

UH2C | E N S E T

GUIDE COMPLET

Gestion des stratégies de groupe (GPO) et sécurisation des postes de travail



RÉALISÉ PAR :
RABIH RAJAA

PROF :
M. KHIAT

2024-2025

Sommaire

Introduction.....	3
PRÉREQUIS.....	4
CRÉATION DES UNITÉS D'ORGANISATION (OU).....	4
Créer des utilisateurs et des groupes dans les UO.....	5
Créer un groupe des utilisateurs :	7
Group Policy Object (GPO) :	10
Bloquer les USB	11
Bloquer PowerShell	16
Cacher la propriété de l'ordinateur :.....	19
Changer le Background de bureau de tous les utilisateurs.....	20
Planifier l'arrêt automatique des ordinateurs	27
Configurer les stratégies de mots de passe.....	37
Désactivation du Panneau de configuration	42
Conclusion	45

Introduction

Dans un environnement réseau d'entreprise, la gestion centralisée de la configuration des ordinateurs et des comptes utilisateurs est cruciale pour garantir la sécurité, la productivité et l'uniformité. Les **Stratégies de Groupe (Group Policy Object - GPO)** offrent aux administrateurs système une méthode efficace pour appliquer automatiquement des règles et des restrictions à l'ensemble des postes clients connectés à un domaine Active Directory. Ce rapport présente la mise en place de différents GPO visant à renforcer la sécurité du système d'information, améliorer l'expérience utilisateur et automatiser certaines tâches administratives.

Objectifs

L'objectif de ce travail est de :

- Comprendre le rôle des GPO dans un environnement Windows Server.
- Créer et gérer des objets de stratégie de groupe.
- Appliquer différentes stratégies afin de :
 - ☒ Bloquer l'accès aux ports USB.
 - ☒ Désactiver PowerShell pour limiter l'exécution de scripts.
 - ☒ Masquer la propriété de l'ordinateur.
 - ☒ Changer le fond d'écran de tous les utilisateurs.
 - ☒ Planifier l'arrêt automatique des ordinateurs.
 - ☒ Appliquer des règles de mot de passe sécurisées.
 - ☒ Désactiver l'accès au Panneau de configuration.

PRÉREQUIS

Machine virtuelle Windows Server 2022/2019 avec :

- AD DS (Active Directory Domain Services) configuré.
- DNS et DHCP fonctionnels.

Machine cliente Windows 10/11 Pro jointe au domaine.

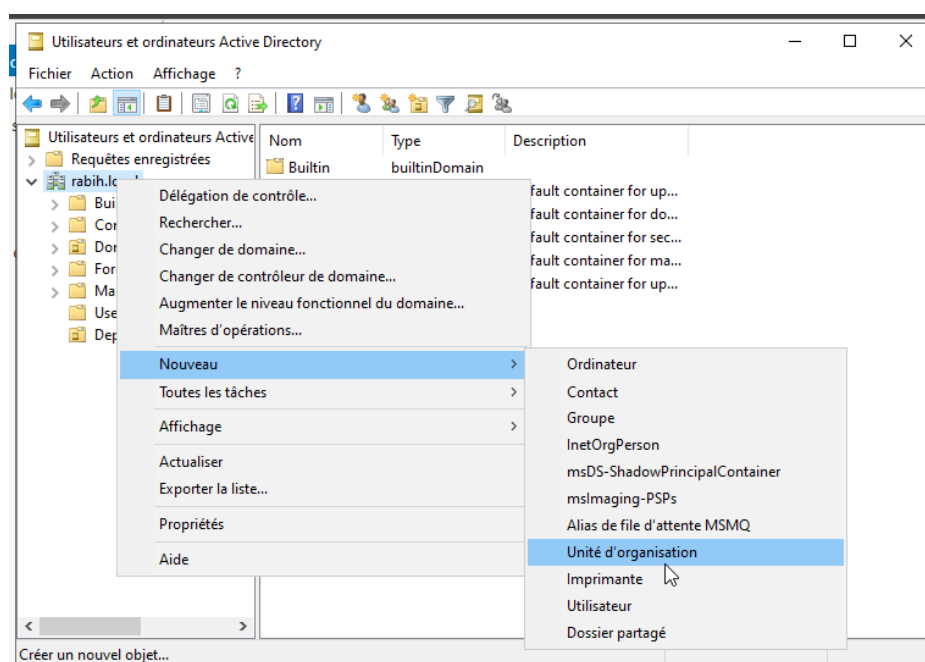
CRÉATION DES UNITÉS D'ORGANISATION (OU)

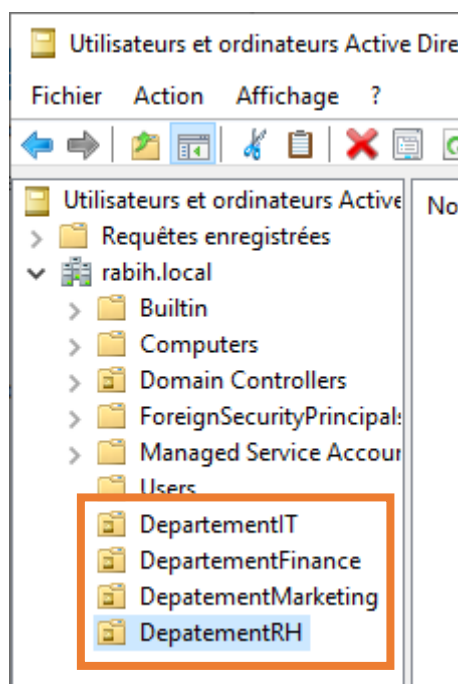
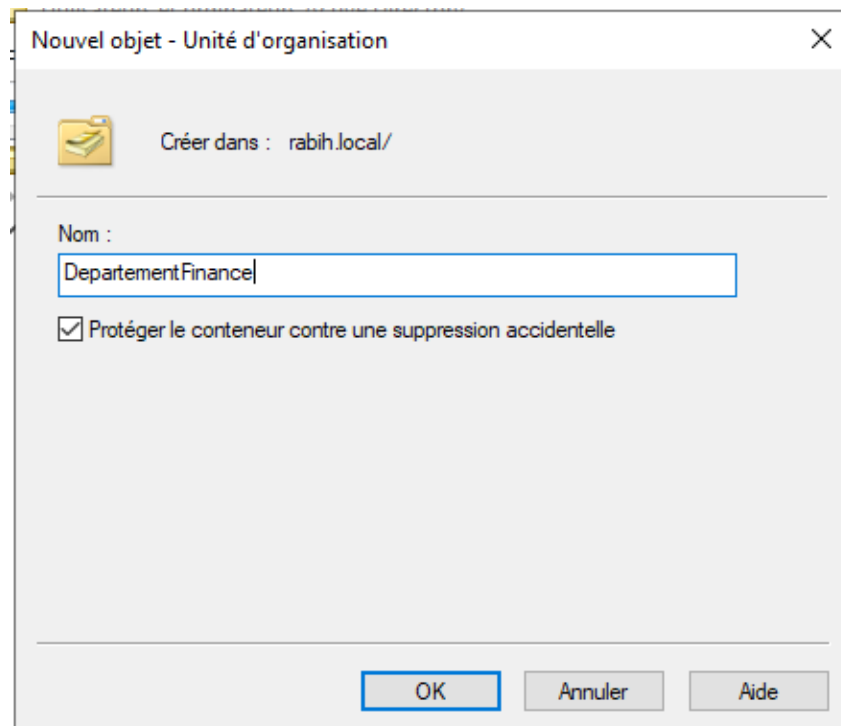
Pour simuler une entreprise, nous avons créé les OU suivantes :

- Département Finance
- Département RH
- Département Marketing
- Département IT

Ces OU permettent d'appliquer des GPO différenciées selon les besoins de chaque service. Sur le serveur Active Directory, ouvrez : **Gestionnaire de serveur** → **Outils** → **Utilisateurs et ordinateurs Active Directory (ADUC)**

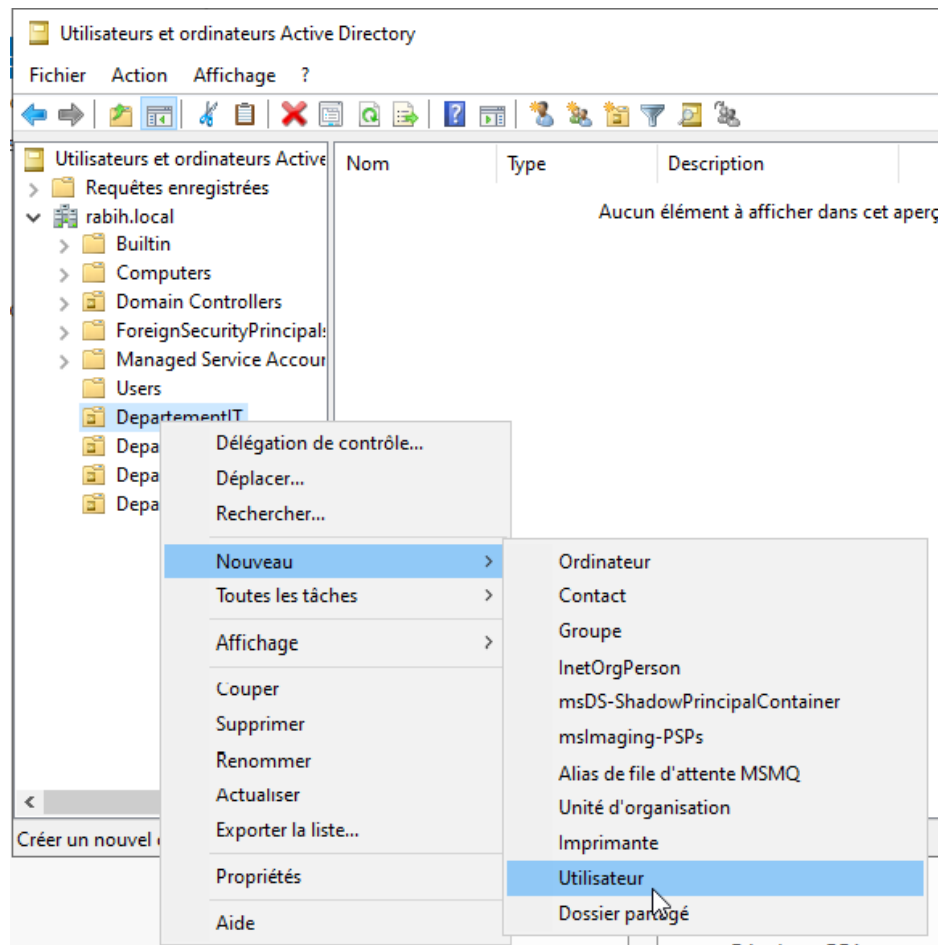
Clic droit sur le domaine (**rabih.local**) → **Nouveau** → **Unité d'organisation**





Créer des utilisateurs et des groupes dans les UO

Après on crée des utilisateurs dans une unité d'organisation. Afin d'appliquer une stratégie (GPO) sur cette unité. Dans l'arborescence de la console, cliquez avec le bouton droit sur l'unité d'organisation à laquelle vous souhaitez ajouter le compte d'utilisateur, puis pointez sur New, puis cliquez sur User



Saisissez le prénom de l'utilisateur, son nom et les autres champs, puis cliquez sur suivant :

Nouvel objet - Utilisateur [X]

Créer dans : rabih.local/DepartementIT

Prénom : Initiales :

Nom :

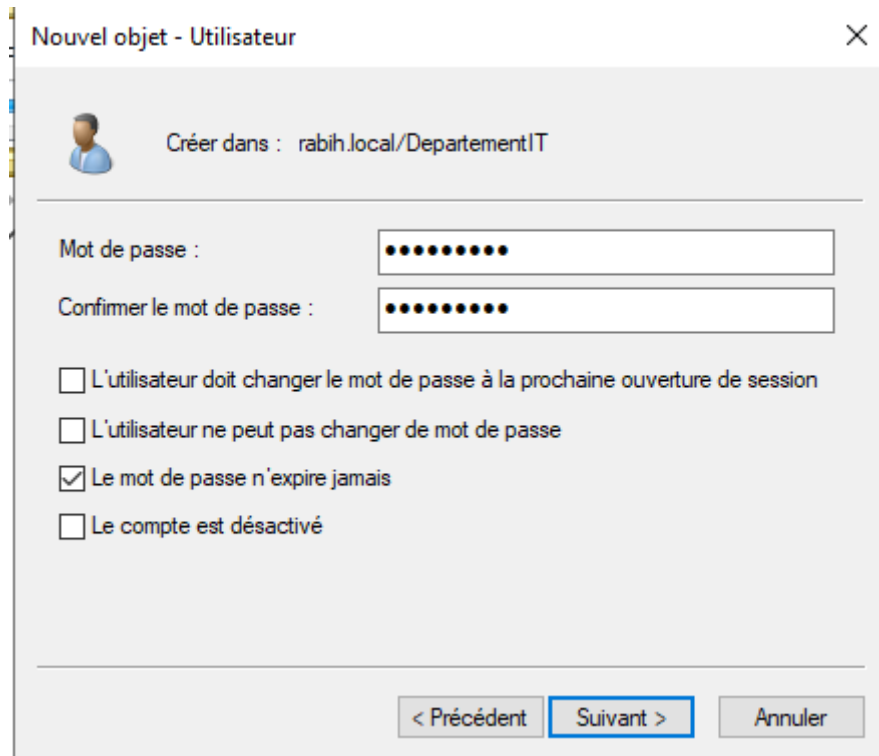
Nom complet :

Nom d'ouverture de session de l'utilisateur : @rabih.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

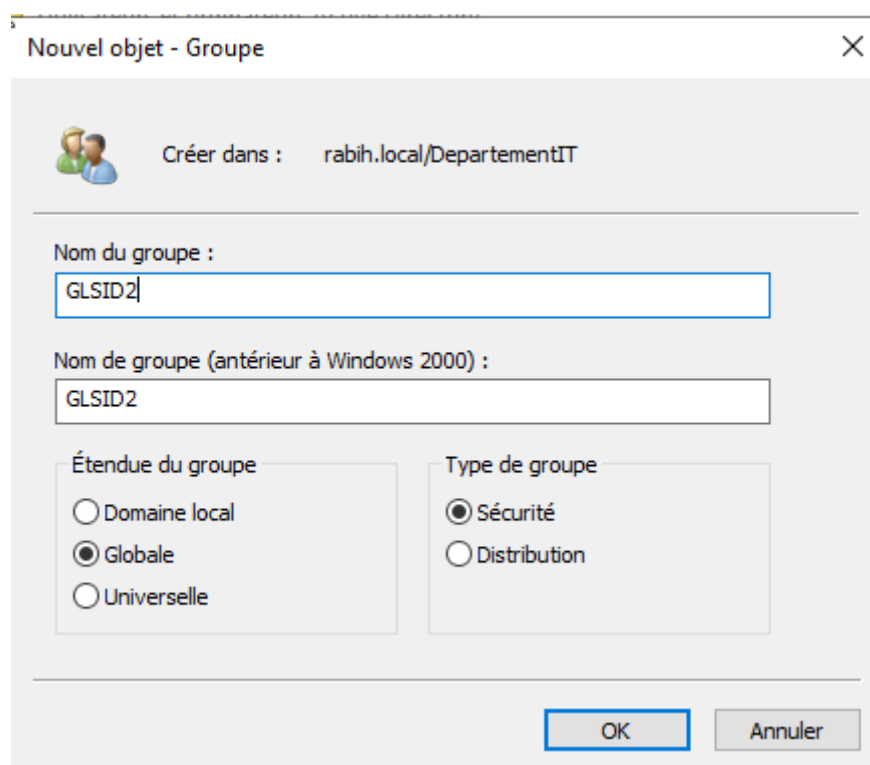
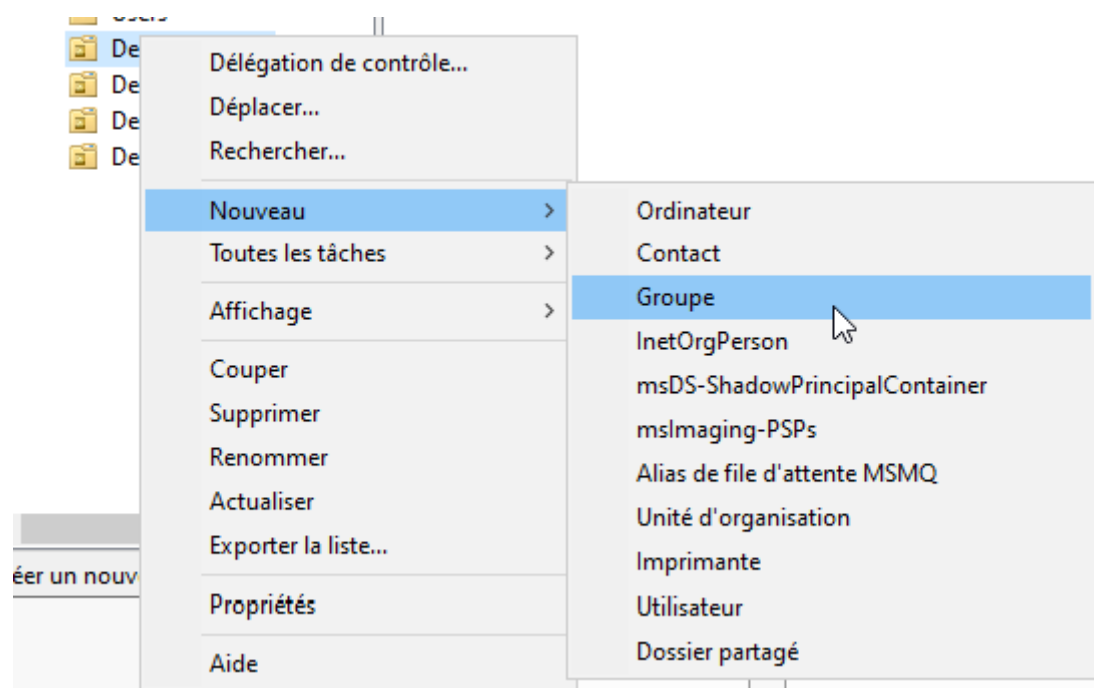
< Précédent **Suivant >** Annuler

Entrez le mot de passe de l'utilisateur, puis sélectionnez les options appropriées du mot de passe, puis cliquez sur suivant :

