Stratégie de groupe
(GPO : Group Policy Objects)

Dernière mise à jour : 04/06/2024

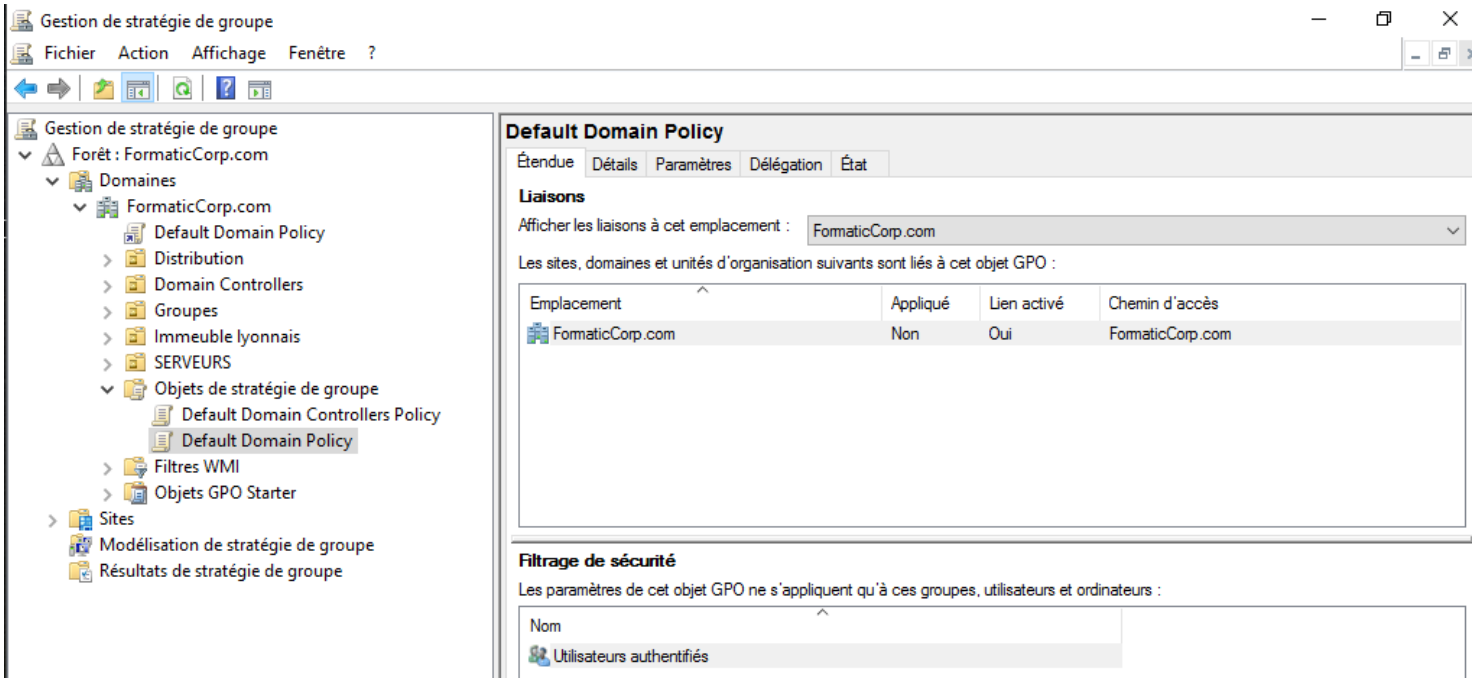
Table des matières

I. Paramètres de sécurité

Nous avons maintenant un annuaire Active Directory, composé de différents objets, dont des utilisateurs, des ordinateurs ou encore des groupes. A partir de tout cela, on pourra finalement mettre en œuvre la fonctionnalité la plus intéressante offerte par Active Directory en créant un nouveau type d'objet spécial dans notre annuaire: **les stratégies de groupe**.

