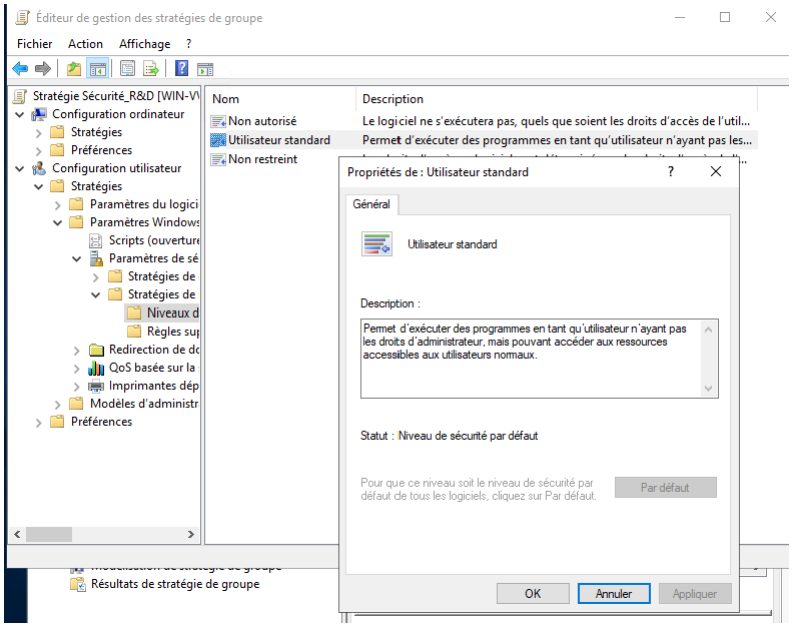
Créer et configurer des GPO pour CorpSolutions Partie 2

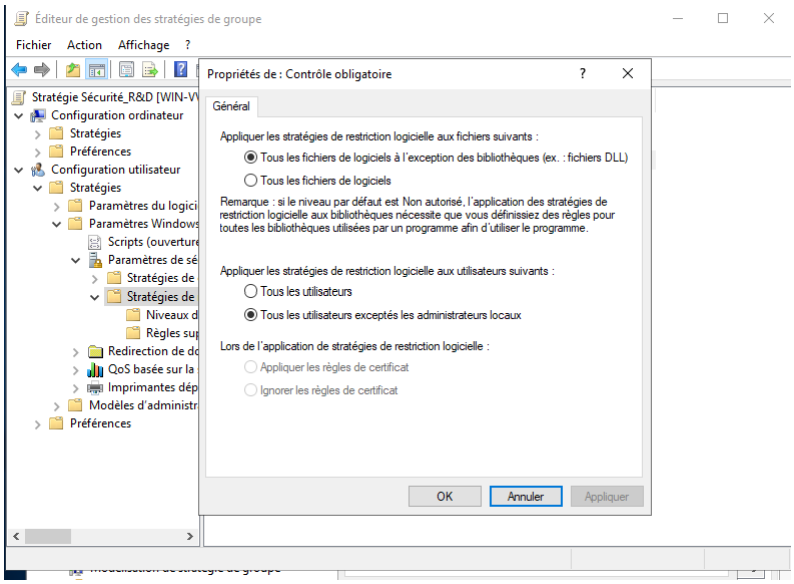
Création des OU :



