**Stratégies de domaine**

Ce laboratoire doit être fait individuellement sur l'ordinateur virtuel 2

**Objectifs**

* Utiliser l’éditeur des objets de stratégies de groupe
* Se familiariser avec les objets de stratégie "Default Domain Policy" et "Default Domain Controllers Policy"
* Créer des objets de stratégie de groupe au niveau du domaine

**IMPORTANT: sous aucun prétexte les stratégies suivantes ne peuvent être détruites ou modifiées**

* Default Domain Controllers Policy
* Default Domain Policy

**Par défaut, les paramètres de la stratégie de l'ordinateur sont appliqués lors du démarrage du poste et mis à jour aux 90 minutes avec un décalage aléatoire compris entre 0 et 30 minutes sur les postes clients mais aux 5 minutes sur le contrôleur de domaine.**

**Par défaut, les paramètres de la stratégie utilisateur sont appliqués à l'ouverture d'une session et mis à jour aux 90 minutes avec un décalage aléatoire compris entre 0 et 30 minutes sur les postes clients mais aux 5 minutes sur le contrôleur de domaine.**

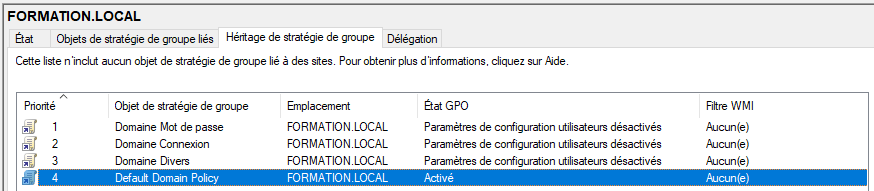
**Documentation sur les GPO qui sont liées au domaine**

Les paramètres qui sont dans la section "**Configuration utilisateur**" d'une stratégie de groupe qui est liée au niveau du domaine s'appliquent à tous les utilisateurs du domaine même si les utilisateurs sont dans le conteneur "**Users**".

Les paramètres qui sont dans la section "**Configuration ordinateur**" d'une stratégie de groupe qui est liée au niveau du domaine s'appliquent à tous les ordinateurs du domaine même si les ordinateurs sont dans le conteneur "**Computers**".

**Documentation sur la priorité d'exécution des GPO**

L’exécution commence par la dernière, celle qui a le chiffre le plus gros et termine par celle qui a le numéro 1, donc la plus haute priorité.



La GPO qui s'exécute en premier est "Default Domain Policy".

Si un administrateur veut modifier des paramètres qui sont dans "Default Domain Policy".

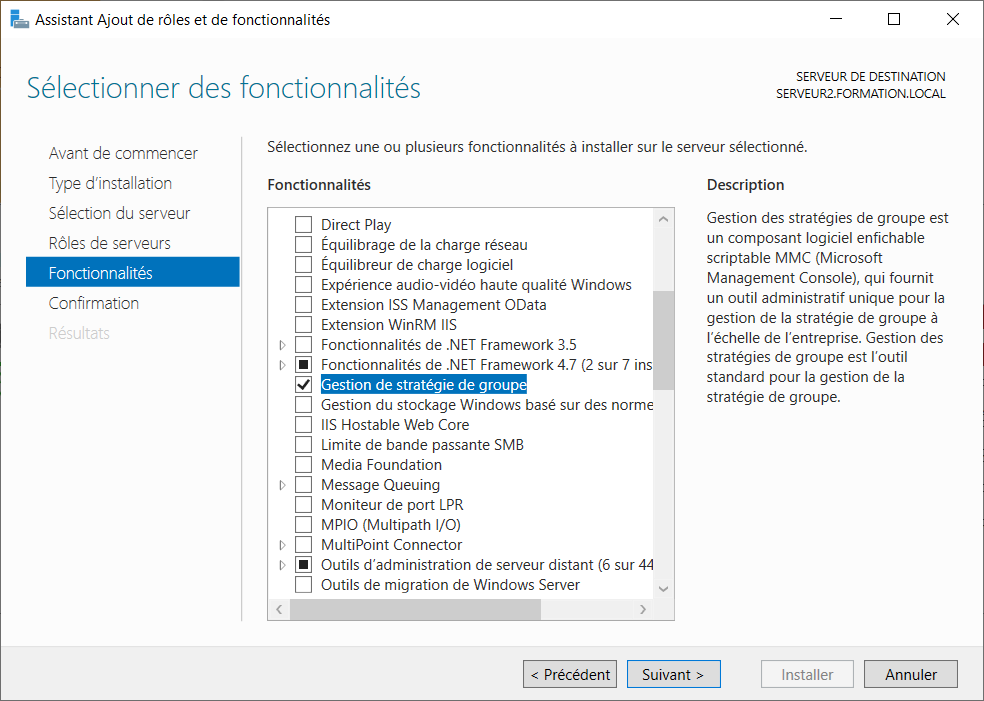
1. Il va créer des GPO qui vont modifier les paramètres.
2. Il va s'assurer que ses GPO vont s'exécuter après la GPO "Default Domain Policy".