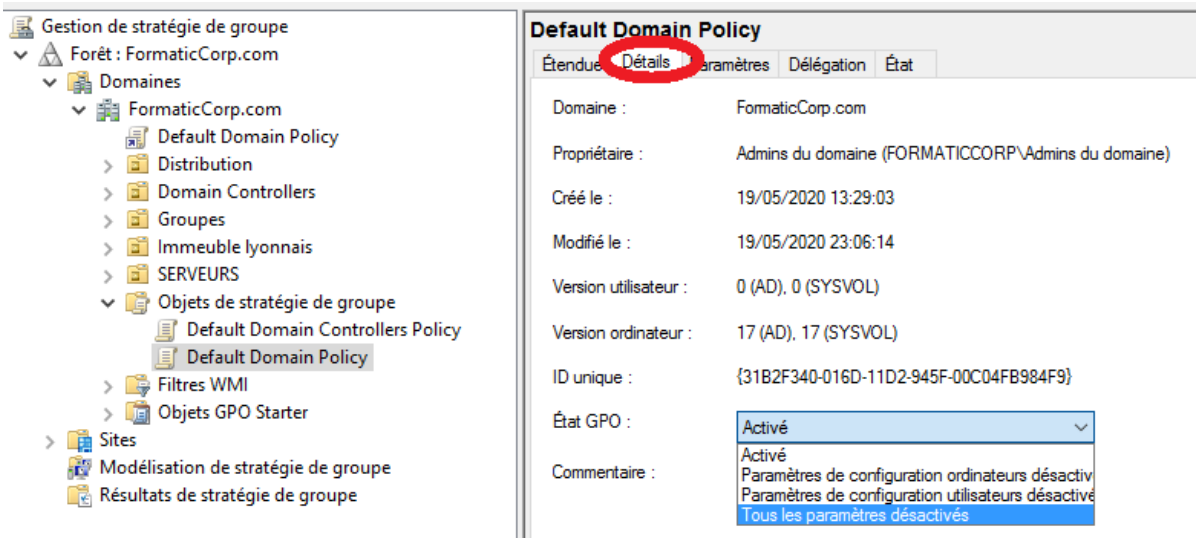
Les stratégies de groupe ou **GPO (Group Policy Object)**, sont des outils puissants pour automatiser de nombreuses tâches en lien avec la personnalisation et la sécurisation de vos ressources.

Vous trouverez la fenêtre « Gestion de stratégie de groupe » (dans notre version nommé Gestion de**s** stratégie**s** de groupe) comme d'habitude via les outils de votre gestionnaire de serveur ou en ouvrant le menu démarrer puis « Outils d'administration Windows ». Tout comme notre annuaire AD, l'installation du rôle a provoqué la création automatique de certaines GPO de base, notamment une pour la gestion du domaine et une autre pour la gestion des contrôleurs de domaine (« Default Domain Policy » et « Default Domain Controllers Policy ») :