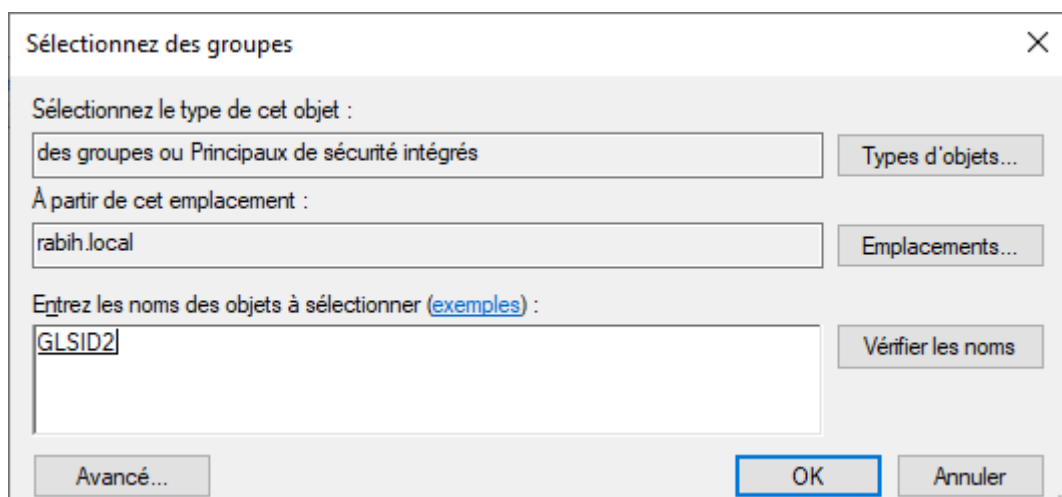
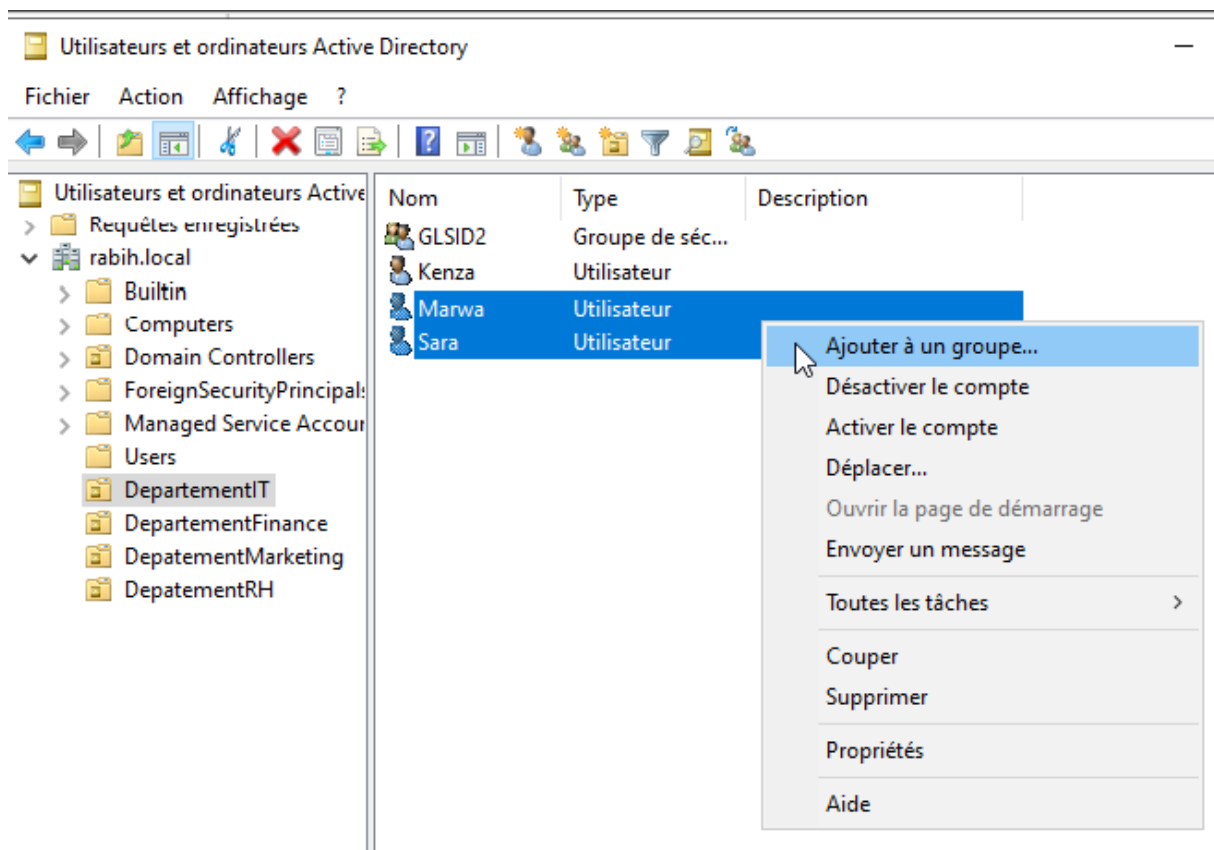


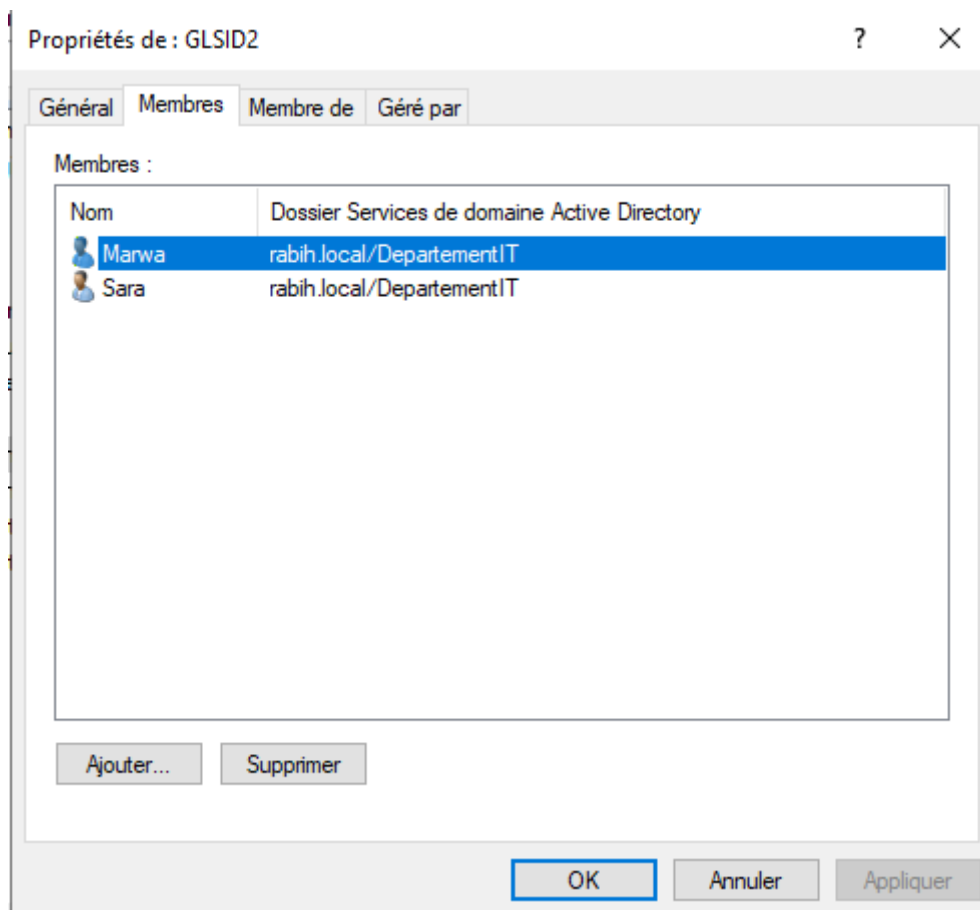
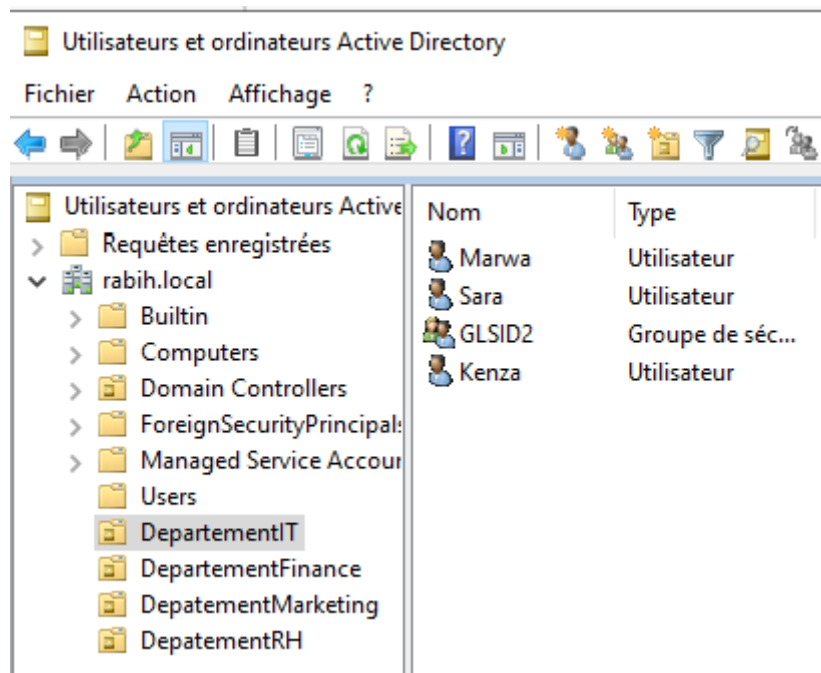
Créer un groupe des utilisateurs :

Les groupes dans les services de domaine Active Directory (AD DS) sont des objets d'annuaire qui résident dans un domaine et dans des objets conteneur d'unité d'organisation. AD DS fournit un jeu de groupes par défaut à l'installation. Il fournit aussi une option pour créer des groupes.



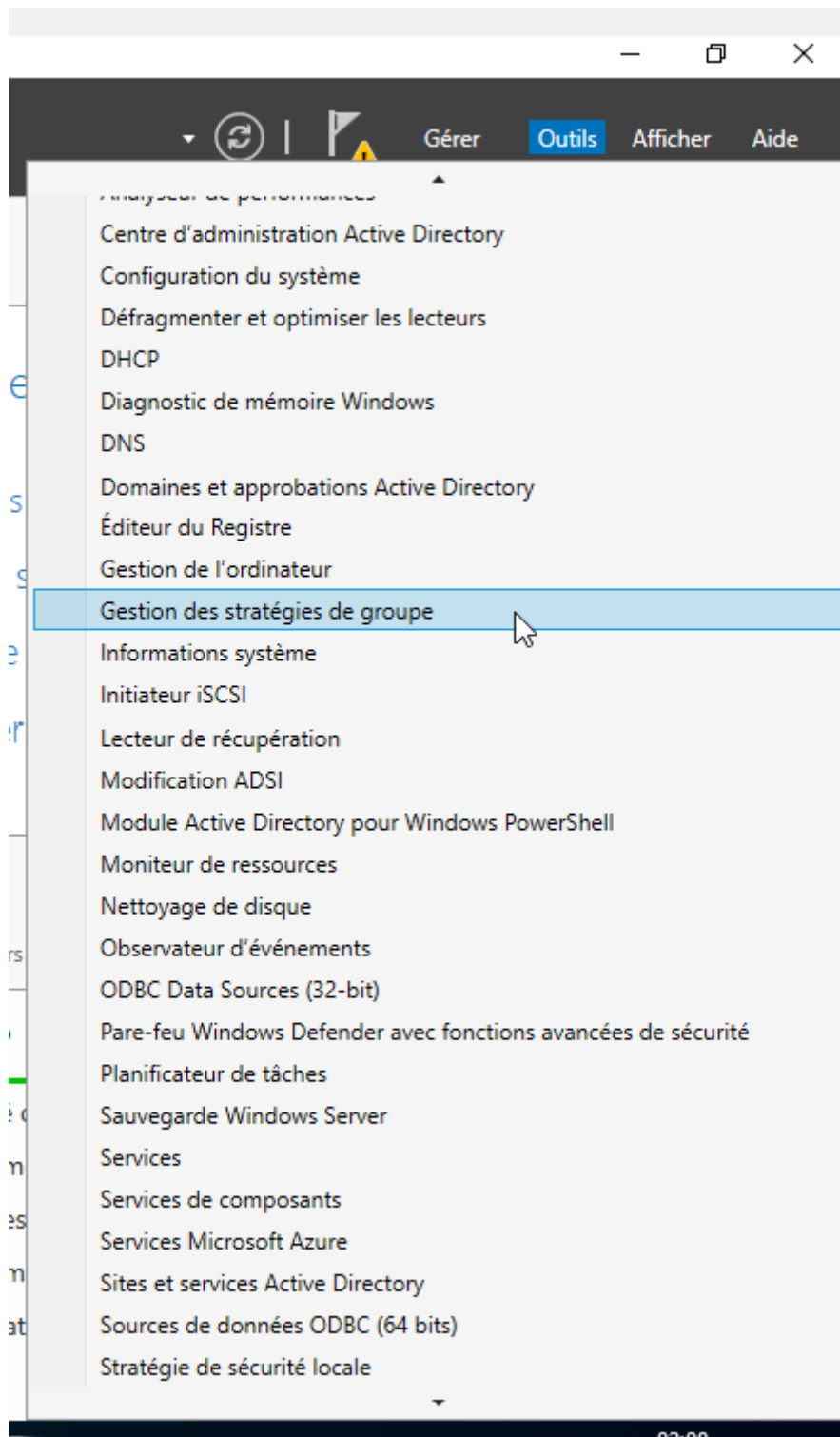
Ajouter des membres au groupe créé :





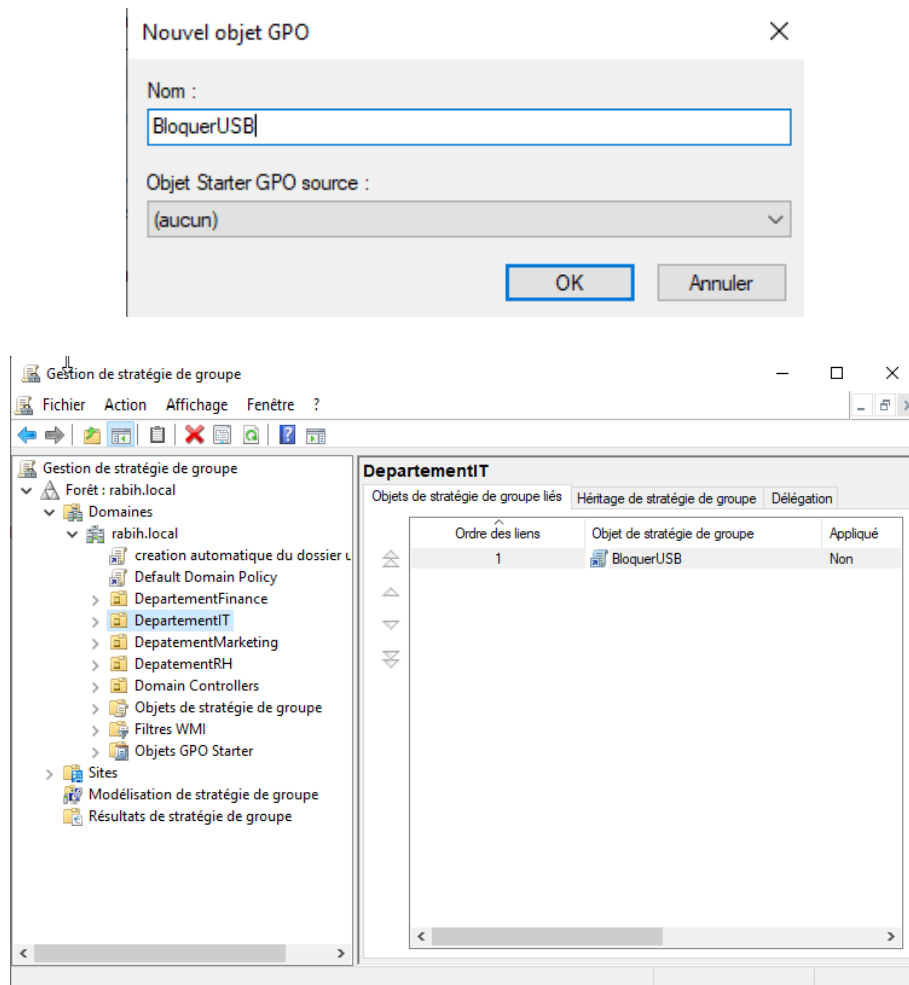
Group Policy Object (GPO) :

Cliquez sur "Outils" puis "Gestion des stratégies de groupe" pour ouvrir la console.

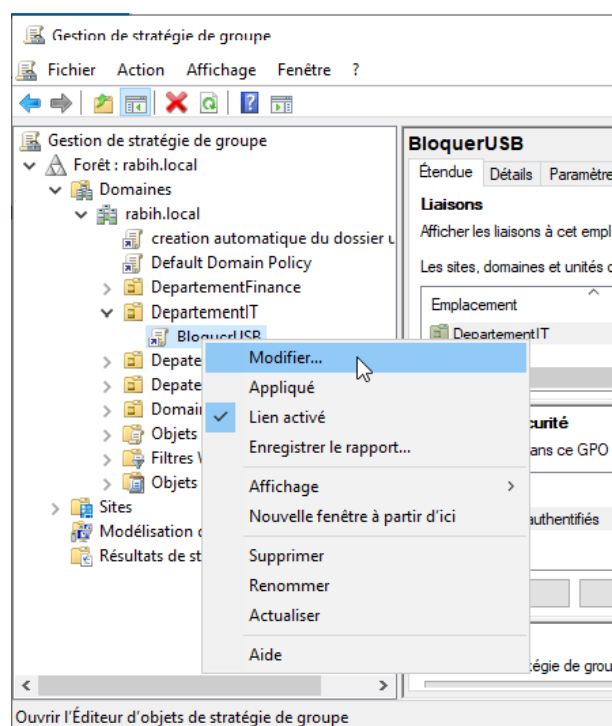


Bloquer les USB

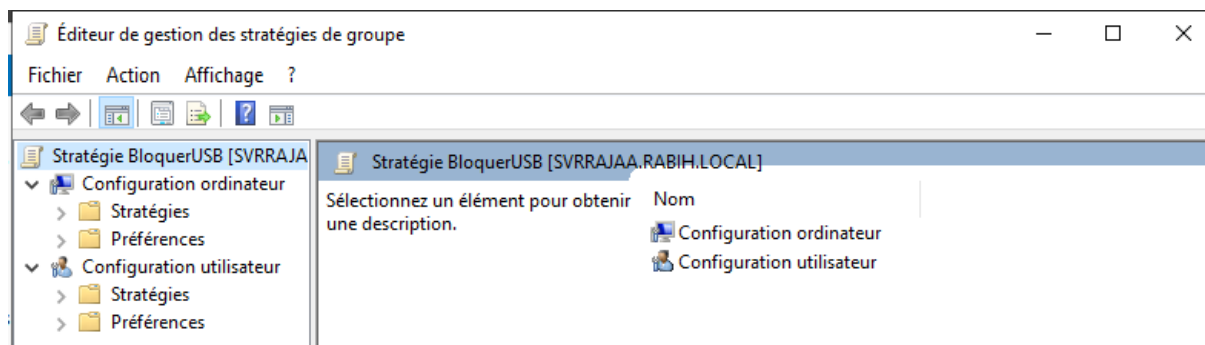
Dans cette partie, nous allons voir comment créer une GPO, et surtout comment configurer les paramètres qui s'y trouvent, pour enfin l'appliquer sur des utilisateurs et ordinateurs. Dans cet exemple, on va créer une stratégie de groupe pour refuser l'accès aux périphériques de stockage comme USB et Disque.... Cette action simple est très répandue en entreprise.