**Si un même paramètre existe dans une autre GPO alors le paramètre est remplacé par l'exécution d'une GPO qui a une plus grande priorité d'exécution.**

**La console "Gestion des stratégies de groupe"**

La console "**Gestion des stratégies de groupe**" est présente sur le serveur virtuel SERVEUR1 parce que c'est le contrôleur de domaine.

Sur votre serveur virtuel SERVEUR2, vous devez installer la console "**Gestion des stratégies de groupe**"



**Étape 1 - La GPO "Default Domain Policy"**

Vous devez créer un rapport HTM de la GPO "Default Domain Policy" dans le dossier C:\\_GPO\_RAPPORTS.

* Vous devez sélectionner la GPO "Default Domain Policy" et dans le menu contextuel sélectionner "**Enregistrer le rapport…**".

Voici la section du rapport "HTM" que vous devez consulter pour répondre aux prochaines questions.

**Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies de comptes /**

**Stratégie de mot de passe**

* Quelle est la durée maximale des mots de passe (antériorité maximale) ?

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Quelle est la durée minimale des mots de passe (antériorité minimale) ?

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Combien de mots de passe garde-t-on dans l'historique ?

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Est-ce que les mots de passe doivent respecter des exigences de complexité ?

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Quelle est la longueur minimale des mots de passe ?

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

En utilisant la console "Gestion des stratégies de groupe" sélectionner la GPO "Default Domain Policy"

* Vous devez choisir "**Modifier…**" dans le menu contextuel.
* Vous devez sélectionner le paramètre.
* Vous devez afficher les propriétés du paramètre et cliquer sur l’onglet "**Expliquer**".

Voici la section que vous devez consulter pour répondre aux prochaines questions.

**Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies de comptes /**

**Stratégie de mot de passe**

* Quelles valeurs sont recommandées comme durée maximale ?

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Que signifie le paramètre "durée minimale du mot de passe" ?

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Quel est le nombre maximal de mots de passe qu’on peut conserver dans l’historique ?

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Quelle est la plus grande longueur minimale pour les mots de passe ?

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Voici la section que vous devez consulter pour répondre à la prochaine question.

**Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies de comptes /**

**Stratégie de verrouillage du compte**

* Dans la GPO de domaine, le seuil de verrouillage de comptes est à 0 tentative.

Qu’est-ce que cela signifie ?

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Étape 2 - La GPO "Default Domain Controllers Policy"**

Vous devez créer un rapport HTM de la GPO "Default Domain Controllers Policy" dans le dossier C:\\_GPO\_RAPPORTS.

* Vous devez sélectionner la GPO "Default Domain Controllers Policy" et dans le menu contextuel sélectionner "**Enregistrer le rapport…**".

Voici la section du rapport "HTM" que vous devez consulter pour répondre aux prochaines questions.

**Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies locales /**

**Attribution des droits utilisateur**

Vous devez vérifier si les groupes mentionnés sont présents dans les paramètres suivants.

Vous devez répondre par **absent** ou **présent**.