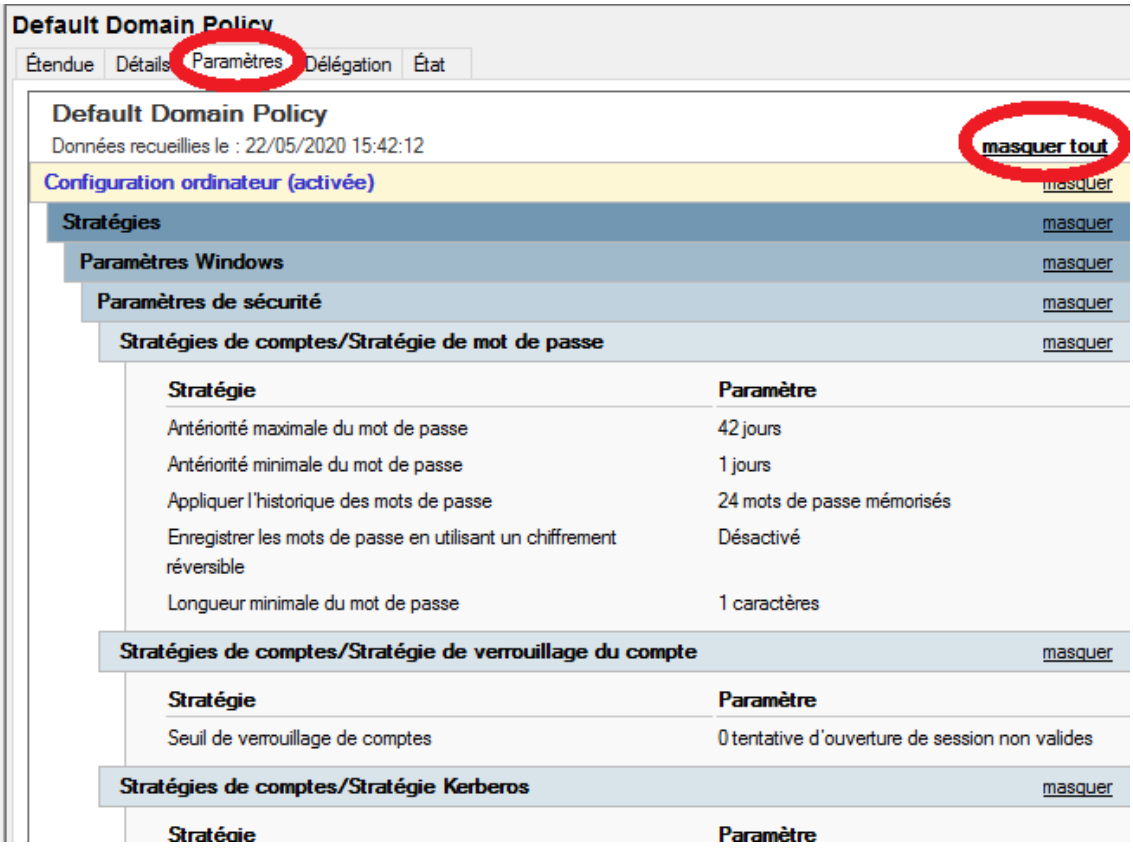


Par défaut vous devriez être positionné sur la stratégie de groupe s'appliquant au domaine. Dans le cadre du bas « Filtrage de sécurité », on peut voir qu'elle ne concernera que le groupe de sécurité « Utilisateurs authentifiés ».

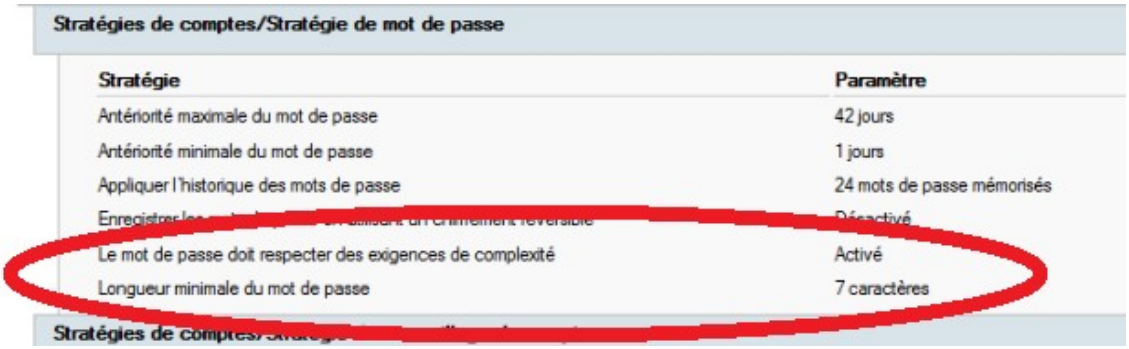
Si vous cliquez sur le deuxième onglet, « Détails », vous aurez accès notamment à la date de création de la GPO, à son numéro d'identifiant unique et à son état (avec la possibilité de désactiver les paramètres ordinateurs ou utilisateurs, ou les 2) :



Si vous cliquez maintenant sur l'onglet « Paramètres » puis « Afficher tout » en haut à droite de la nouvelle fenêtre « Default Domain Policy » vous aurez en visuel l'ensemble des stratégies liées à cette GPO :



Cette fenêtre devrait vous rappeler quelque chose. C'est la stratégie de groupe que nous avons modifié pour pouvoir ajouter rapidement nos utilisateurs dans notre annuaire sans avoir à respecter les exigences de complexité ou la longueur de base de 7 caractères minimum. Ainsi, si nous n'avions pas modifié cette GPO nous aurions eu les informations suivantes :



Dans notre cas la ligne « Le mot de passe doit respecter des exigences de complexité » a complètement disparu et la « Longueur minimale du mot de passe » a été positionné à 1 caractère dans mon cas.