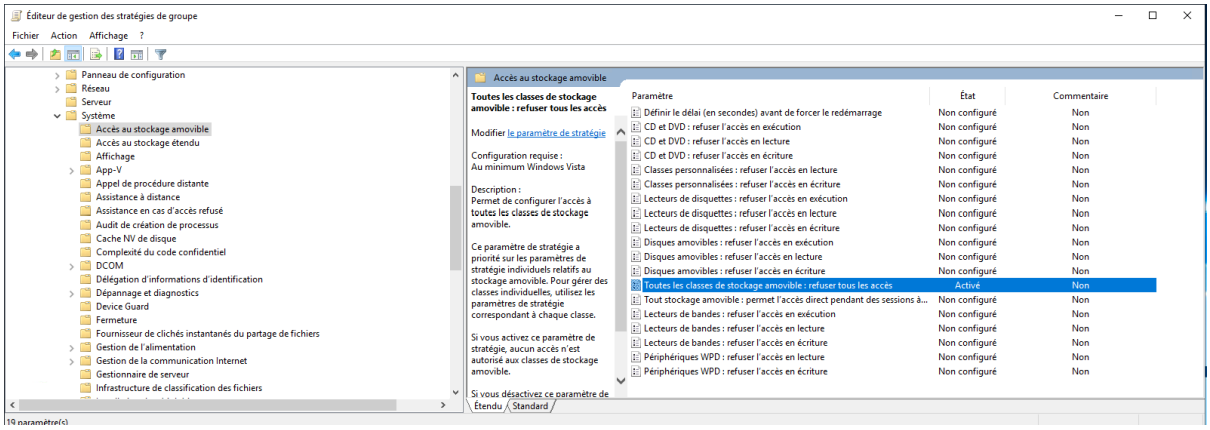
1ère GPO : Sécurité R&D :







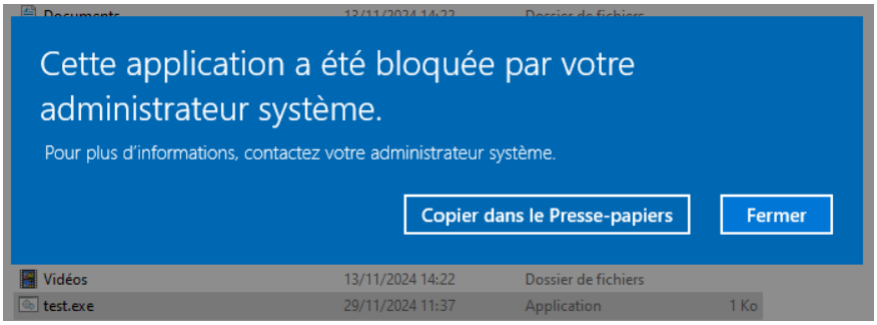
Nous bloquons ainsi l'exécution de certains types de fichiers dont les .bat et les .exe