* **Accéder à cet ordinateur à partir du réseau**

AUTORITE NT\Utilisateurs authentifiés réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

BUILTIN\Administrateurs réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tout le monde réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* **Ajouter des stations de travail au domaine**

AUTORITE NT\Utilisateurs authentifiés réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

BUILTIN\Administrateurs réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* **Arrêter le système**

AUTORITE NT\Utilisateurs authentifiés réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

BUILTIN\Administrateurs réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* **Forcer l’arrêt à partir d’un système distant**

AUTORITE NT\Utilisateurs authentifiés réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

BUILTIN\Administrateurs réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* **Modifier l’heure système**

AUTORITE NT\Utilisateurs authentifiés réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

BUILTIN\Administrateurs réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* **Permettre l'ouverture d’une session locale**

AUTORITE NT\Utilisateurs authentifiés réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

BUILTIN\Administrateurs réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Ce qui veut dire que les utilisateurs qui ne sont pas membres du groupe Administrateurs ne peuvent pas se connecter sur le "Contrôleur de domaine".**

**Étape 3 - Création de stratégies au niveau du domaine**

Dans la console "Gestion des stratégies de groupe"

* Créer les GPO suivants dans la section "Objets de stratégies de groupe"

La GPO "C\_Domaine Mot de passe" qui définit des paramètres sur les mots de passe

La GPO "C\_Domaine Connexion" qui définit des paramètres pour l'ouverture de session

La GPO "C\_Domaine Divers" qui définit divers paramètres

**note: au début chaque GPO est vide**

* Fixer les paramètres mentionnés pour chaque GPO.

**note: présentement, les GPO ne sont liés à aucune unité d’organisation**

**La GPO "C\_Domaine Mot de passe"**

La section utilisateur doit être désactivée sur la GPO, onglet "Détails", paramètre "État GPO"

**Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies de comptes /**

**Stratégie de mot de passe**

* Durée de vie maximale du mot de passe

**note: configurer la valeur de ce paramètre à 365 jours**

* Durée de vie minimale du mot de passe

**note: configurer la valeur de ce paramètre à 0 jours**

* Longueur minimale du mot de passe

**note: configurer la valeur de ce paramètre à 9 caractères**

**Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies locales /**

**Options de sécurité**

* Ouverture de session interactive: prévenir l'utilisateur qu'il doit changer son mot de passe avant qu'il n'expire

**note: configurer la valeur de ce paramètre à 7 jours**

Vous devez créer un rapport HTM de de la GPO "C\_Domaine Mot de passe" dans le dossier C:\\_GPO\_RAPPORTS.

* Vous devez sélectionner la GPO "C\_Domaine Mot de passe" et dans le menu contextuel sélectionner "**Enregistrer le rapport…**".

**La GPO "C\_Domaine Divers"**

La section utilisateur doit être désactivée sur la GPO, onglet "Détails", paramètre "État GPO"

**Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies locales /**

**Options de sécurité**

* Arrêt: permet au système d’être arrêté sans avoir à se connecter

**note: configurer la valeur de ce paramètre à Activé**

**Configuration ordinateur / Stratégies / Modèles d'administration / Composants Windows / Windows PowerShell**

* Activer l’exécution des scripts

**note: configurer la valeur de ce paramètre à "Autoriser tous les scripts"**

Vous devez créer un rapport HTM de de la GPO "C\_Domaine Divers" dans le dossier C:\\_GPO\_RAPPORTS.

* Vous devez sélectionner la GPO "C\_Domaine Divers" et dans le menu contextuel sélectionner "**Enregistrer le rapport…**".

**La GPO "C\_Domaine Connexion"**

La section utilisateur doit être désactivée sur la GPO, onglet "Détails", paramètre "État GPO"

**Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies locales /**

**Options de sécurité**

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

**note: configurer la valeur de ce paramètre à Activé**

* Ouvertures de sessions interactives: nombre d’ouverture de sessions précédentes réalisées en utilisant la cache (lorsqu'aucun contrôleur de domaine n'est disponible)

**note: configurer la valeur de ce paramètre à 0**

**Configuration ordinateur / Stratégies / Modèles d'administration / Composants Windows /**

**Options d'ouverture de session Windows**

* Afficher les informations sur les ouvertures de session précédentes au cours d'une ouverture de session utilisateur

**note: configurer la valeur de ce paramètre à Activé**

**Configuration ordinateur / Stratégies/ Modèles d'administration / Système**

* Afficher le moniteur d’évènements de mise hors tension

**note: configurer la valeur de ce paramètre à Désactivé**

**Configuration ordinateur / Stratégies / Modèles d'administration / Système / Ouverture de session**

* Toujours attendre le réseau lors du démarrage de l’ordinateur et de l’ouverture de session

**note: configurer la valeur de ce paramètre à Activé**

Vous devez créer un rapport HTM de de la GPO "C\_Domaine Connexion" dans le dossier C:\\_GPO\_RAPPORTS.