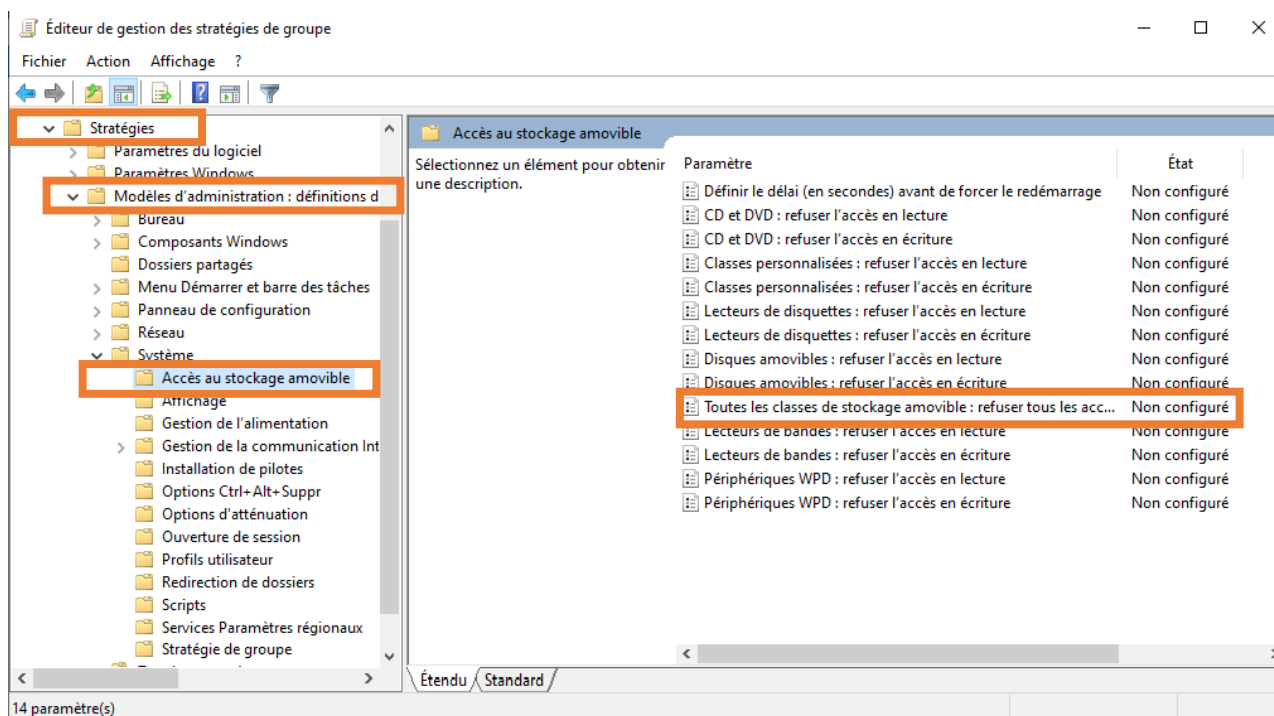
Passant maintenant à la Modification des paramètres de cette stratégie.

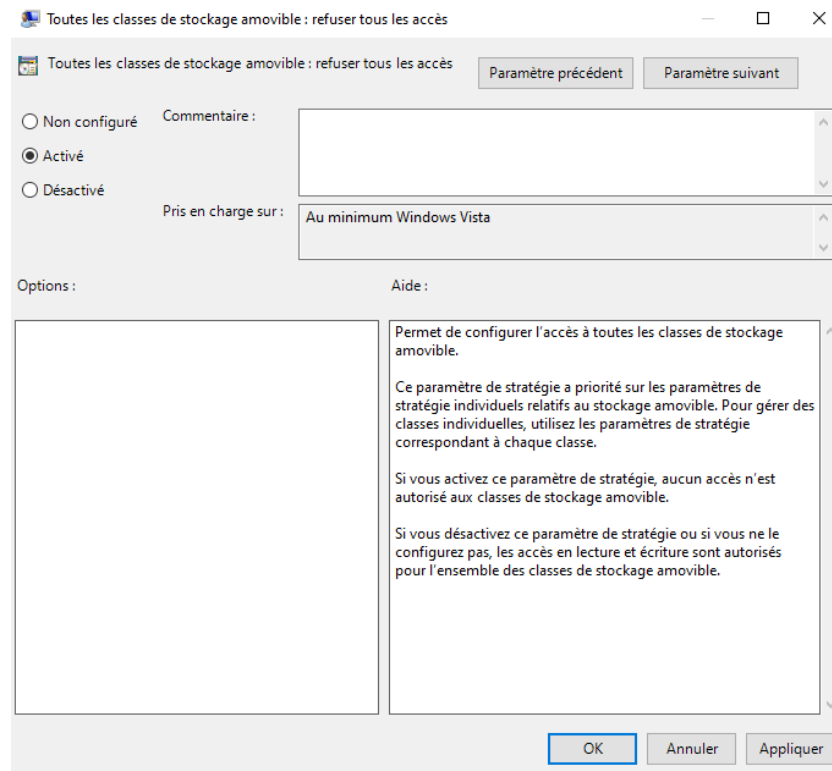


Une fenêtre "Éditeur de gestion des stratégies de groupe" va s'ouvrir, cela permet de configurer la GPO. Autrement dit, c'est ici que l'on va activer ou configurer certains paramètres à appliquer sur les utilisateurs (ou les ordinateurs).



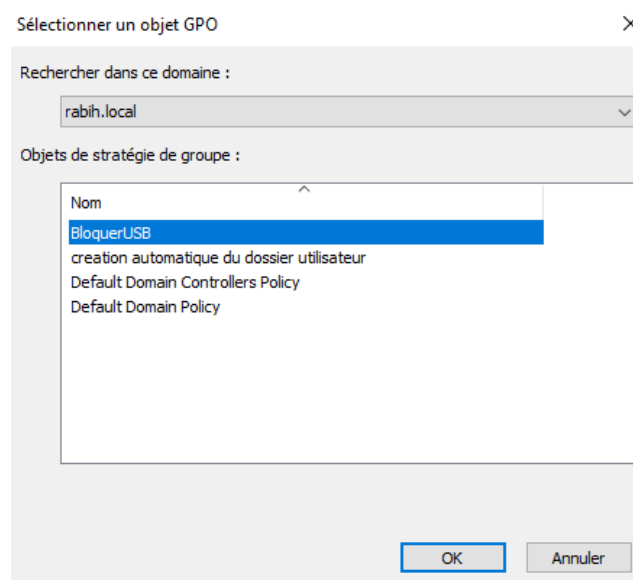
L'objectif maintenant va être de trouver le paramètre qui permet de refuser l'accès aux périphériques de stockage. Voici le chemin vers notre paramètre : Configuration utilisateur > Stratégies > Modèles d'administration > Système > Périphériques de stockage amovibles. Double-cliquez dessus.

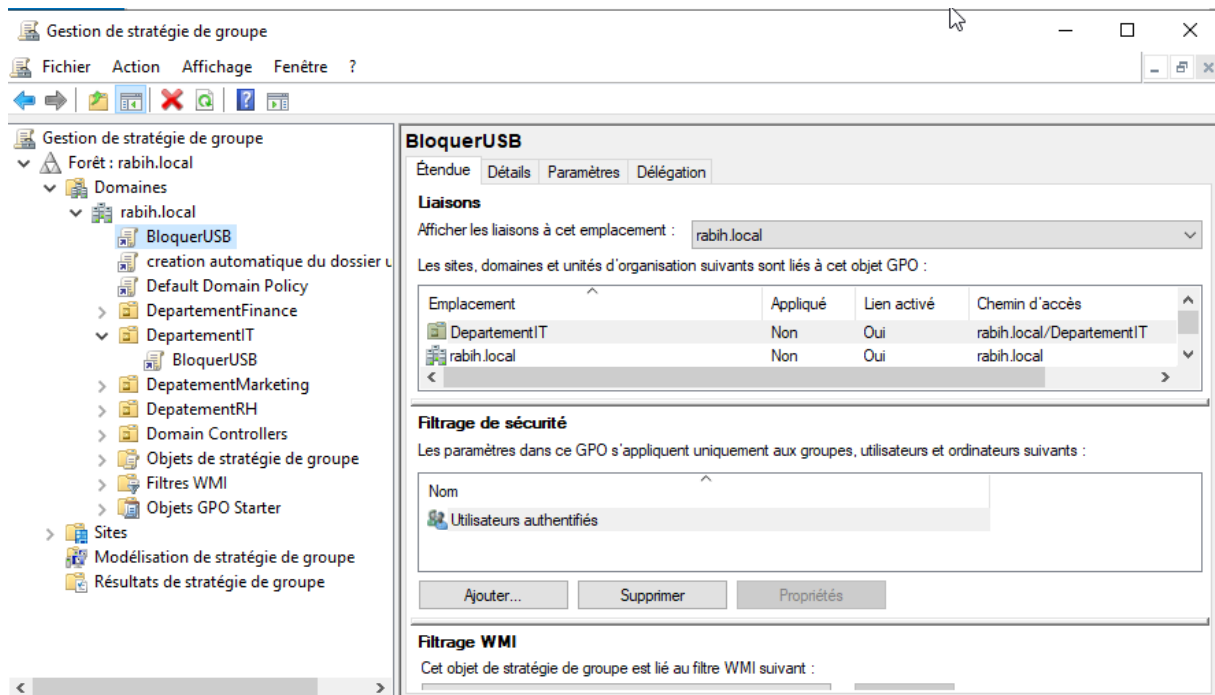




Donc on active cette stratégie et click sur OK.

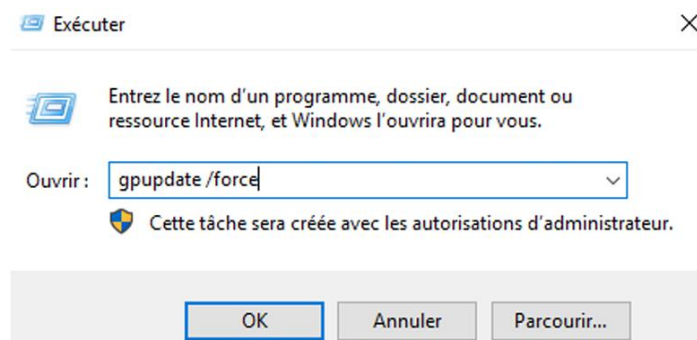
- Gestion des liens de GPO Pour créer une liaison entre une GPO et une unité d'organisation, effectuez un clic droit sur le domaine et cliquez sur "Lier un objet de stratégie de groupe existant". Puis choisir la GPO déjà créée « **BloquerUSB** », ensuite cliquer sur OK :

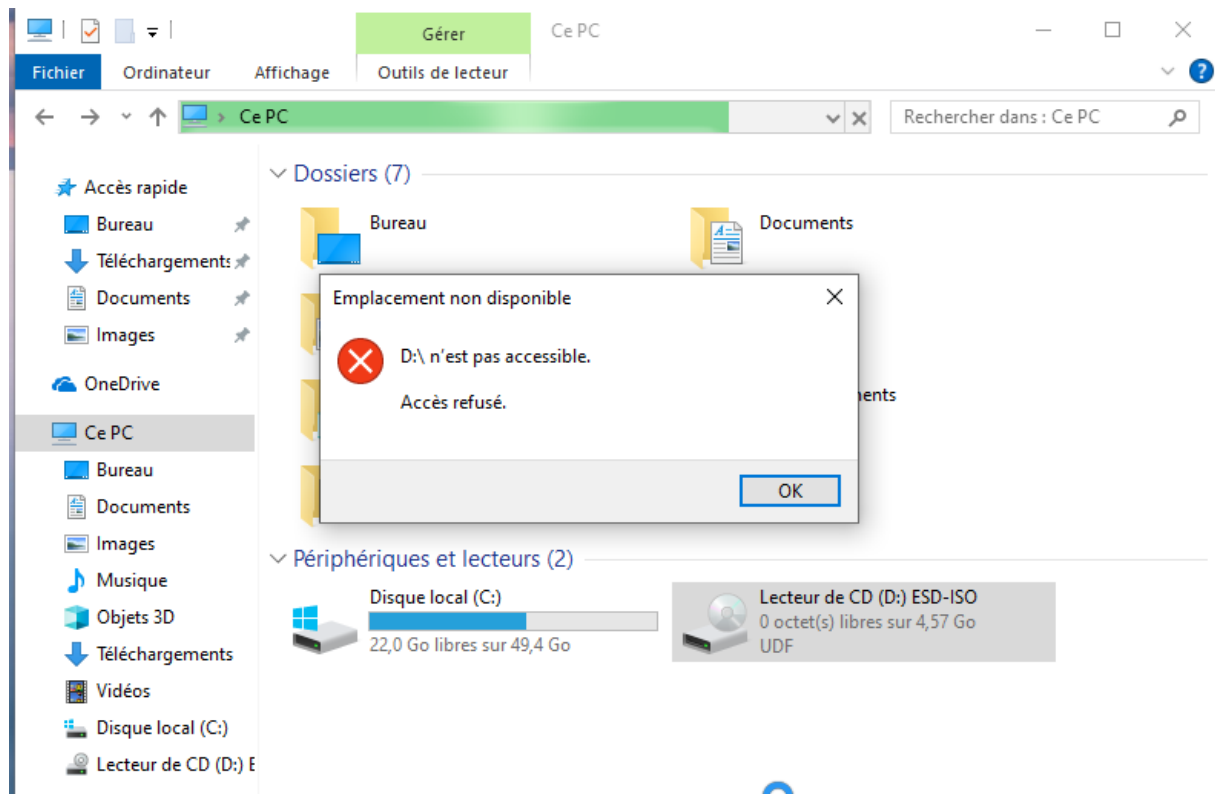




Cette liaison permet d'appliquer cette stratégie sur tout le domaine. • Tester la GPO : Sur un poste qui est dans le domaine, nous allons ouvrir une session d'un utilisateur dont le compte se situe dans l'OU "**DepartementIT**" :

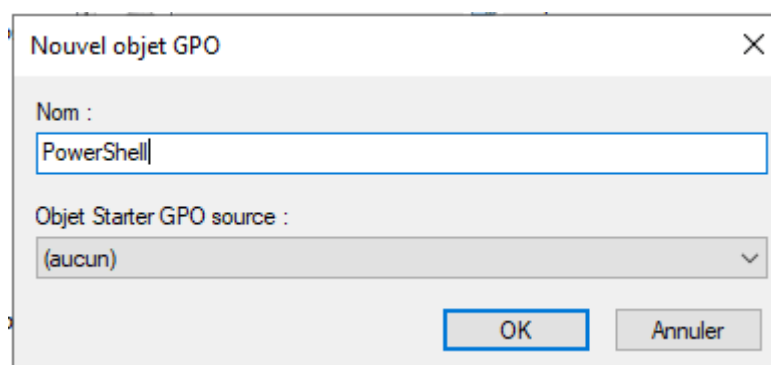
Une fois la session ouverte, on exécute la commande « gpupdate /force » pour forcer la mise à jour des stratégies de group.

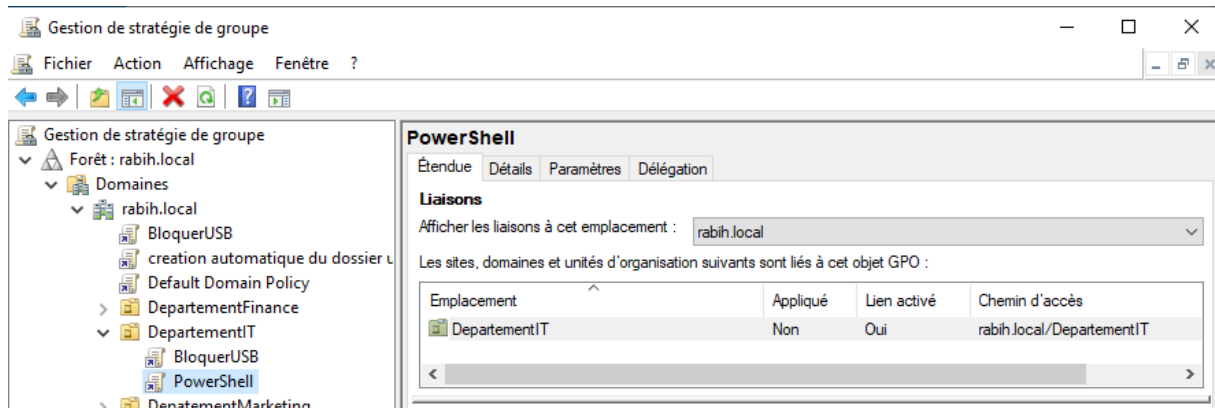




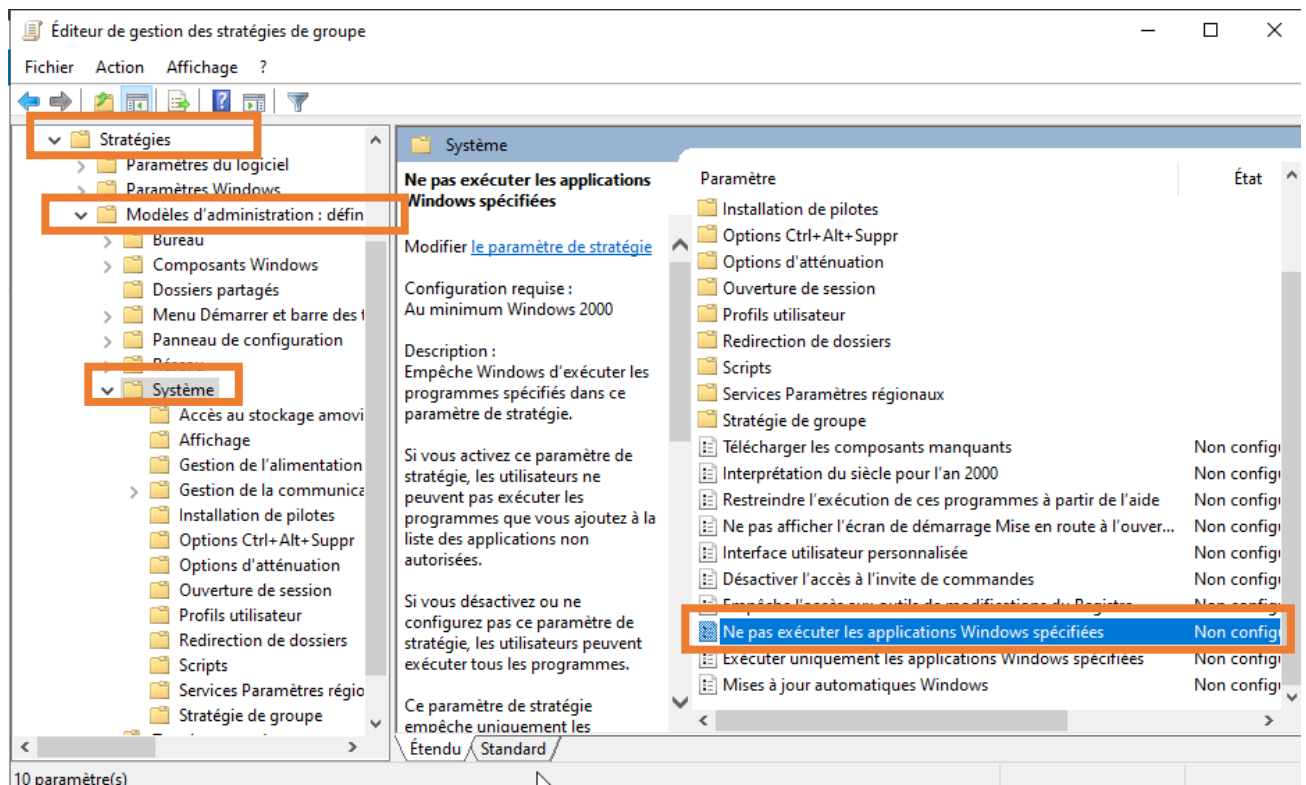
Bloquer PowerShell

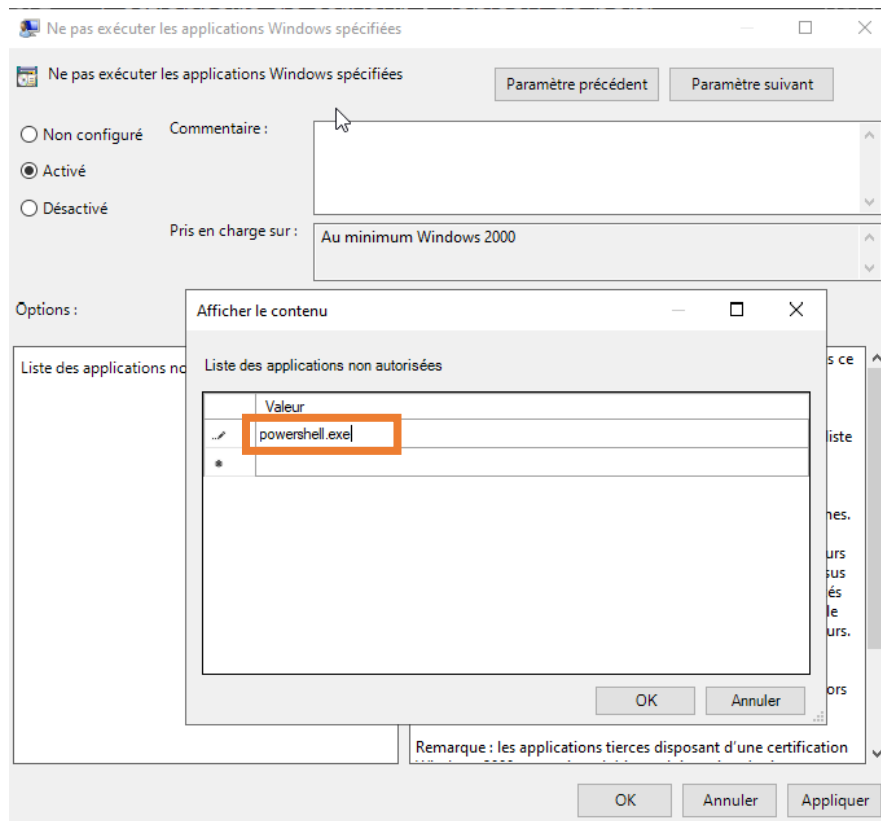
Dans cet exemple, on va créer une stratégie de groupe pour bloquer PowerShell sur les utilisateurs normaux.