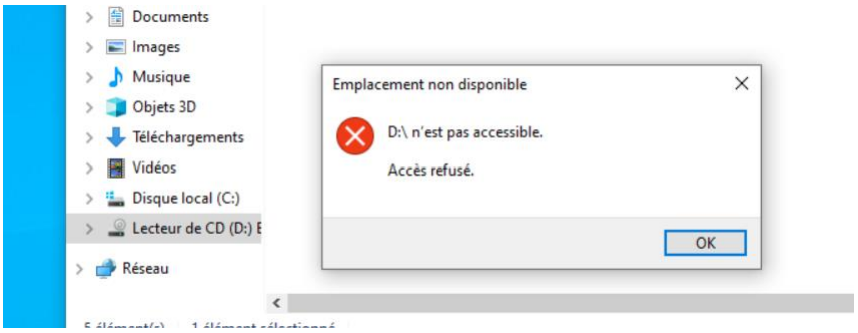
Ici nous bloquons le stockage amovible

Vérification : gpresult /r

a. Bloquer les .exe et les .bat

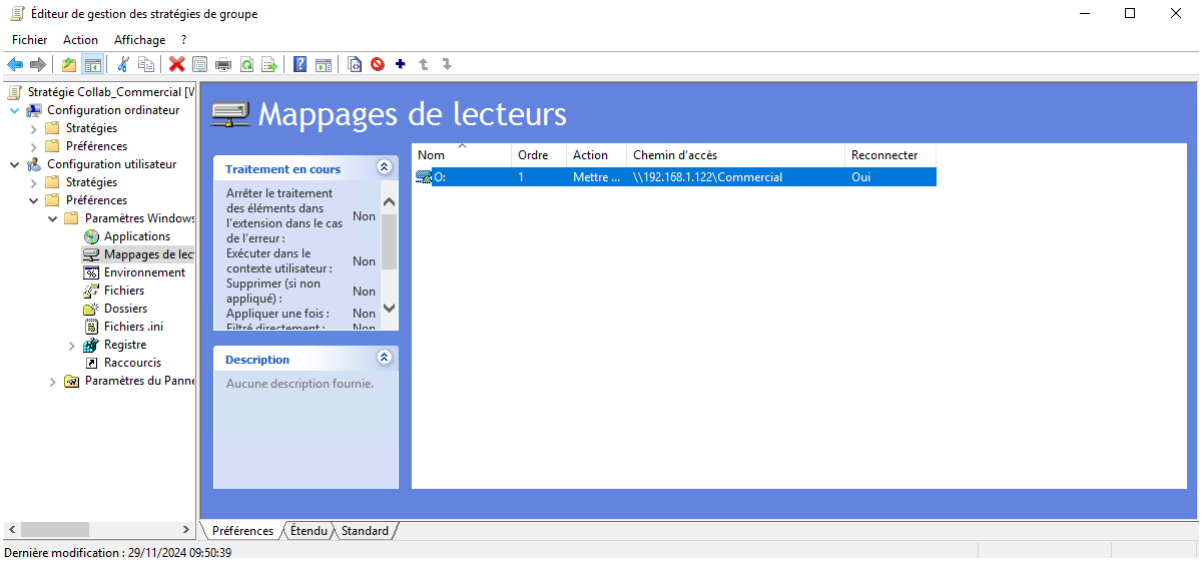


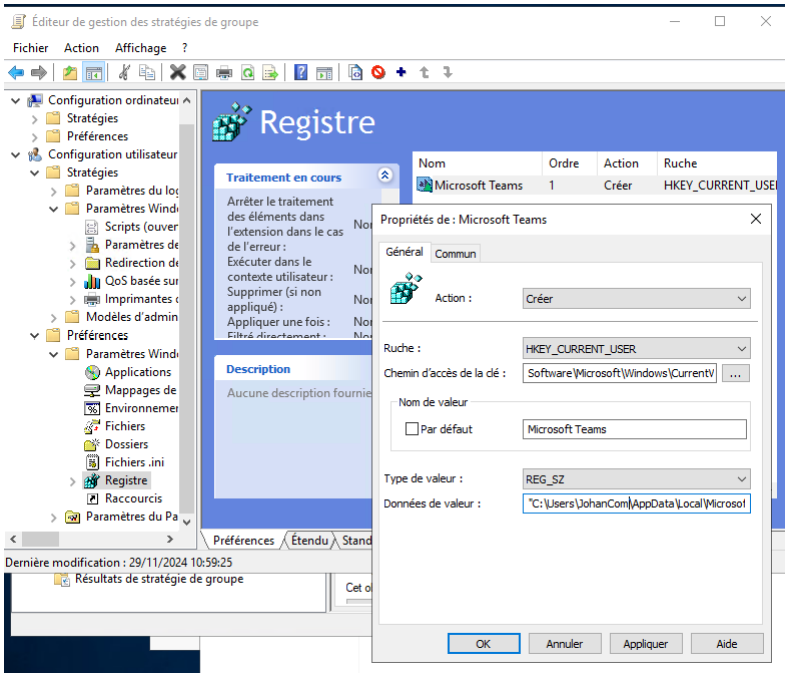
b. Bloquer les périphériques



2ème GPO Collab_Commercial:

Après avoir créé un groupe de sécurité qui comprend les utilisateurs de l'OU commercial et donner les autorisations à ce groupe de lire et écrire dans le dossier commercial, nous devons mapper le lecteur :