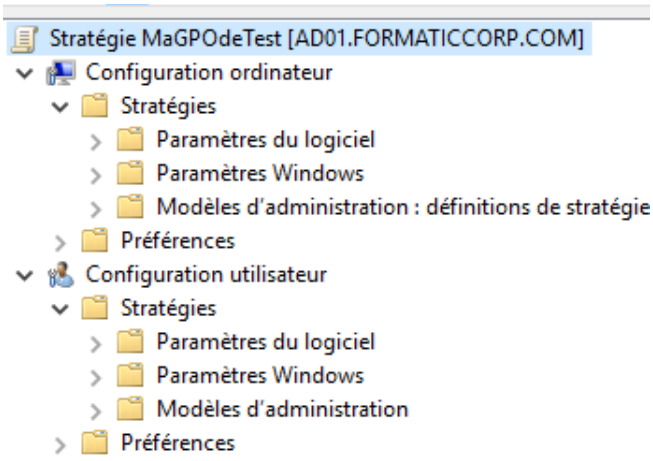
L'avant dernier onglet « Délégation » permettra d'obtenir la liste des utilisateurs et groupes ayant les autorisations de modification de cette GPO.

Pour finir, l'onglet « Etat » présente l'état de la réplication en place (il sera effectivement important de répliquer et sauvegarder vos GPOs).

Si on étudie la GPO pour la gestion des contrôleurs de domaine on verra dans les paramètres qu'elle s'intéresse principalement à la gestion des droits utilisateurs mais aussi aux accès réseaux et aux paramètres d'échanges de données entre les membres du domaine (avec les notions de signature et de chiffrement notamment).

Nous avons vu précédemment dans les paramètres et les possibilités d'activation qu'**une GPO pouvait affecter un utilisateur ou un ordinateur**. Ainsi, le premier type de paramètres s'appliquera en **fonction de l'utilisateur** connecté sur la machine, **peut importe la machine** et un second qui **s'appliquera sur la machine**, **peut importe l'utilisateur** connecté.

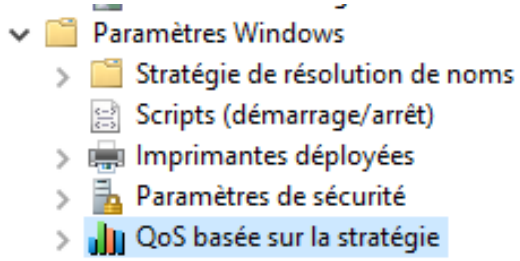
Les 2 types de configuration seront sous divisés en 3 parties :



Les **paramètres logiciels** permettent de gérer des déploiements de logiciels de façon centralisée. On pourra gérer et installer automatiquement des logiciels pour un utilisateur ou un ordinateur donné. Nous verrons des cas concrets un peu plus tard.

Les **paramètres Windows** permettrons de lancer différents scripts qui exécuteront des actions à différents moments clés (démarrage du poste, connexion d'un utilisateur, etc…). Certains paramètres ne seront disponibles que pour l'ordinateur, notamment les paramètres de pare-feu. D'autres ne peuvent être mis en place que pour un utilisateur, comme les paramètres d'Internet Explorer.

On pourra par exemple configurer une stratégie de mot de passe pour un groupe d'utilisateurs particuliers, faire des redirections de dossiers, déployer des imprimantes ou encore mettre en place des **QoS (Quality of Services**, soit des restrictions de bande passante au sein de votre réseau) :



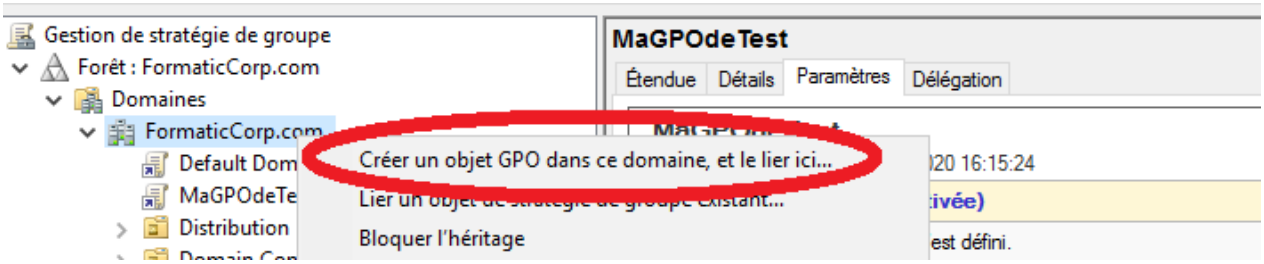
Les **modèles d'administration** sont des fichiers au format ADMX qui permettent de gérer la base de registre de Windows. Cela va permettre de modifier un grand nombre de paramètres en lien avec les différentes zones du registre Windows. À noter que vous disposez ici d'une description du paramètre et de l'impact qu'il pourra avoir sur le comportement des clients.