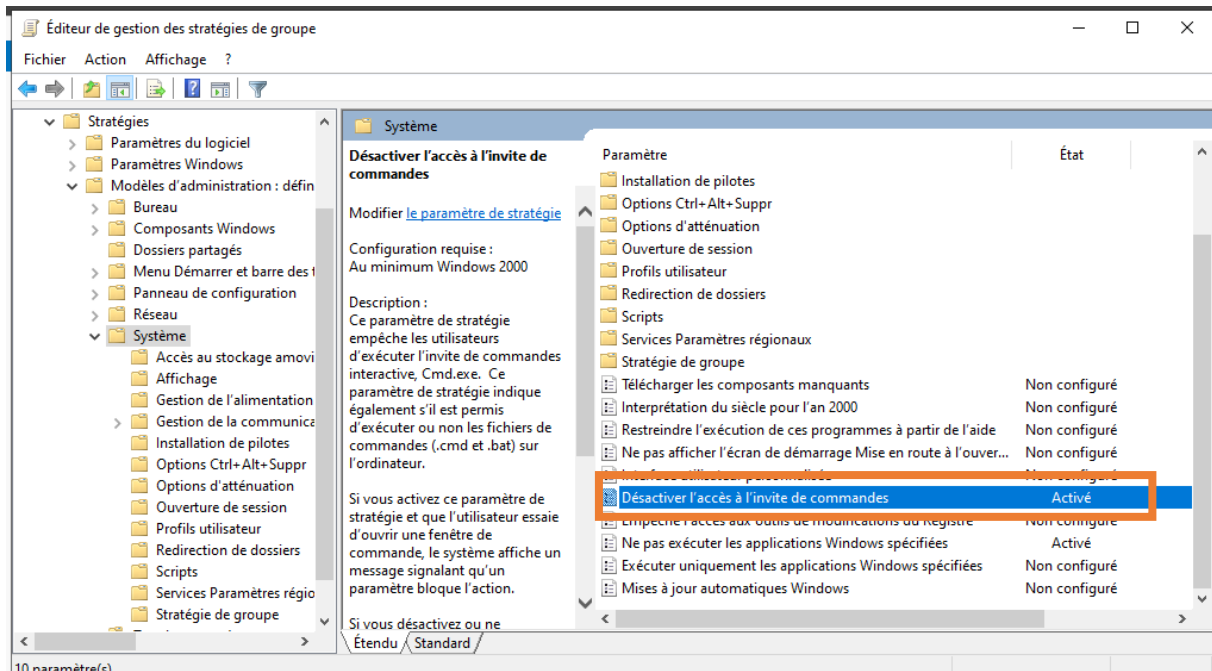


Pour appliquer cette stratégie Voici le chemin vers notre paramètre : **Configuration utilisateur** -> **Stratégies** -> **Modèles d'administration** -> **Système** > **Ne pas exécuter les applications Windows spécifiées**. Double-cliquez dessus pour activer et on ajoute l'application non autorisée, dans notre cas « **powershell.exe** ».

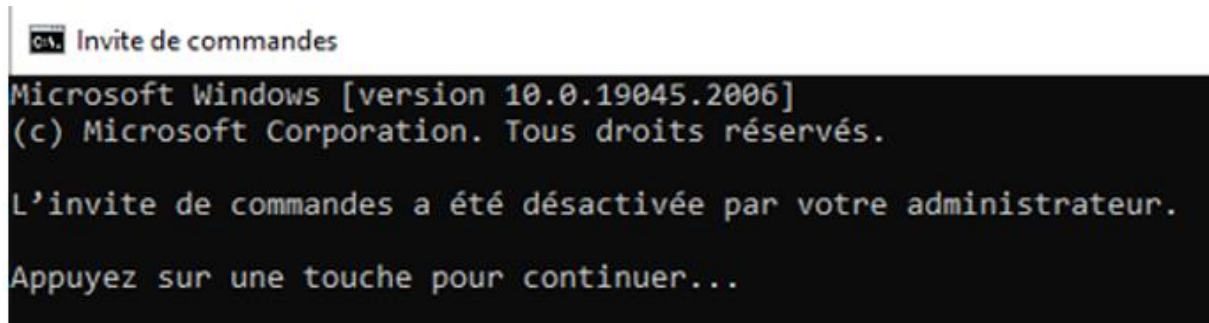




Aussi on peut désactiver l'invite de commande (cmd)

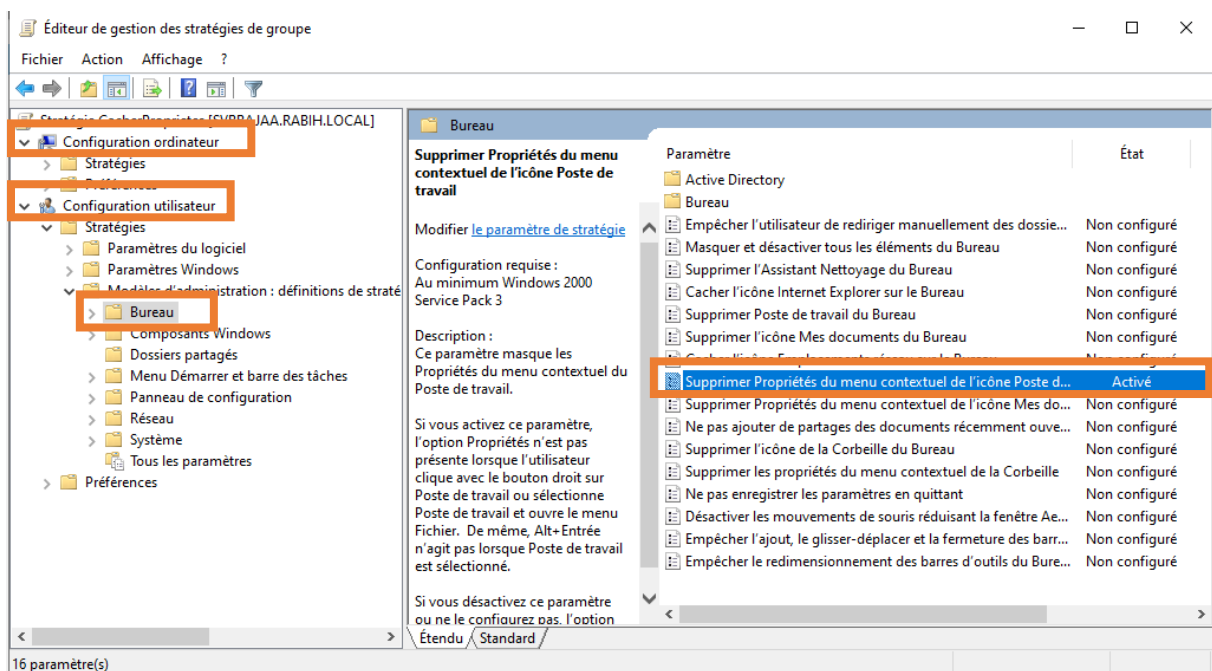
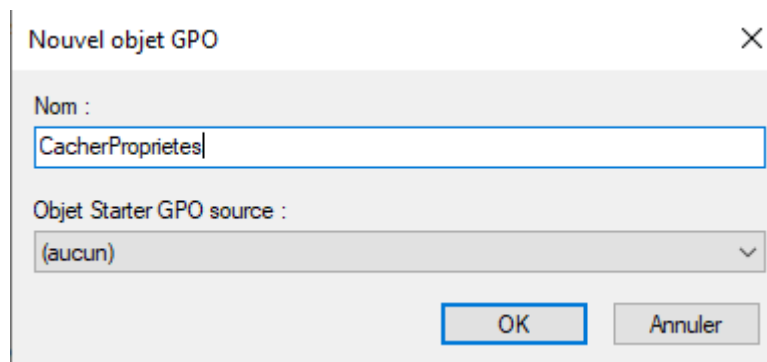


Résultat :

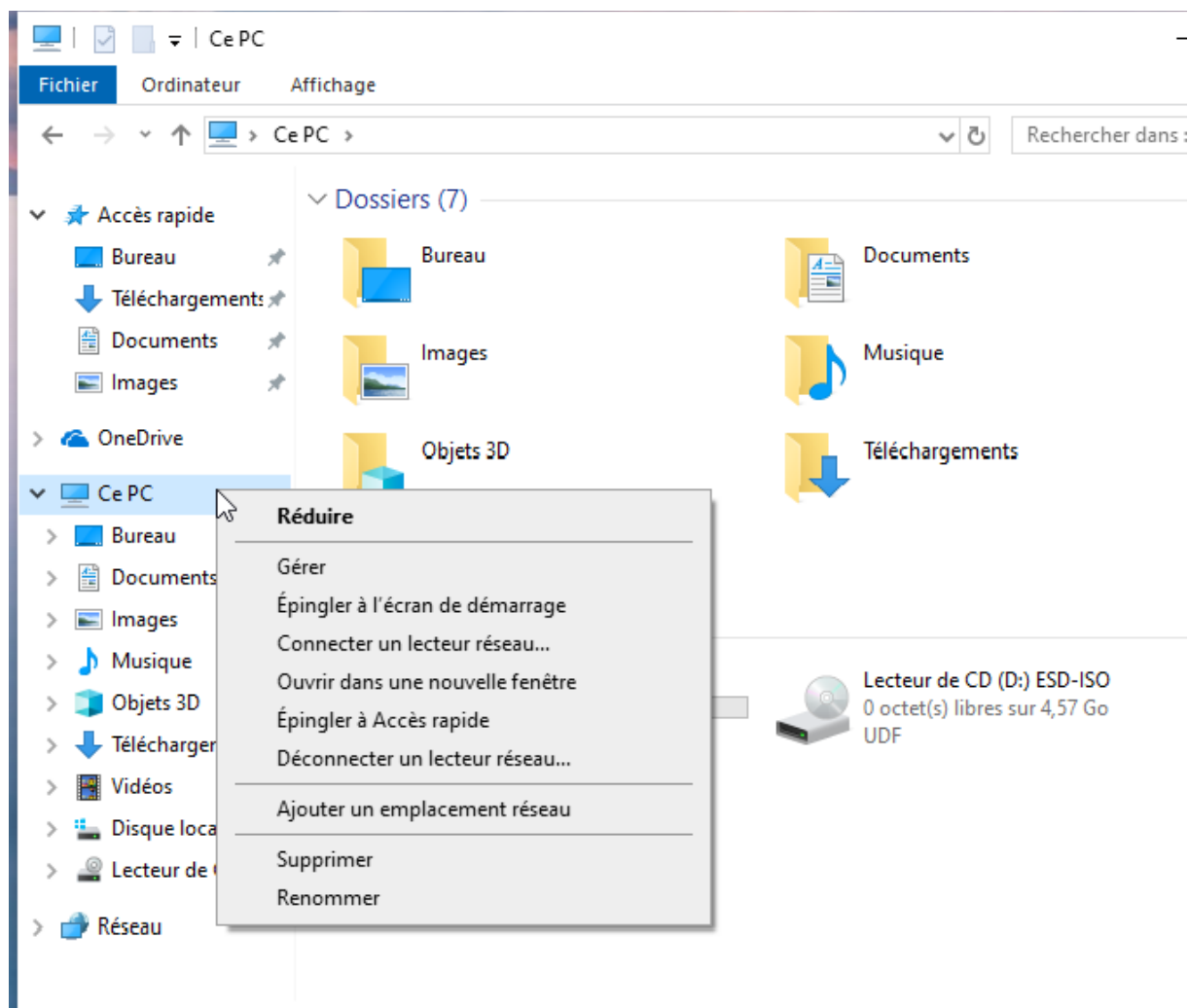


Cacher la propriété de l'ordinateur :

Les propriétés de l'ordinateur peuvent être cachées aux utilisateurs normaux pour des raisons de sécurité ou pour des raisons de politique d'entreprise. En cachant ces propriétés, l'administrateur système peut mieux contrôler les modifications apportées aux paramètres système importants, tels que les paramètres de sécurité ou de réseau, et éviter que les utilisateurs normaux ne les modifient accidentellement ou intentionnellement.



Sur un poste qui est dans le domaine, nous allons ouvrir une session d'un utilisateur dont le compte se situe dans l'OU "DepartementIT" : Une fois la session ouverte, on exécute la commande « gpupdate /force » pour forcer la mise à jour des stratégies de groupe.



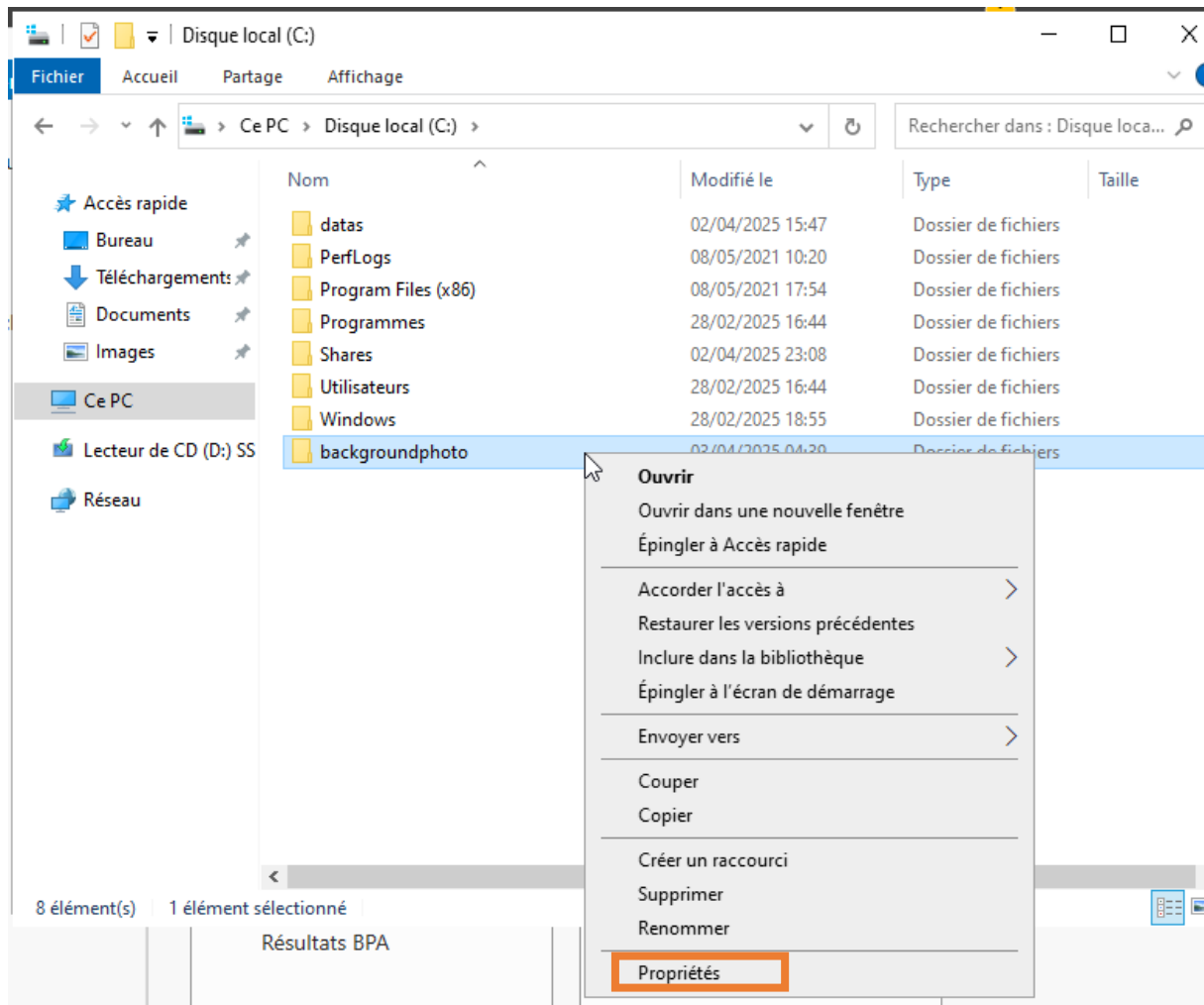
Changer le Background de bureau de tous les utilisateurs.