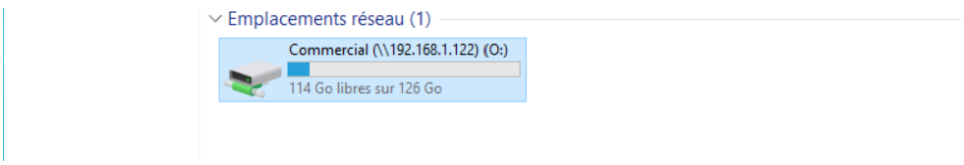




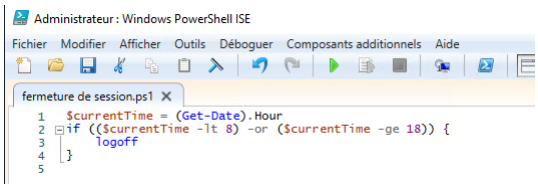
"C:\Users\JohanCom\AppData\Local\Microsoft\Teams\Update.exe" --processStart "Teams.exe" dans données de la valeur

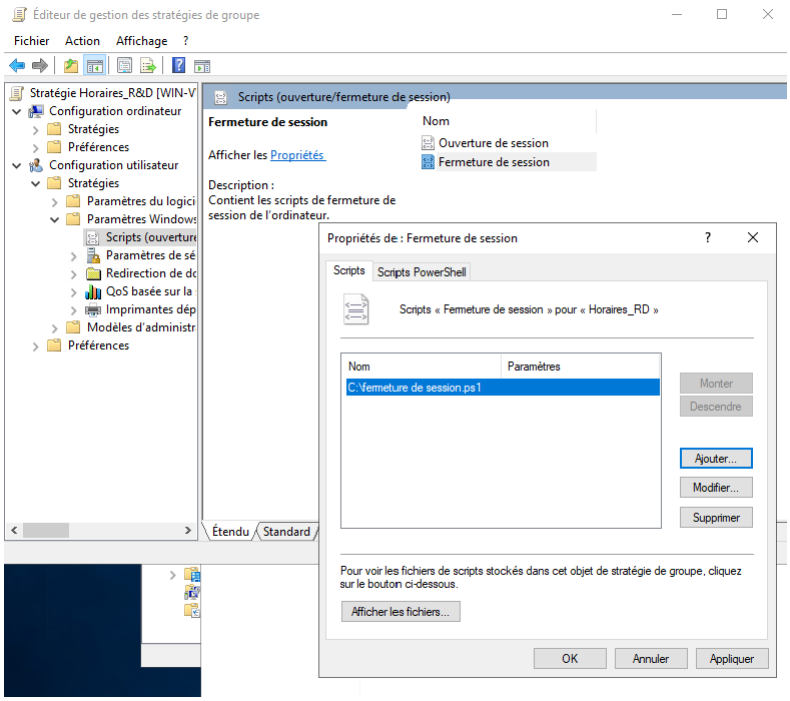
Ainsi par script nous lançons team's au démarrage