Les Préférences permettrons de simplifier de nombreuses tâches en apportant une interface graphique proche de celle que l'on pourrait retrouver sur un poste client. On parlera aussi de Group Policy Preferences **(GPP)**, qui, à la différences des autres GPO, seront **déployées, mais pourront être modifiées par l'utilisateur.**

II. Configuration des postes utilisateurs avec les GPO

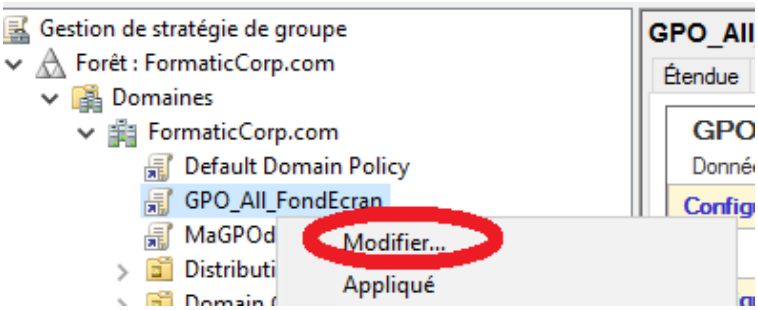
Pour aborder notre première GPO nous allons en créer une toute simple (exemple classique) qui permets de changer le fond d'écran de tous les utilisateurs de l'entreprise.

Dans votre fenêtre « Gestion de stratégie de groupe », vous allez faire un clic droit sur le nom de votre domaine puis sélectionnez « Créer un objet GPO dans ce domaine, et le lier ici... »:

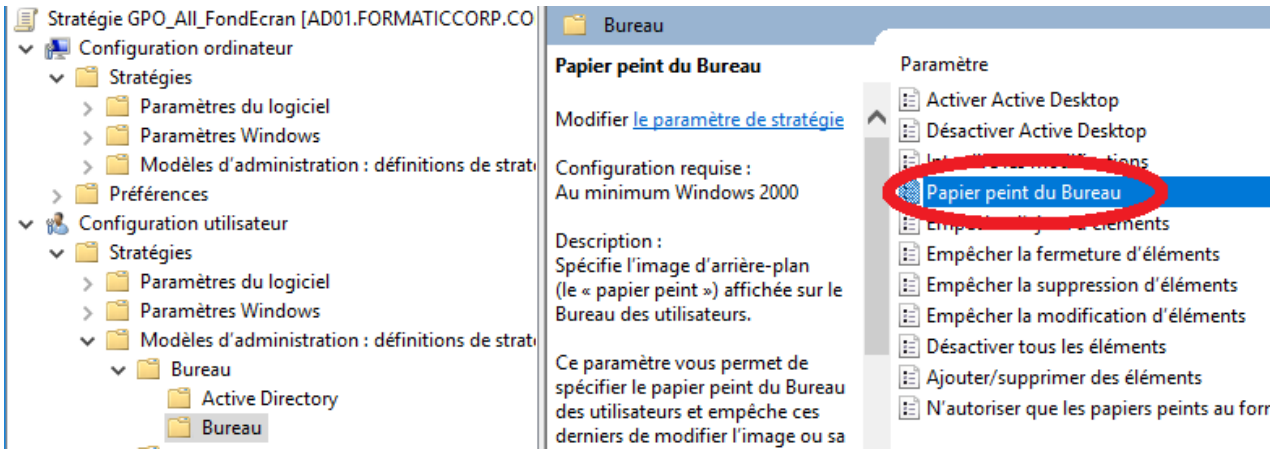


Donnez un nom explicite à votre nouvelle GPO, par exemple GPO_All_FondEcran qui vous permettra de voir qu'il s'agit d'un objet de type stratégie de groupe, qui s'appliquera à tous (All) et concerne le fond d'écran.