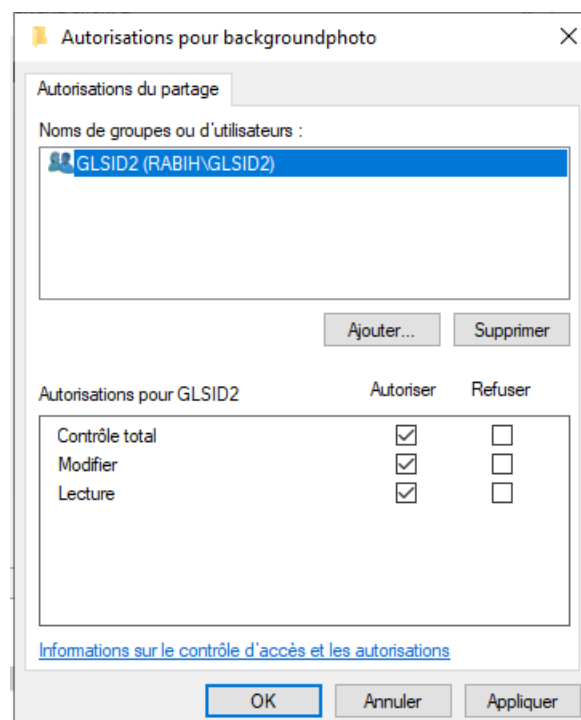
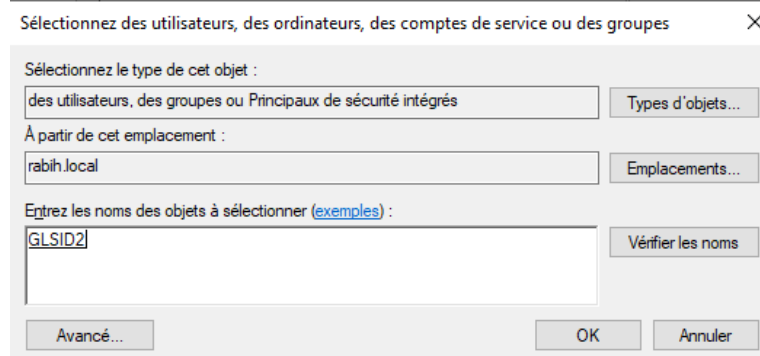
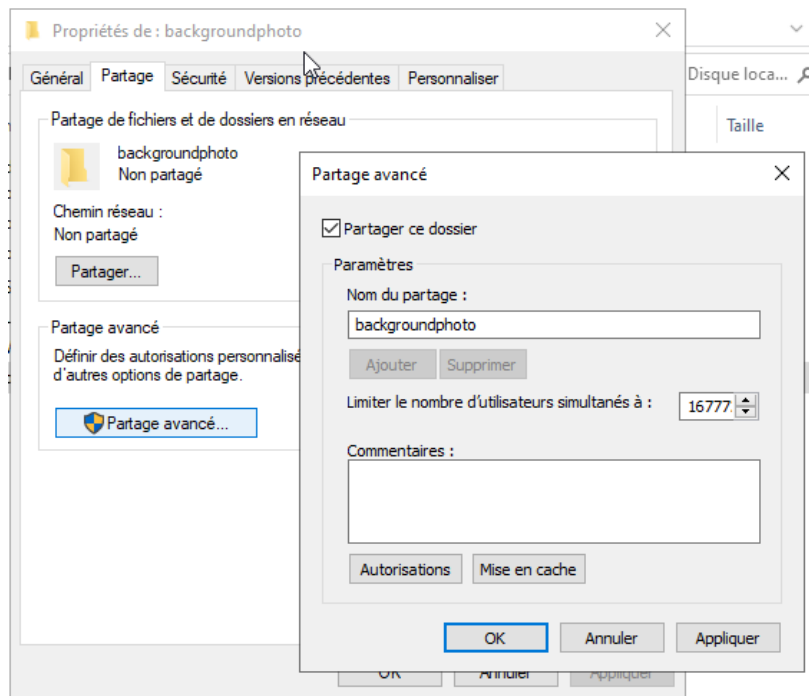
Pour changer le background de bureau de l'utilisateur il doit créer un dossier partager avec tous les utilisateurs qui contient cette image.

Premièrement on va voir comment créer un dossier partager :

Créer un dossier et modifier les propriétés de ce dossier : Faites un clic droit sur le dossier que vous venez de créer et sélectionnez "Propriétés". Dans l'onglet "Partage", cliquez sur le bouton "Partager" et choisissez les utilisateurs ou les groupes avec lesquels vous souhaitez partager le dossier.

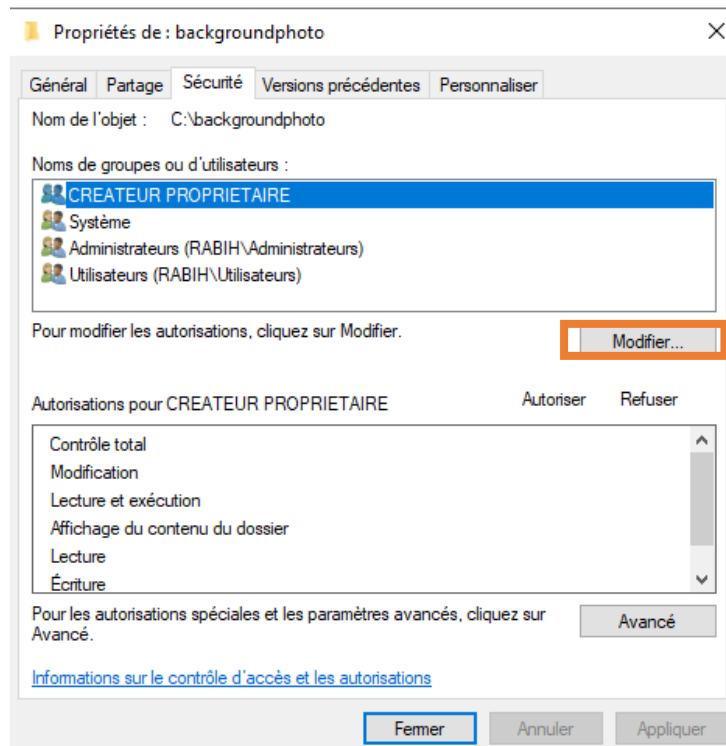
Configurez les autorisations de partage en spécifiant les autorisations d'accès pour les utilisateurs ou les groupes sélectionnés.



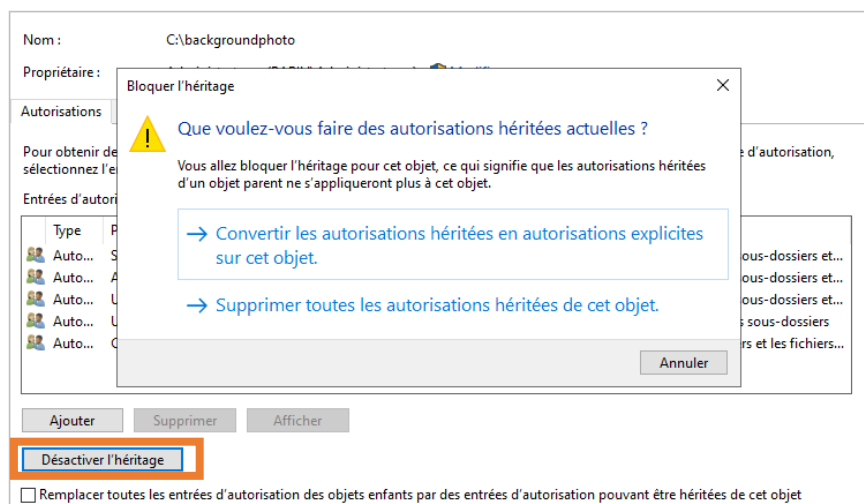


Et après on passe à la configuration des autorisations NTFS

Dans l'onglet "Sécurité", cliquez sur le bouton "Modifier" pour modifier les autorisations.



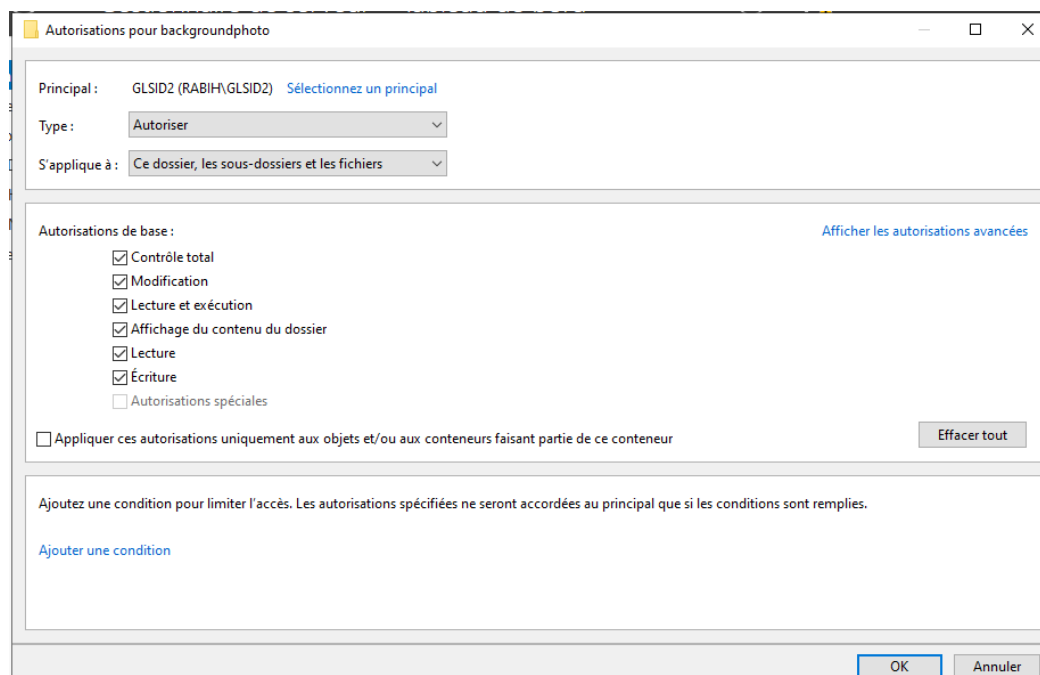
Désactiver l'héritage pour limiter les autorisations.



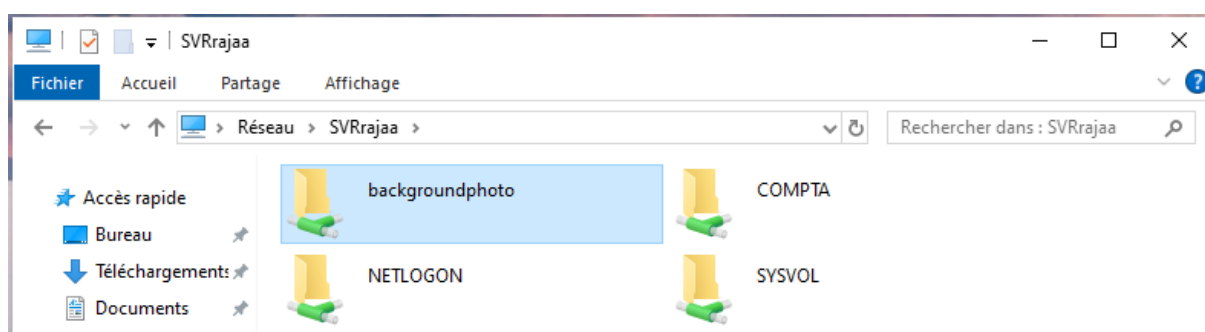
Cliquez sur "Ajouter" pour ajouter des utilisateurs ou des groupes.

Dans la fenêtre qui s'ouvre, entrez le nom d'utilisateur ou de groupe que vous souhaitez ajouter et cliquez sur "Vérifier les noms". Si le nom est correct, il sera souligné. Cliquez sur "OK" pour ajouter l'utilisateur ou le groupe. Configurez les autorisations pour l'utilisateur ou le groupe que vous venez d'ajouter. Vous pouvez spécifier des autorisations de lecture, d'écriture ou de

contrôle total pour chaque utilisateur ou groupe. Cliquez sur "Appliquer" pour enregistrer les modifications et fermez la fenêtre des propriétés.

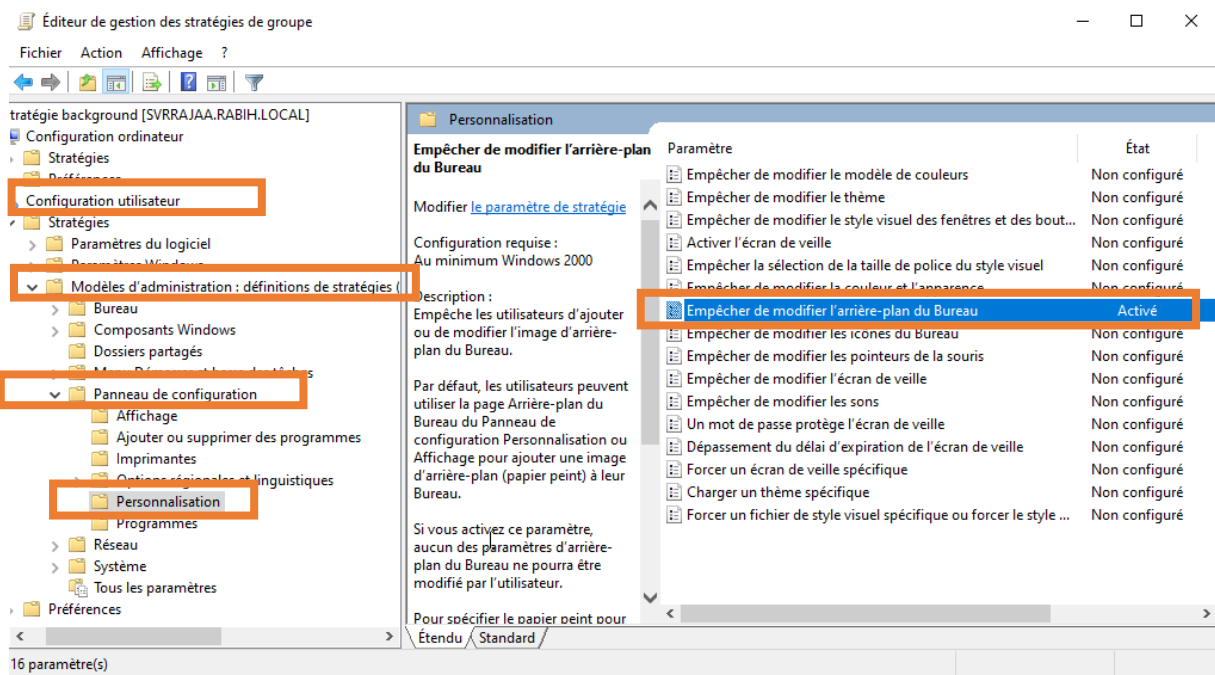


Cliquez sur "OK" pour enregistrer les modifications et fermez la fenêtre des propriétés. Le dossier partagé est maintenant créé et les utilisateurs ou les groupes sélectionnés peuvent y accéder en utilisant leur nom d'utilisateur et leur mot de passe. Alors pour voir le dossier partagé chez l'utilisateur, dans l'interface Exécuter on écrit le nom de serveur.



Alors maintenant on peut utiliser le dossier pour partager une image, et par GPO on peut mettre cette image comme fond écran commun entre les utilisateurs. Donc on crée une nouvelle stratégie et on configure ses paramètres :

1- Empêcher de modification l'arrière-plan du bureau



Naviguer vers "Configuration utilisateur" > "Stratégies" > "Modèles d'administration" > "Bureau" > "Bureau".

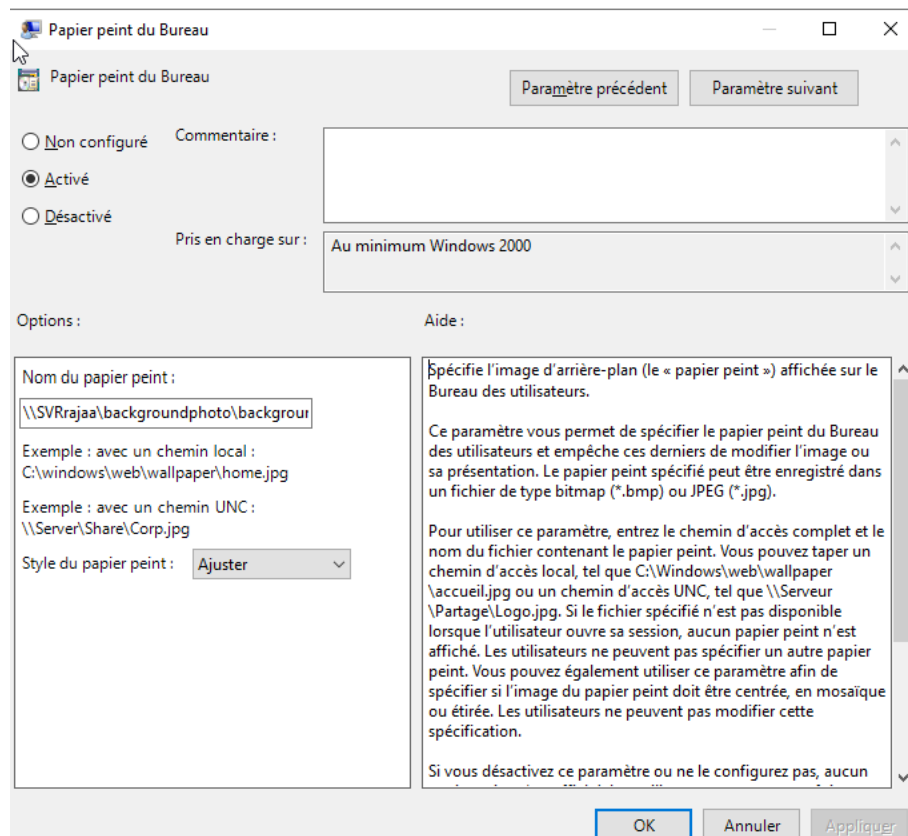
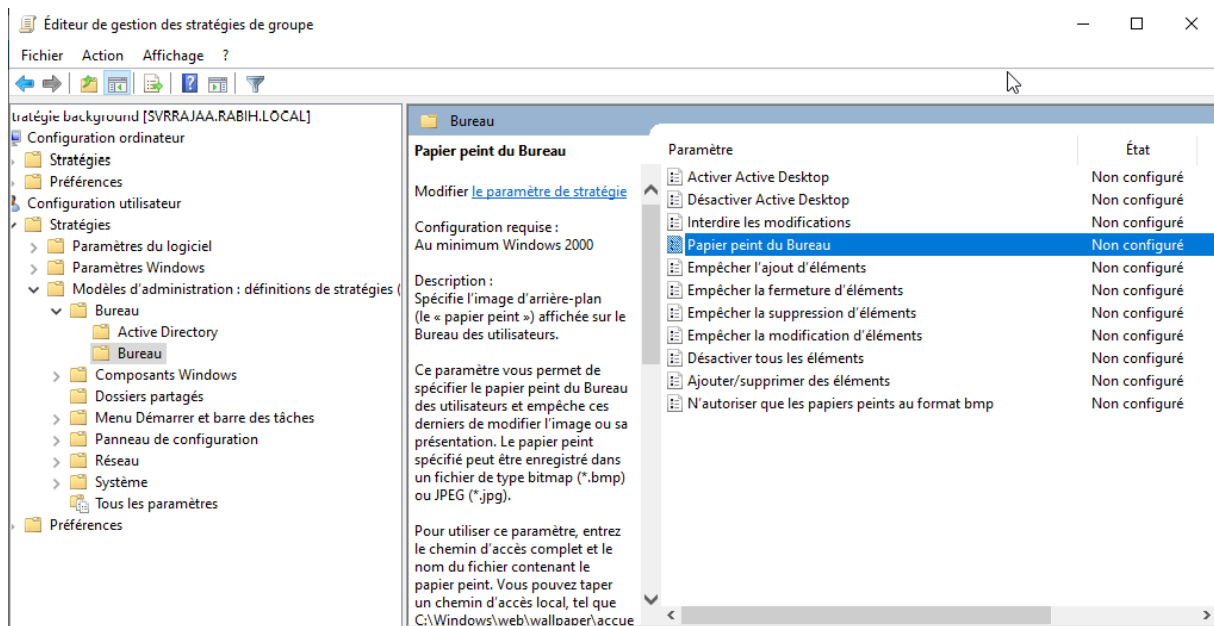
Double-cliquer sur "Fond d'écran du bureau" dans la fenêtre de droite pour ouvrir la fenêtre de propriétés.