Verification: Dossier partagé



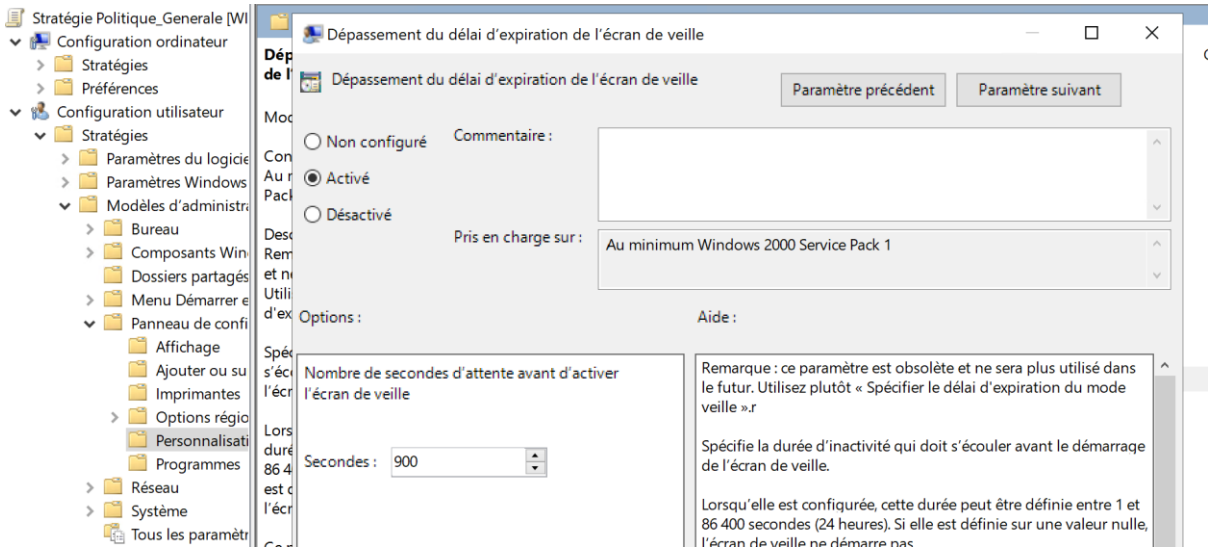
3ème GPO : Contrôle des horaires d'accès aux postes de travail sur l'OU R&D **:**