On va ensuite modifier notre GPO, en faisant un clic droit dessus puis « Modifier » :

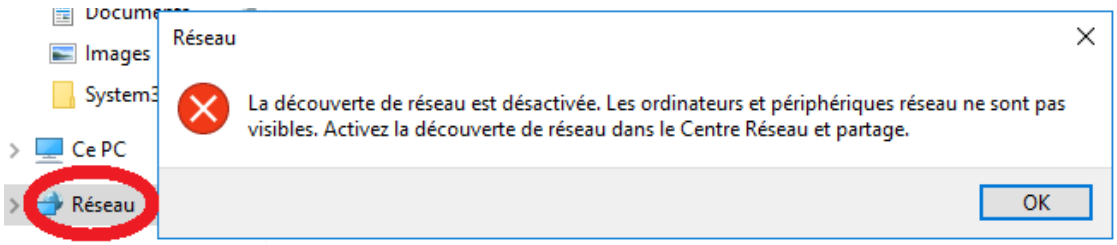


Nous allons accéder au paramètre souhaité en naviguant dans la « Configuration utilisateur », puis « Stratégies » -> « Modèle d'administration:définition de stratégie... » -> « Bureau » → « Bureau » :

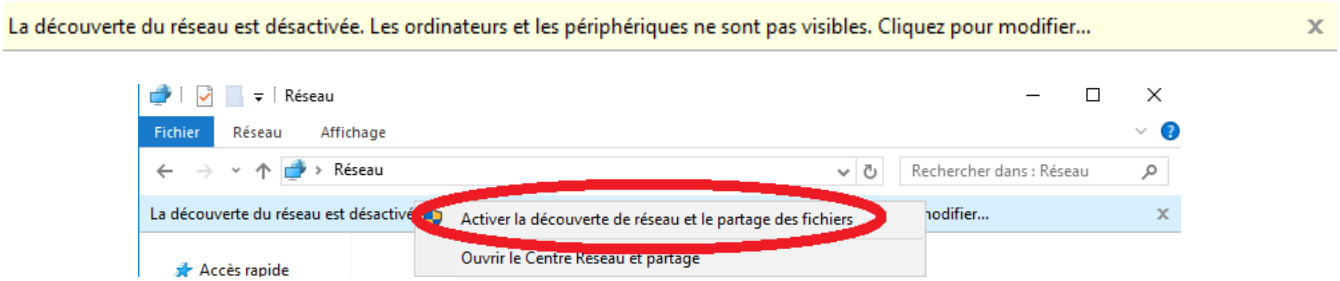


Pour finir nous allons sélectionner « Papier peint du Bureau » dans le 3ème volet « Paramètre » tout à droite. Lorsque l'on clique dessus on a la petite description du paramètre sélectionné dans la fenêtre centrale. On peut ensuite faire un clic droit dessus puis « Modifier »(un double clic dessus marchera aussi) pour accéder au paramètre. On va cocher la case « **Activé »** puis on va devoir aller chercher notre image pour le fond d'écran souhaité. Ce fond d'écran devra être **stocké sur un emplacement réseau accessible** (sinon vos postes clients ne pourrons pas l'afficher…). On pourra mettre en place un partage ou utiliser ceux mis en place par défaut sur notre contrôleur de domaine lors de son installation: **NETLOGON** et **SYSVOL**.

Dans votre explorateur de fichiers Windows, cliquez sur réseau et fermer la fenêtre qui s'affiche :

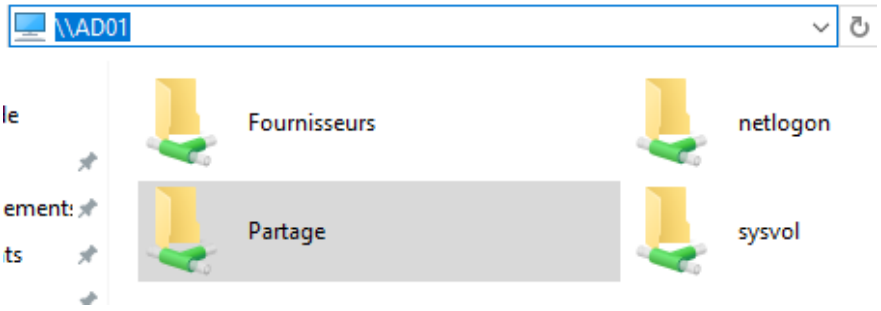


Dans cette même fenêtre on pourra cliquer tout en haut sur :