Choisir l'option "Activé" pour activer la GPO.

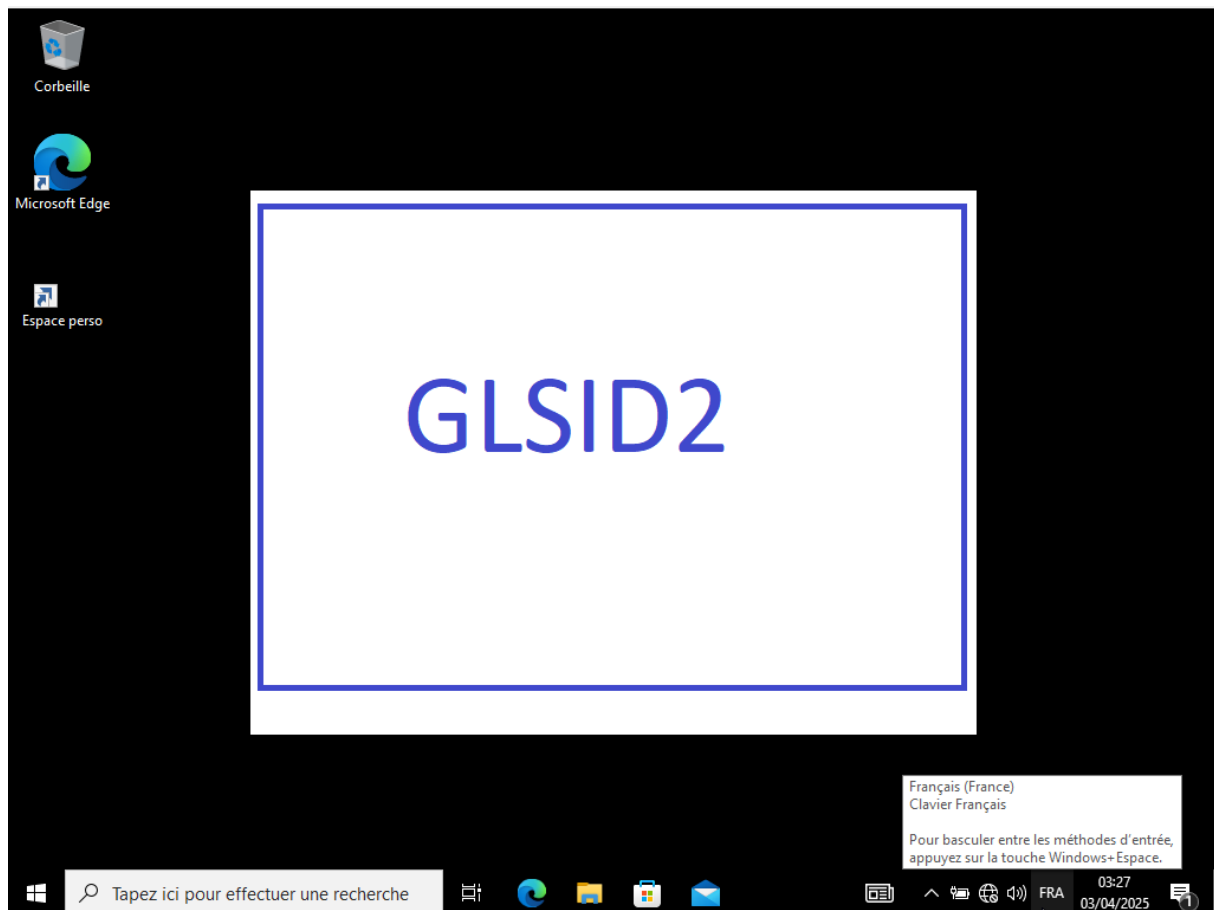
Indiquer le chemin d'accès du fichier d'image pour le fond d'écran en utilisant l'option "Chemin d'accès à l'image du papier peint".

Sélectionner l'option "Centrer" pour aligner l'image au centre de l'écran. Cliquer sur "Appliquer" et "OK" pour enregistrer les modifications.

Mettre à jour la stratégie de groupe en utilisant la commande "gpupdate /force" dans la boîte de dialogue Exécuter.

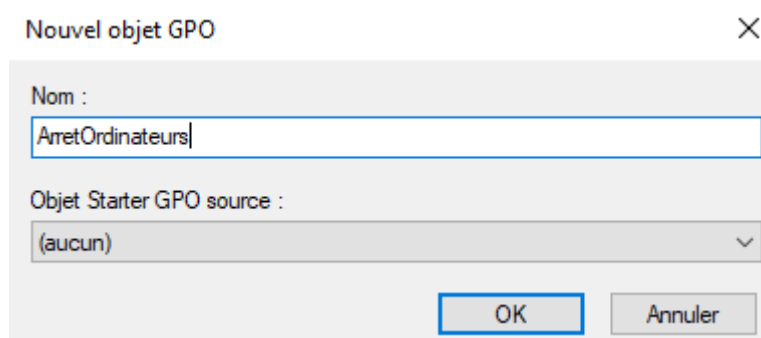


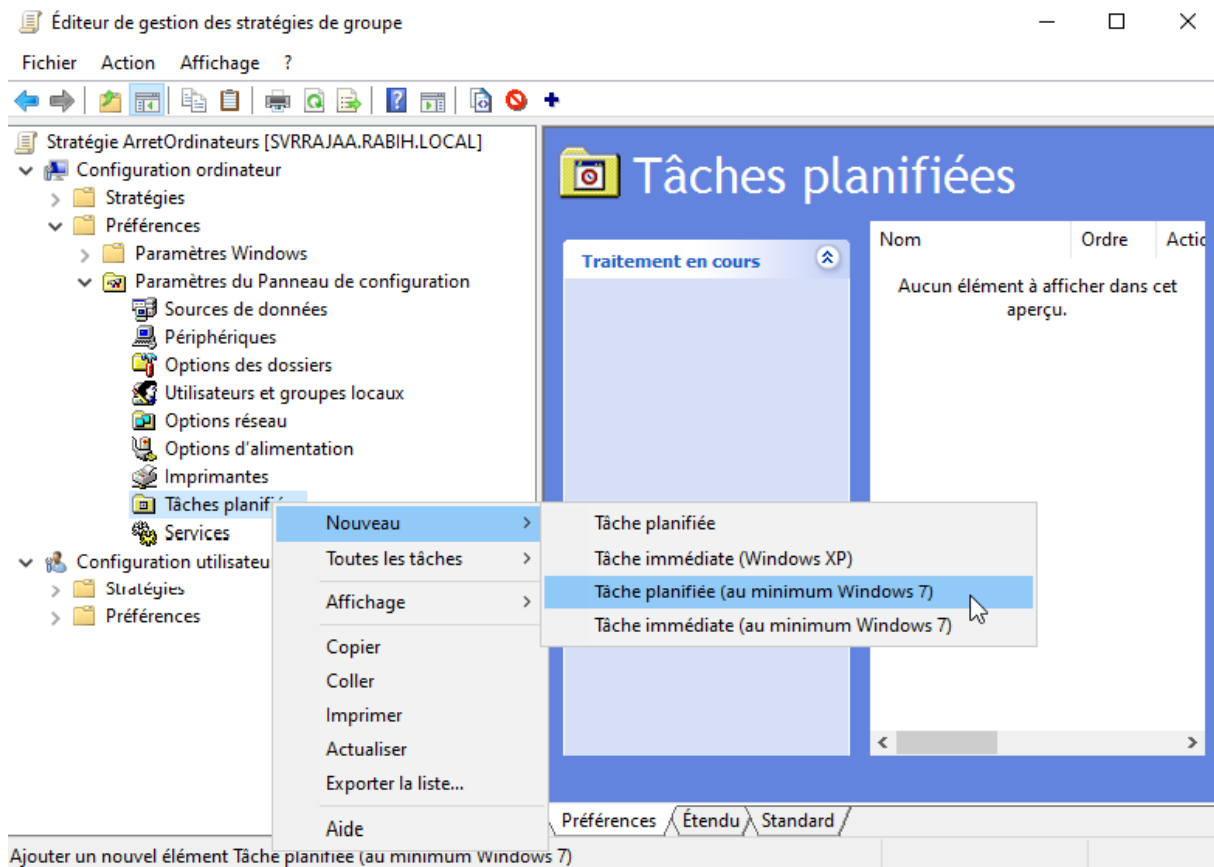
Une fois ces étapes effectuées, tous les utilisateurs du domaine verront le même fond d'écran lorsqu'ils se connecteront à leur session.



Planifier l'arrêt automatique des ordinateurs

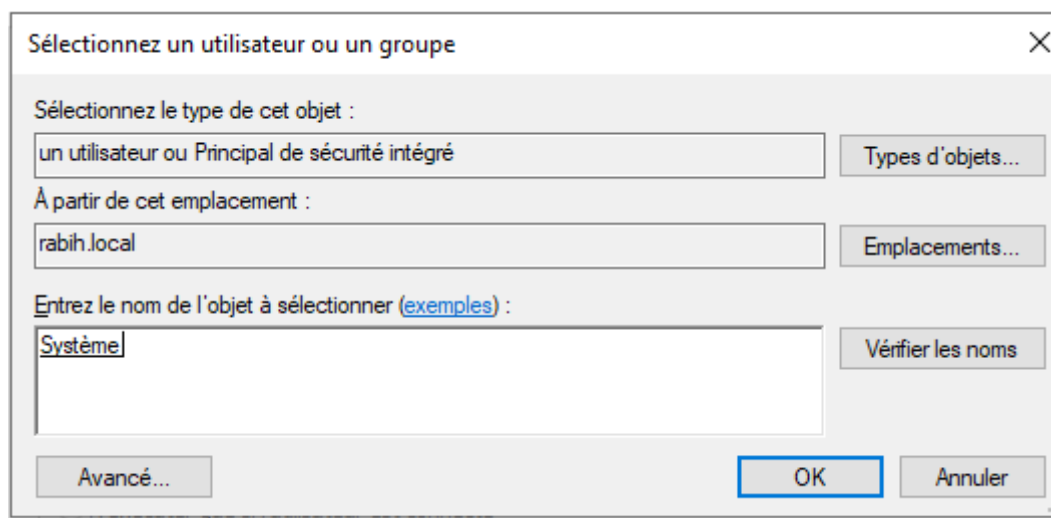
L'objectif de cette partie est de configurer un GPO qui permet de faire un arrêt automatique des ordinateurs d'une ou plusieurs unités d'organisation à partir d'une certaine date et heure et avec une certaine fréquence. Pour ce faire, nous allons procéder comme les figures ci-dessous le montrent.





Une fenêtre contenant plusieurs onglets est affichée

- Sur l'onglet Général, nous choisissons l'action Mettre à jour.
- Par la suite, nous devons donner un nom significatif à cette tâche (je vais garder le même nom que celui que j'ai donné à la GPO)
- Lors de l'exécution de la tâche utiliser le compte utilisateur suivant



Nouvelles propriétés de Tâche (au minimum Windows 7)

Général Déclencheurs Actions Conditions Paramètres Commun

Action : Mettre à jour

Nom : ArretOrdinateurs

Auteur : RABIH\Administrateur

Description :

Options de sécurité

Lors de l'exécution de la tâche, utilisez le compte d'utilisateur suivant :

AUTORITE NT\System

Utilisateur ou groupe...

☒ N'exécuter que si l'utilisateur est connecté

☐ Exécuter même si l'utilisateur n'est pas connecté

☐ Ne pas stocker le mot de passe. La tâche n'aura accès qu'aux ressources locales.

☐ Exécuter avec les privilèges les plus élevés

☐ Masquer

Configurer pour : Windows Vista™ ou Windows Server™ 2008

OK Annuler Appliquer Aide

- Ensuite, Nous allons cliquer sur l'onglet déclencheur puis Nouveau
- Le but est de préciser la fréquence, la date et l'heure de l'exécution de cette tâche.

Nouvelles propriétés de Tâche (au minimum Windows 7)

Général Déclencheurs Actions Conditions Paramètres Commun

Lorsque vous créez une tâche, vous pouvez spécifier les conditions qui déclencheront la tâche.

Déclencheur	Détails	État
-------------	---------	------

Nouveau... Modifier... Supprimer

OK Annuler Appliquer Aide

Nouveau déclencheur ✕

Commencer la tâche : À l'heure programmée ▼

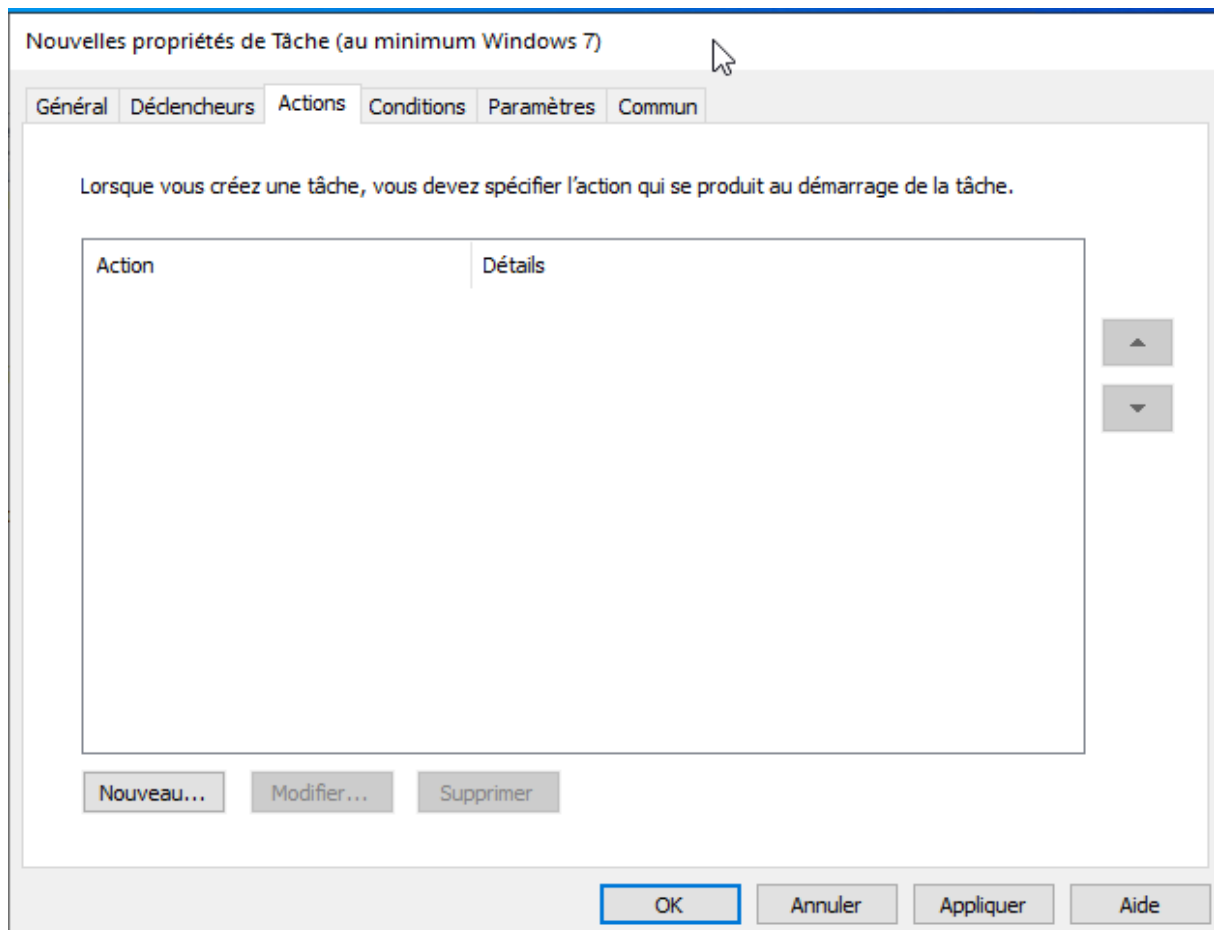
Paramètres

☐ Une fois Démarrage : 10/04/2025 ▼ 21:00:32 ▼ ☐ Synch. fuseaux horaires
☒ Tous les jours
☐ Hebdomadaire Répéter toutes 1 jour
☐ Tous les mois

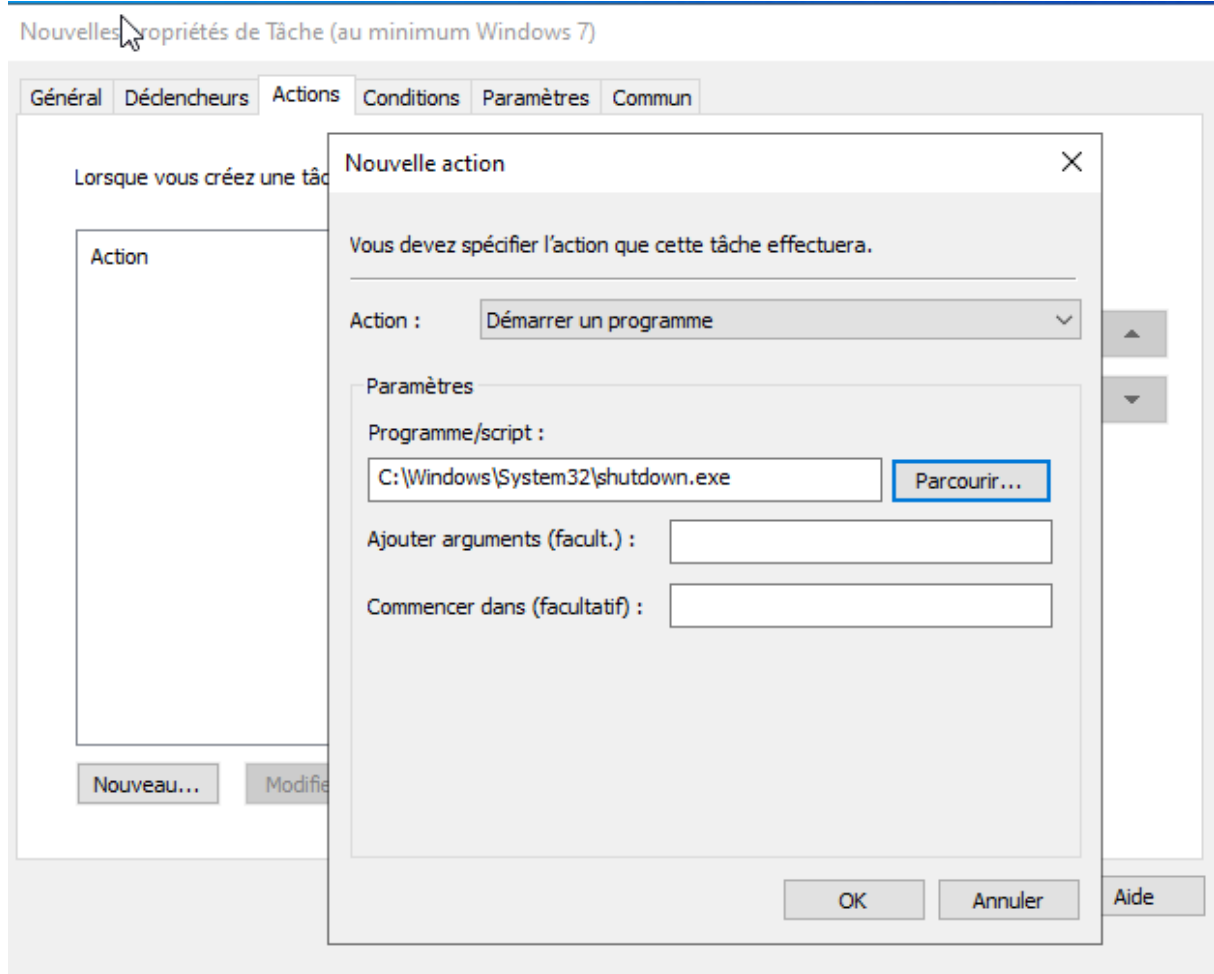
Paramètres avancés

☐ Report maximal de la tâche (aléatoire) : 1 heure ▼
☐ Répéter la tâche toutes les : 1 heure ▼ pour une durée de : 1 jour ▼
☐ Arrêter toutes les tâches à l'issue de la durée de répétition
☐ Arrêter la tâche si elle s'exécute plus de : 3 jours ▼
☐ Expiration : 03/04/2025 ▼ 05:26:26 ▼ ☐ Synch. fuseaux horaires
☒ Activée

- Nous cliquons sur l'onglet Actions puis Nouveau pour préciser qu'est-ce que nous devons faire à cette heure exactement



- En cliquant sur parcourir, nous allons chercher le programme shutdown.exe qui est inclut dans Windows et qui se trouve dans le chemin C:\Windows\System32\shutdown.exe



Après avoir sélectionner le programme/script à exécuter, nous pouvons spécifier plusieurs arguments (facultatifs).