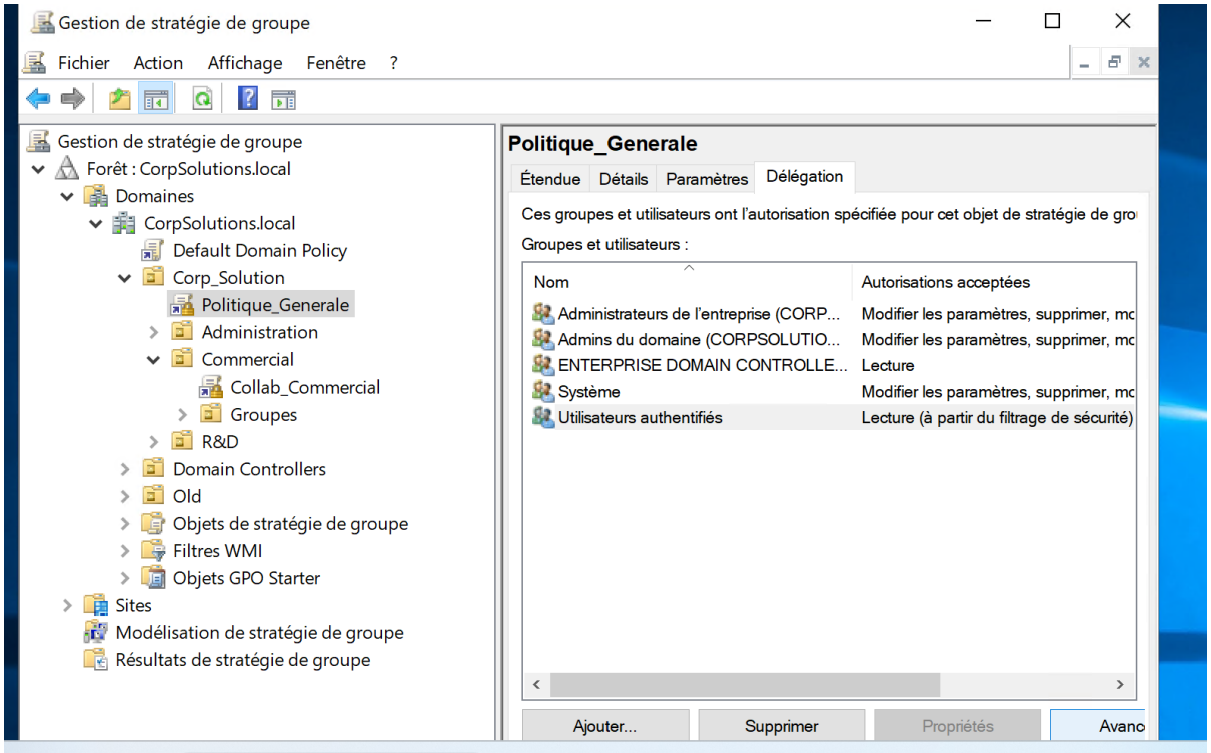


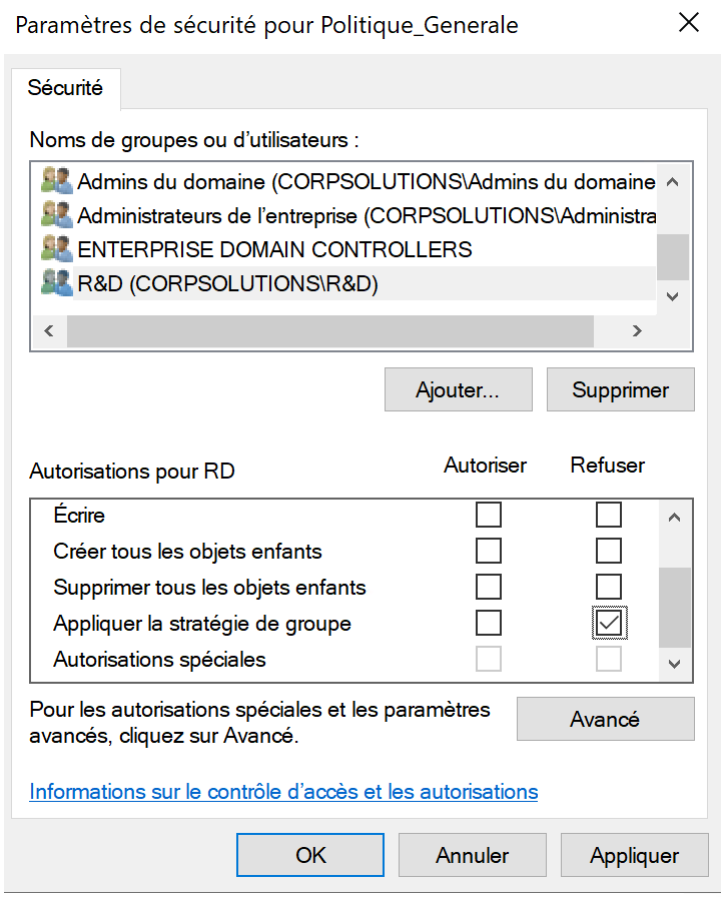
Vérification :

4ème GPO Gestion des conflits :