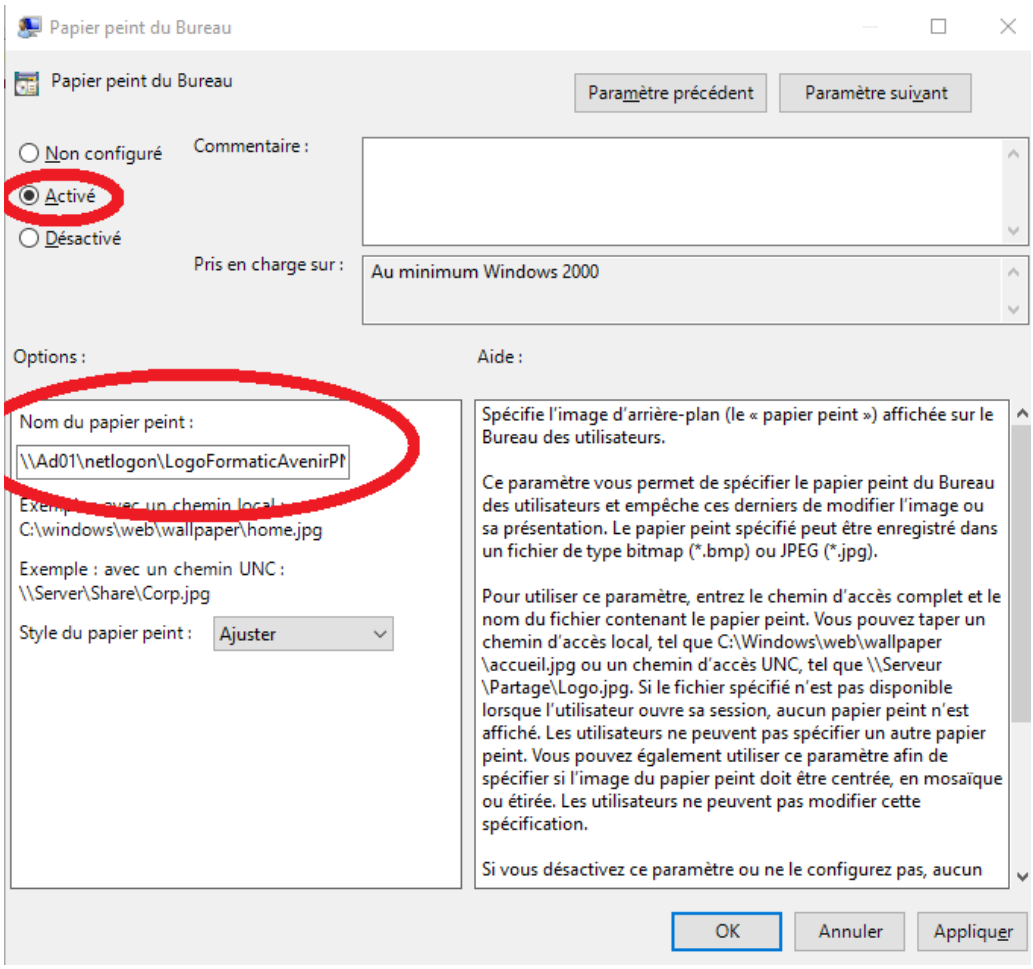
Après avoir activé la découverte du réseau vous devriez voir apparaître 2 dossiers.

Si vous ne voyez pas apparaître ces dossiers taper \\ »nom de votre contrôleur de domaine » dans la barre de navigation en haut (dans mon cas \\DC01) :



On pourrait aussi tester la création d'un nouvel objet AD de type dossier partagé après avoir créé dans C : un dossier partagé, et mis les autorisations à tout le monde en lecture dessus (comme les 2 dossiers « Fournisseurs » et « Partage »).

Enregistrez une image de votre choix dans le dossier « netlogon » puis revenez sur la fenêtre de votre GPO et indiquez le chemin vers votre fichier partagé (attention de bien indiquer le chemin vers le serveur et non vers le dossier présent physiquement sur votre lecteur C : du serveur par exemple) :



Vous venez de créer une GPO pour tous les utilisateurs authentifiés de votre domaine. Chaque personne qui se connectera avec ses identifiants AD aura pour fond d'écran l'image que vous avez choisi.

On va maintenant sur notre poste client (si la machine était éteinte, le nouveau fond d'écran se mets en place dès la connexion de l'utilisateur au domaine et le chargement de son profil utilisateur AD). Pour forcer l'application de vos stratégies de groupe sur un poste, vous pouvez utiliser des commandes. Si vous tapez « gpupdate » dans une invite de commande vous appliquerez les paramètres modifiés uniquement. « Gpupdate /force » va provoquer le rechargement de tous les paramètres liés à vos GPO :

```
C:\Users\bob>gpupdate
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:\Users\bob>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.
```