* Vous devez sélectionner la GPO "C\_Domaine Connexion" et dans le menu contextuel sélectionner "**Enregistrer le rapport…**".

**Étape 4 - Vérification**

Dans la console de gestion des GPO

* Lier les GPO au niveau du domaine
* Dans *Ordre des liens*, faire correspondre le plus petit chiffre (le chiffre 1) à la GPO "Domaine Mot de passe"

Rectifier l’ordre des GPO au besoin

Inscrire l’ordre final des liens dans le tableau suivant:

|  |  |
| --- | --- |
| **Stratégie** | **Ordre** |
| **C\_Domaine Mot de passe** |  |
| **C\_Domaine Connexion** |  |
| **C\_Domaine Divers** |  |
| **Default Domain Policy** | **4 - Cette stratégie doit être complètement en bas de la liste.** |

Ouvrir une "Invite de commandes" en tant qu'administrateur et exécuter la commande "**gpupdate.exe /force**".

Fermer la session de FORMATION\TECH sur le SERVEUR2.

Avant d’entrer le nom de l'utilisateur et le mot de passe, remarquez le bouton en bas à droite de l’écran.

C’est à cause de la GPO "C\_Domaine Divers" (permet au système d’être arrêté sans avoir à se connecter).

Ouvrir une session en tant que FORMATION\TECH.

Remarquez les informations qui sont affichées tout de suite après l'ouverture de session (écran bleu).

C’est à cause de la GPO "C\_Domaine Connexion" (afficher les informations lors de l'ouverture de session).

Le changement de mot de passe de l'utilisateur TECH pour **Secret1** sera refusé.

Comparer les rubriques "Longueur minimale du mot de passe" des GPO "C\_Domaine Mot de passe" et "Default Domain Policy".

Que concluez-vous ?

**Étape 5 - Créer une sauvegarde des GPO**

Vous devez créer une copie de sécurité de toutes les GPO dans le dossier C:\\_GPO\_BACKUP.

* Dans le menu contextuel de "**Objets de stratégie de groupe**"
* Vous devez sélectionner l'option "**Sauvegarder tout…**"

**Étape 6 - Supprimer des GPO et les récupérer dans la sauvegarde**

Vous devez supprimer les GPO "C\_Domaine Mot de passe", "C\_Domaine Divers" et "C\_Domaine Connexion".

* Dans le menu contextuel de "**Objets de stratégie de groupe**"
* Vous devez sélectionner l'option "**Gérer les sauvegarde…**"

Vous devez restaurer une GPO à la fois.

Vous devez lier chaque GPO au domaine.

**ANNEXE**

Voici la liste des CMDLETS du module GroupPolicy.

**PS C:\\_OUTILS> (Get-Command -Module GroupPolicy).Name**

**Get-GPPermissions**

**Set-GPPermissions**

**Backup-GPO**

**Copy-GPO**

**Get-GPInheritance**

**Get-GPO**

**Get-GPOReport**

**Get-GPPermission**

**Get-GPPrefRegistryValue**

**Get-GPRegistryValue**

**Get-GPResultantSetOfPolicy**

**Get-GPStarterGPO**

**Import-GPO**

**Invoke-GPUpdate**

**New-GPLink**

**New-GPO**

**New-GPStarterGPO**

**Remove-GPLink**

**Remove-GPO**

**Remove-GPPrefRegistryValue**

**Remove-GPRegistryValue**

**Rename-GPO**

**Restore-GPO**

**Set-GPInheritance**

**Set-GPLink**

**Set-GPPermission**

**Set-GPPrefRegistryValue**

**Set-GPRegistryValue**