Voici un tableau récapitulatif des arguments facultatifs (ou "*options*") que l'on peut utiliser avec la commande shutdown.exe, comme on le voit dans l'image. Ces arguments permettent de configurer le comportement de l'arrêt ou du redémarrage du système.

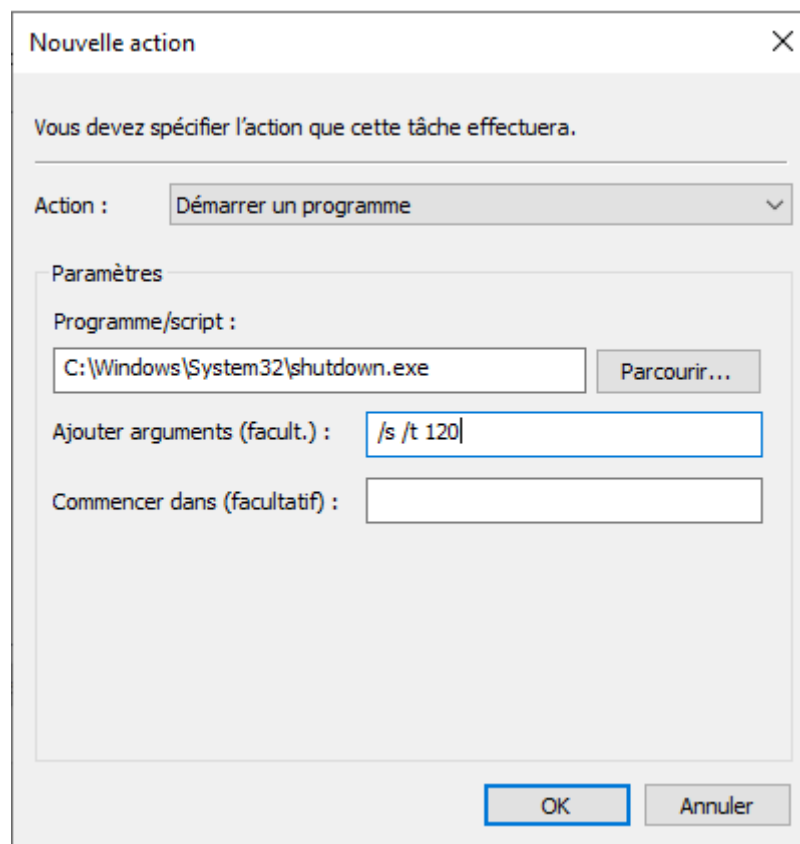
Argument	Signification
/s	Arrête (shutdown) l'ordinateur.
/r	Redémarre l'ordinateur après l'arrêt.
/t [secondes]	Définit un délai avant l'arrêt/redémarrage (en secondes). Par défaut : 30s.
/f	Force la fermeture des applications en cours sans avertissement.
/l	Ferme la session de l'utilisateur courant (ne peut pas être utilisé avec /s ou /r).
/a	Annule un arrêt ou redémarrage planifié (à utiliser avant que le délai expire).
/h	Met l'ordinateur en veille prolongée (hibernation).

/hybrid Arrête le système et prépare un démarrage rapide (Fast Startup).

Exemple de combinaison :

shutdown.exe /s /f /t 120

- /s : Arrêt du PC
- /f : Ferme les applications ouvertes de force
- /t 120 : Délai de 120 secondes avant l'arrêt



Nouvelles propriétés de Tâche (au minimum Windows 7)

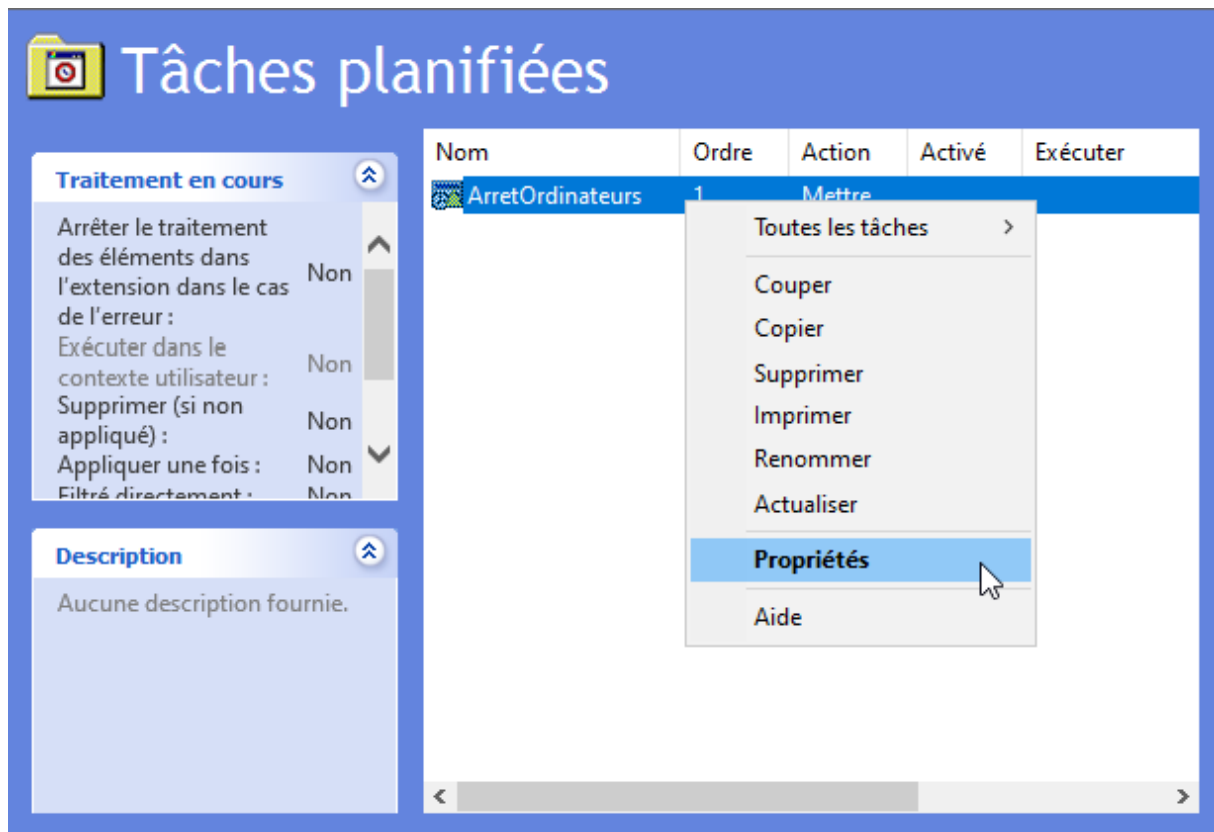
The screenshot shows the 'Nouvelles propriétés de Tâche' (New Task Properties) dialog box, specifically the 'Actions' tab. The dialog has a title bar and several tabs: 'Général', 'Déclencheurs', 'Actions', 'Conditions', 'Paramètres', and 'Commun'. The 'Actions' tab is active, displaying a list of actions. The first action is 'Démarrer un programme' (Start a program), with its details set to 'C:\Windows\System32\shutdown.exe /s /t 120'. To the right of the list are up and down arrow buttons. Below the list is a horizontal scrollbar. At the bottom of the list area are three buttons: 'Nouveau...' (New...), 'Modifier...' (Modify...), and 'Supprimer' (Remove). At the bottom of the dialog are four buttons: 'OK', 'Annuler' (Cancel), 'Appliquer' (Apply), and 'Aide' (Help). The 'OK' button is highlighted with a blue border.

Action	Détails
Démarrer un programme	C:\Windows\System32\shutdown.exe /s /t 120

Nouveau... Modifier... Supprimer

OK Annuler Appliquer Aide


Nous allons cliquer sur appliquer puis Ok



- Après, nous allons cliquer sur Propriétés à nouveau et cliquer sur le radio bouton exécuter même si l'utilisateur n'est pas connecté (parce que cette option était désactivée la dernière fois)
- En plus, nous devons ressaisir le compte utilisateur : NT AUTHORITY\SYSTEM

Propriétés de : ArrêtOrdinateurs

Général Déclencheurs Actions Conditions Paramètres Commun


 Action : Mettre à jour

Nom : ArrêtOrdinateurs

Auteur : RABIH\Administrateur

Description :

Options de sécurité

Lors de l'exécution de la tâche, utilisez le compte d'utilisateur suivant :

 AUTORITE NT\System

 Utilisateur ou groupe...

☐ N'exécuter que si l'utilisateur est connecté

☒ Exécuter même si l'utilisateur n'est pas connecté

☒ Ne pas stocker le mot de passe. La tâche n'aura accès qu'aux ressources locales.

☐ Exécuter avec les privilèges les plus élevés

☐ Masquer

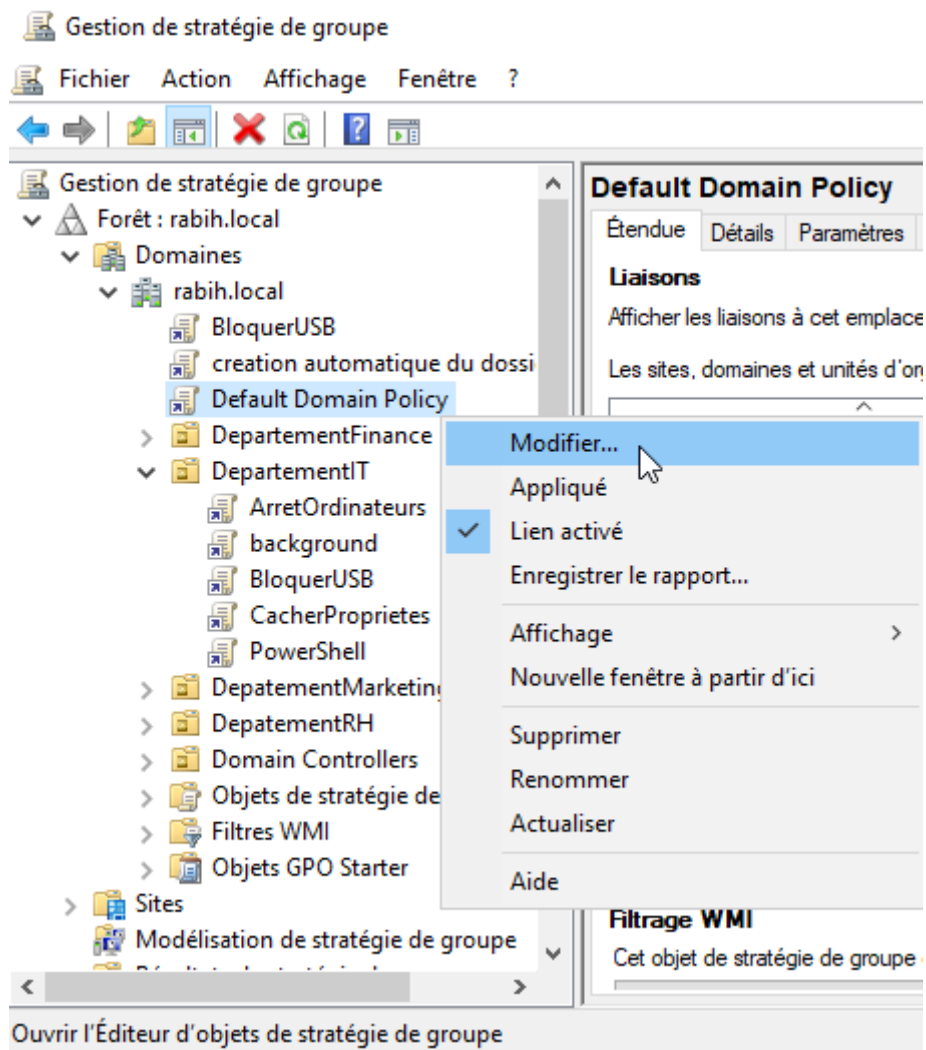
Configurer pour : Windows Vista™ ou Windows Server™ 2008

OK Annuler Appliquer Aide

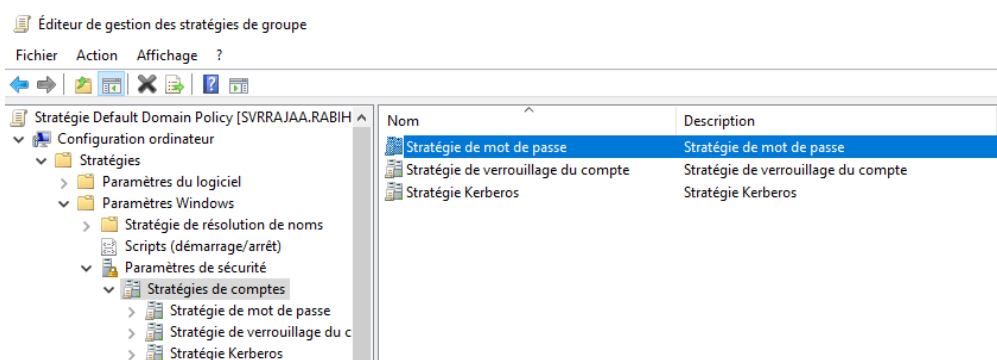
Pour tester le fonctionnement de cette gpo, nous devons se connecter avec la machine cliente et attendre jusqu'à ce que l'heure que vous avez précisé est arrivée pour voir que la machine

Configurer les stratégies de mots de passe









Toujours en suivant la même démarche, nous allons accéder au menu outils puis gestion de stratégie de groupe mais cette fois-ci nous allons modifier le gpo par défaut du domaine : Default Domaine Policy



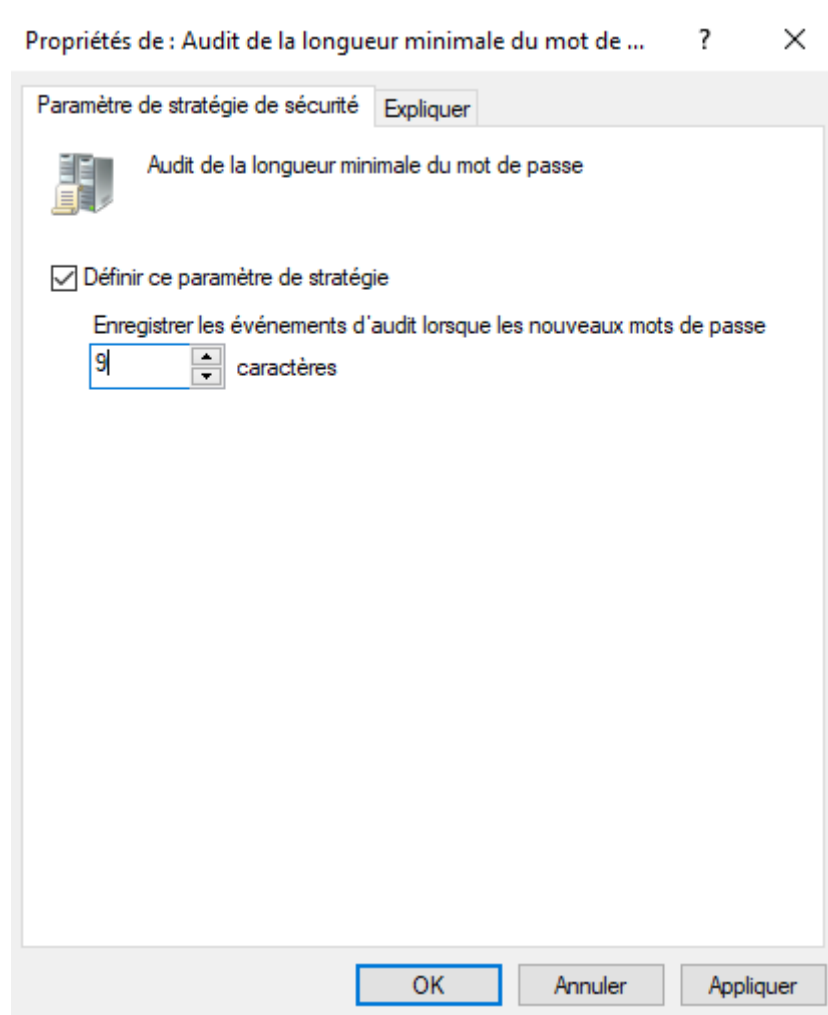
Configuration ordinateur -> Paramètres de Windows -> Paramètres de sécurité -> stratégie de mot de passe