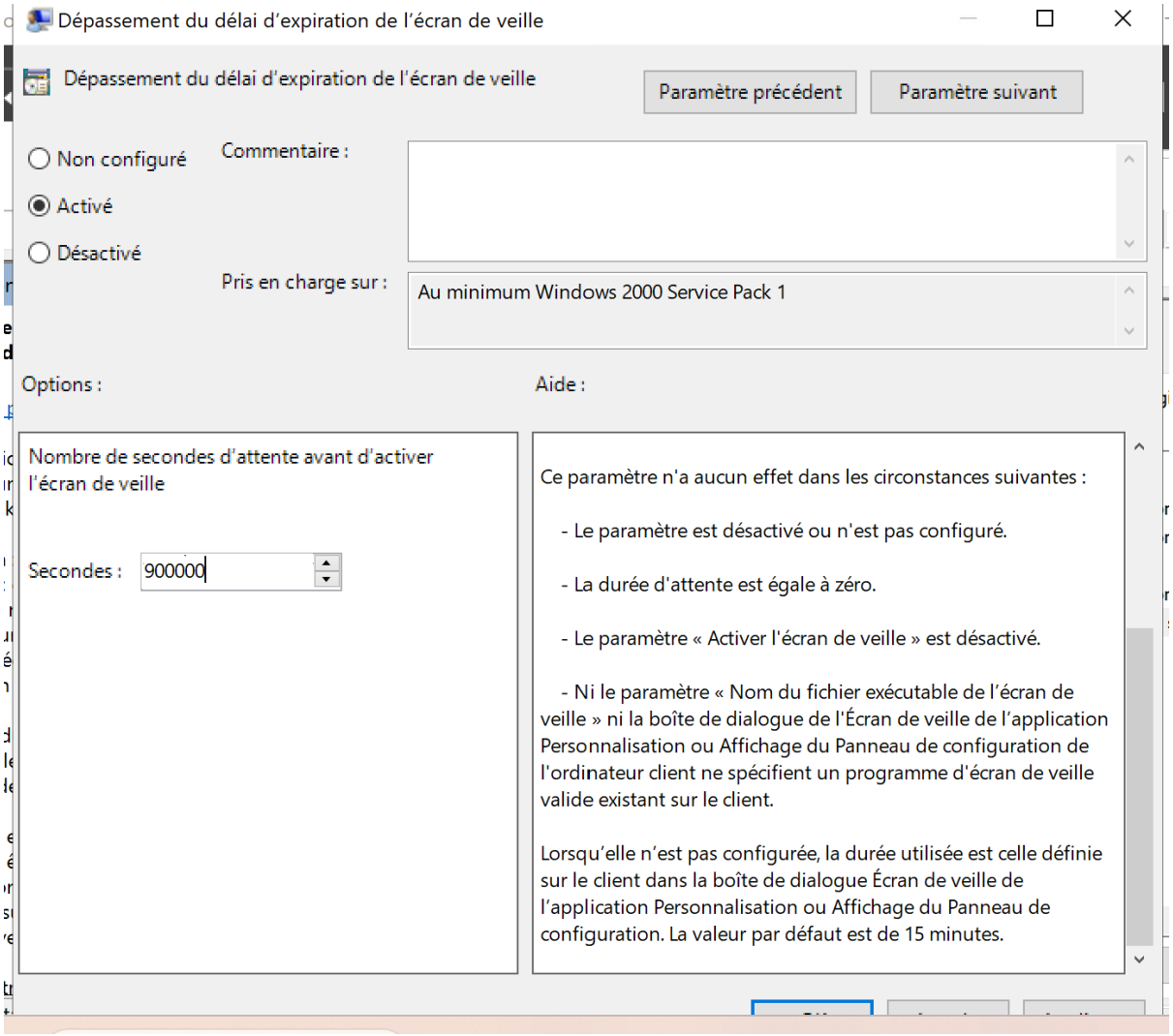
Nous créons ici une GPO de veille de l'écran qui s'applique à l'entièreté de CorpSolutions.





Après avoir créé le groupe de sécurité comprenant les utilisateurs de R&D nous décidons de Refuser la GPO pour ce groupe

Maintenant nous allons regarder de plus près l'incohérence que nous allons créer sur l'OU commercial



L'observateur d'évènement comme vous le voyez ci-dessous montre bien que c'est la GPO qui est appliqué sur l'OU Commercial qui prend le dessus.

Synthèse et question :

1. Les filtres de sécurité qui sont gérés par des groupes de sécurité et dans les délégations sont primordiaux. En effet dans une entreprise nous devons segmenter les activités. Ainsi les recommandations et les besoins sont différents d'un service à l'autre et même parfois à l'intérieur d'un service. De plus un Active Directory bien sécurisé est un Active Directory bien segmenté avec des autorisations spécifique et granulaires qui sont aussi gérés par des groupes de sécurité.

2. Dans l'application des GPO nous pouvons diagnostiquer les erreurs avec 2 outils principalement :
    a. gpresult /r
    b. Observateur d'évènements

3. Pour résoudre les conflits entre deux GPO il faut 1 diagnostiquer et 2 remédier au plus près de la cible. Dans la dernière OU de préférence.