Testez maintenant la commande « gpresult ». Elle vous permettra de réaliser plusieurs opérations sur les stratégies de groupe et notamment afficher les informations RSoP (Results of Set of Policy) avec la commande « gpresult /R ». Vous devriez trouver des informations sur votre ordinateur, l'objet AD concerné, le contrôleur de domaine, ses groupes de sécurité et l'indication que notre GPO est bien chargée :

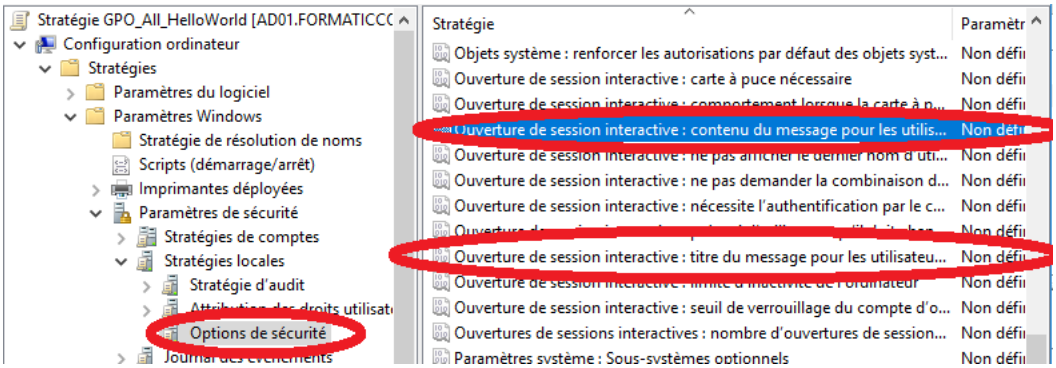
```
Objets Stratégie de groupe appliqués
-----------------------------------
    GPO_All_FondEcran
```

On pourra créer une nouvelle GPO « GPO_All_HelloWorld », toujours au niveau de la racine de notre domaine, qui affichera le message HelloWorld après le démarrage de Windows, avant la connexion de votre utilisateur.

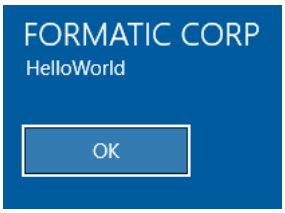
Pour cela vous devrez aller dans « Configuration ordinateur » → « Stratégies » -> « Paramètres Windows » -> « Paramètres de sécurité » -> « Stratégies locales » -> « Options de sécurité » et modifier les 2 paramètres suivants :

- **Ouverture de session interactive** : contenu du message pour les utilisateurs essayant de se connecter.

- **Ouverture de session interactive** : titre du message pour les utilisateurs essayant de se connecter.



Si vous redémarrez votre machine cliente vous devriez avoir ceci (dans ce cas on aura mis « FORMATIC CORP » pour le titre et « Hello World » pour le message ; l'affichage sera différent suivant votre version de Windows) :



Vous pouvez ainsi donner des instructions générales, ou ponctuelles, sur votre entreprise, votre réseau, les bonnes pratiques, etc. Si vous travaillez dans une petite entreprise familiale ou une start-up vous pouvez mettre un message hebdomadaire pour indiquer les dernières nouvelles de l'entreprise, un message d'humour ou encore le dicton de la semaine, etc…

Vous pourrez « enrichir » les GPO existantes avec des modèles d'administration ce qui vous donnera accès à de nouveaux type de paramétrages pour les éléments existants, plus fins ou carrément accès à des nouveaux éléments de paramétrages (microsoft office, microsoft edge, etc...). Ce sont des fichiers de type ADMX qui seront stockés dans un magasin central, le Central Store, au sein du dossier SYSVOL (qui est répliqué entre tous les contrôleurs de domaine).

Vous pourrez télécharger ces modèles depuis le site de Microsoft Windows pour récupérer les fichiers .admx liés à Windows Serveur 2022 par exemple.

Pour aller plus loin : Téléchargez des modèles ADMX et créer une GPO à partir des nouveaux modèles d'administration. On pourra par exemple modifier les paramètres de Microsoft Edge pour choisir notre page d'accueil (mettre par défaut le site web de votre entreprise) ou encore mettre en place des favoris par défaut (site web de votre entreprise, site intranet de votre entreprise et boîte mail professionnelle par exemple).

Si on télécharge le fichier .msi de google chrome, on aura dans le dossier zip les fichiers .admx associés.

On pourra aussi créer ses propres modèles d'administration.