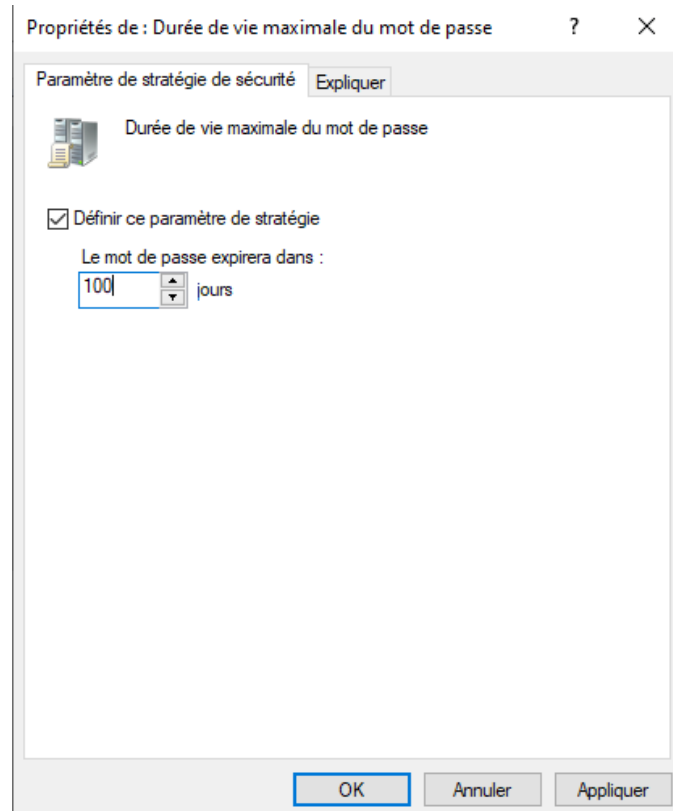
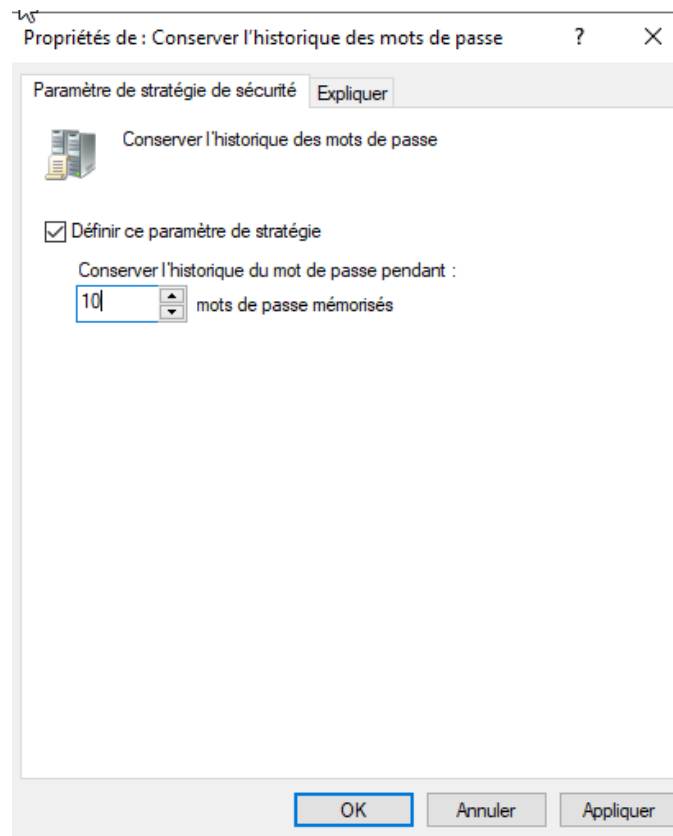
Lorsque nous cliquons sur la stratégie de mot de passe, plusieurs options sont disponibles

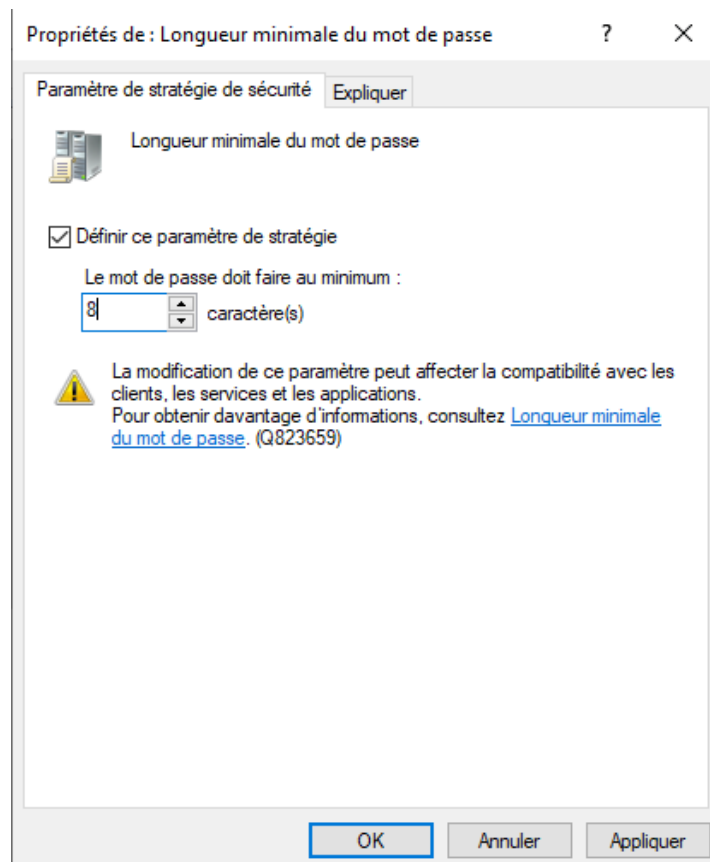
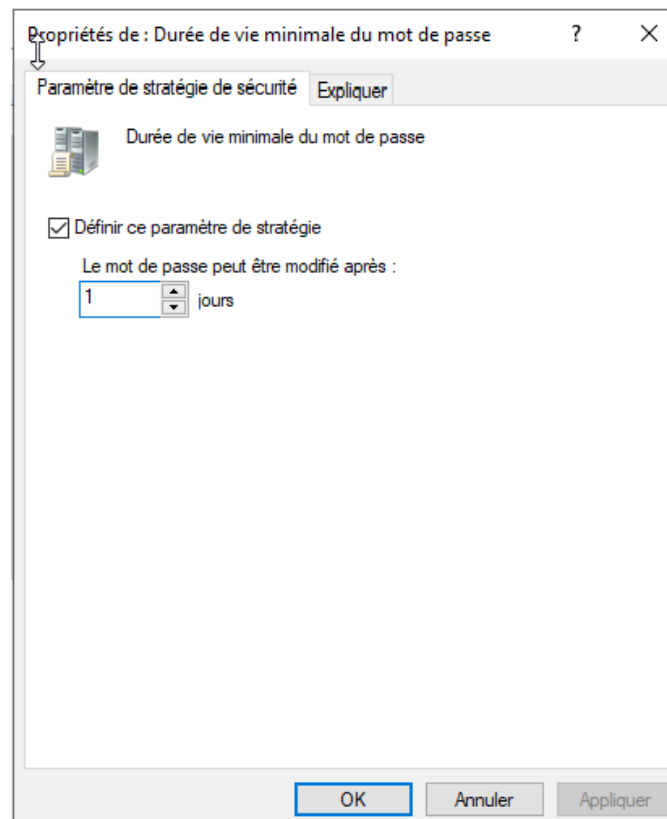
Stratégie	Paramètres de stratégie
 Assouplir les limites de longueur minimale du mot de passe	Non défini
 Audit de la longueur minimale du mot de passe	Non défini
 Conserver l'historique des mots de passe	24 mots de passe mémorisés
 Durée de vie maximale du mot de passe	42 jours
 Durée de vie minimale du mot de passe	1 jours
 Enregistrer les mots de passe en utilisant un chiffrement rév...	Désactivé
 Le mot de passe doit respecter des exigences de complexité	Activé
 Longueur minimale du mot de passe	7 caractère(s)

Audit de la longueur Minimal du mot de passe



Conserver l'historique des mots de passe





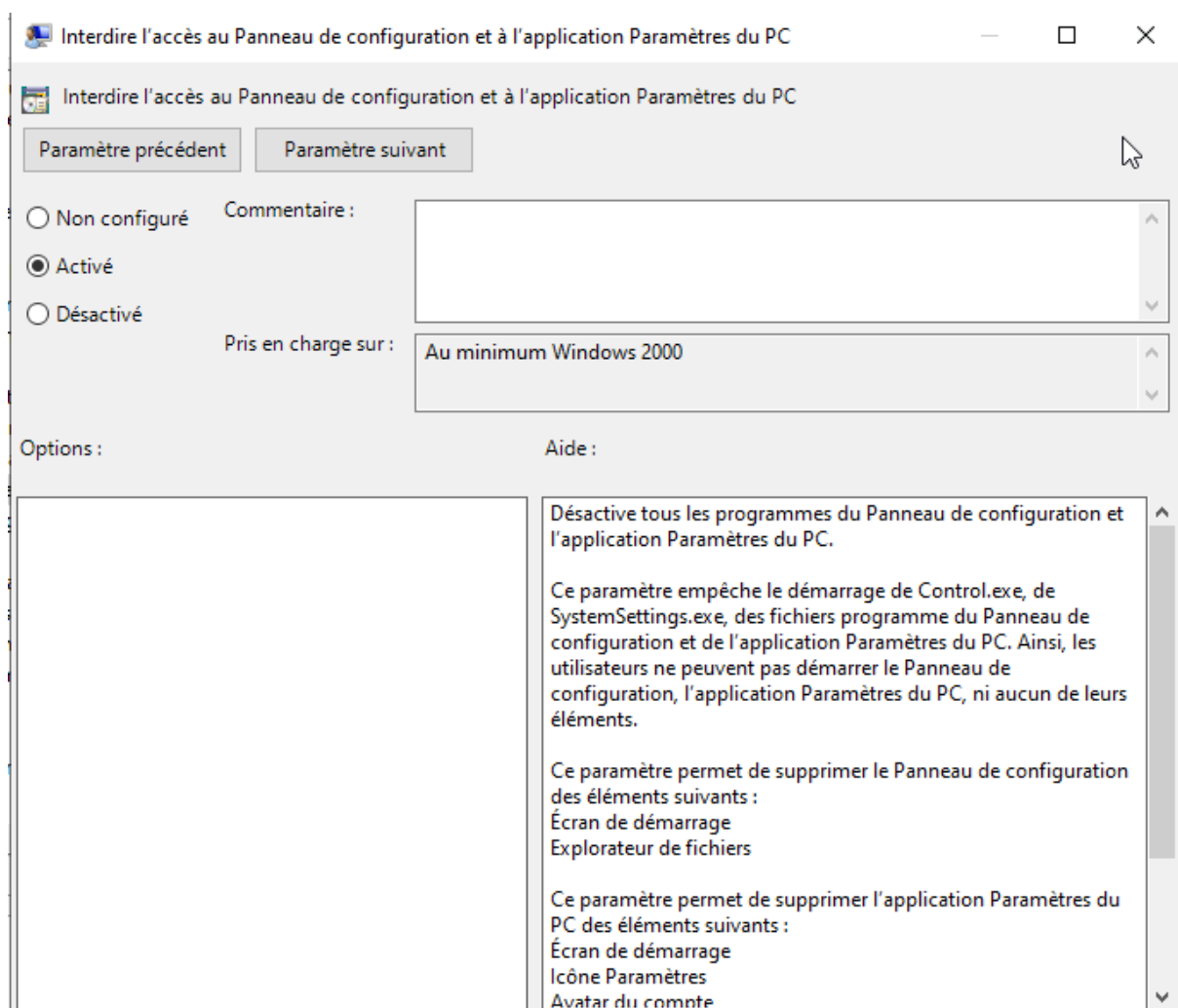
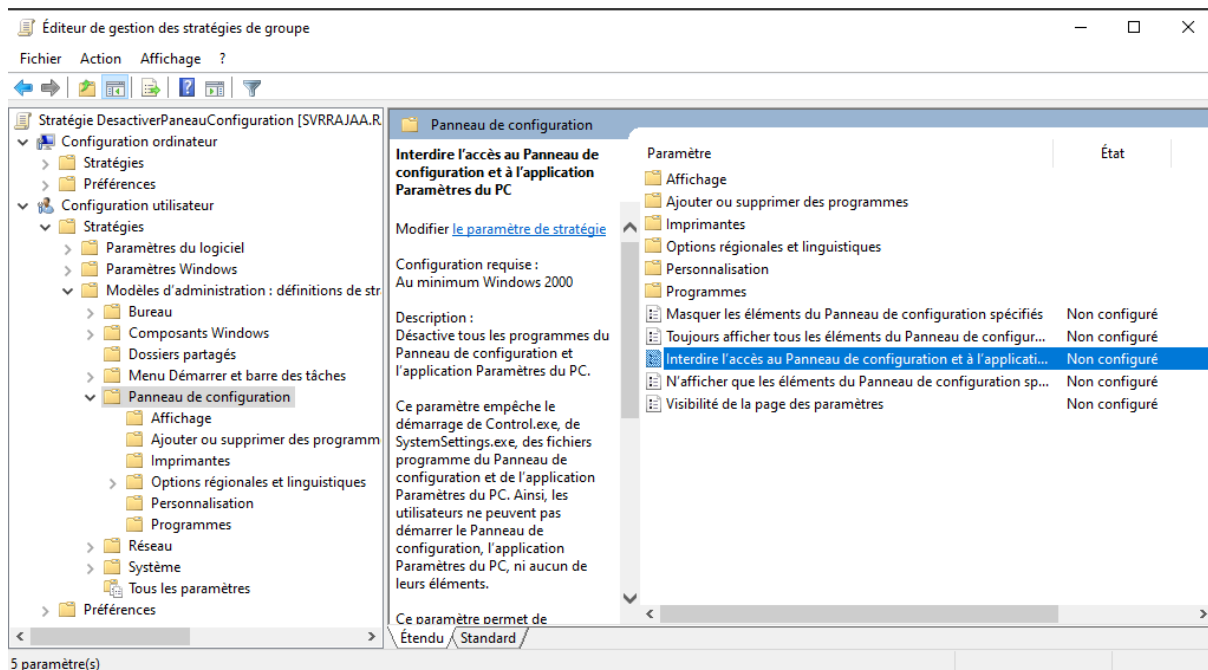
Pour vérifier l'application de ces stratégies, nous allons vers **outils-> Utilisateurs et ordinateurs Active Directory** Nous allons vers le département IT. Nous allons essayer de

modifier le mot de passe de l'utilisateur Sara par 12345 sachant que nous avons exigé dans la stratégie que la longueur minimale du mot de passe ne doit pas être inférieure ou égale à 9 caractères

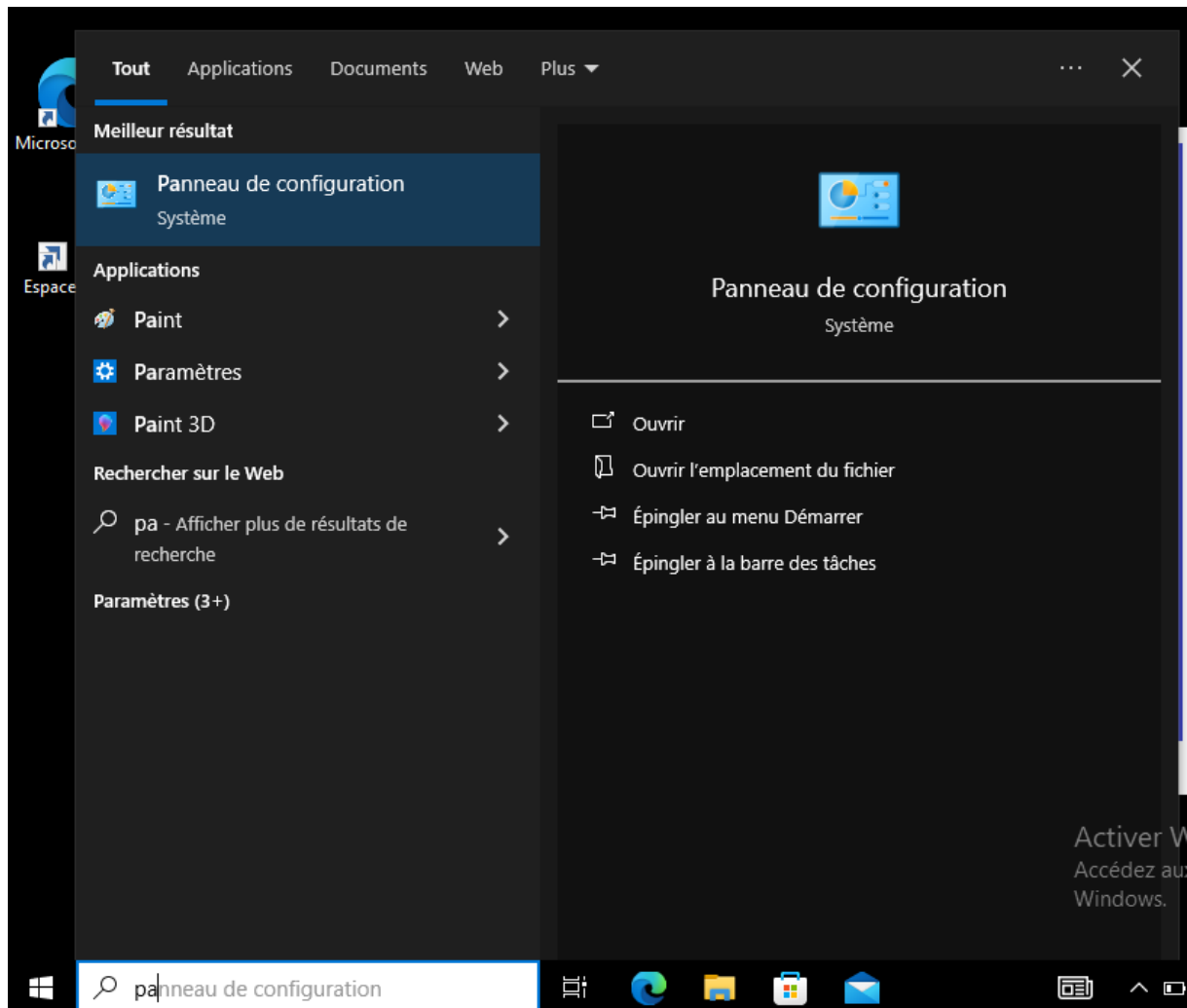
Lorsque nous cliquons sur OK, nous remarquons qu'un message d'erreur est affiché indiquant que le mot de passe que nous avons saisi ne respecte pas les critères de la gpo

Désactivation du Panneau de configuration

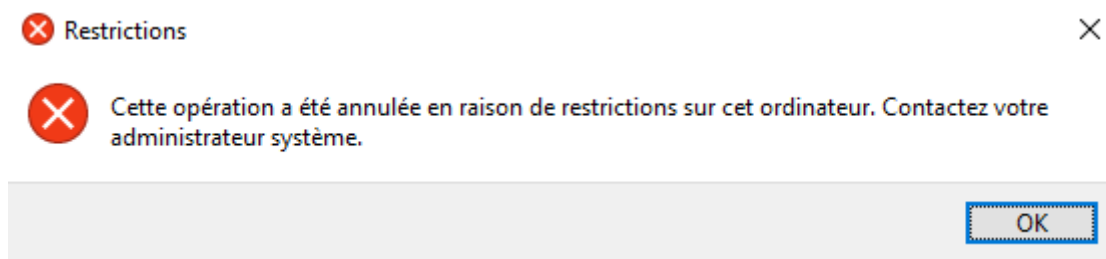
En suivant le même principe, nous allons créer une GPO pour désactiver l'accès au panneau de configuration par les utilisateurs de l'unité d'organisation « DépartementIT »



Pour vérifier, nous allons se connecter à la machine cliente et essayer d'accéder au panneau de configuration



Comme vous pouvez voyer, l'accès au panneau de configuration pour les utilisateurs de Users est devenu impossible grâce à la gpo que nous avons appliquée.



Conclusion

La mise en œuvre des stratégies de groupe à travers les GPO constitue une solution puissante pour la gestion centralisée de la sécurité et de l'environnement de travail dans un réseau d'entreprise. Grâce à l'application des différentes stratégies développées dans ce rapport, l'administrateur réseau peut réduire les risques de sécurité, assurer la conformité des postes, et simplifier la gestion quotidienne. Ces mesures, bien que techniques, s'inscrivent dans une démarche globale de gouvernance et de maîtrise du système d'information.