

Durcissement de l'Active Directory

Version de Windows : Serveur 2022

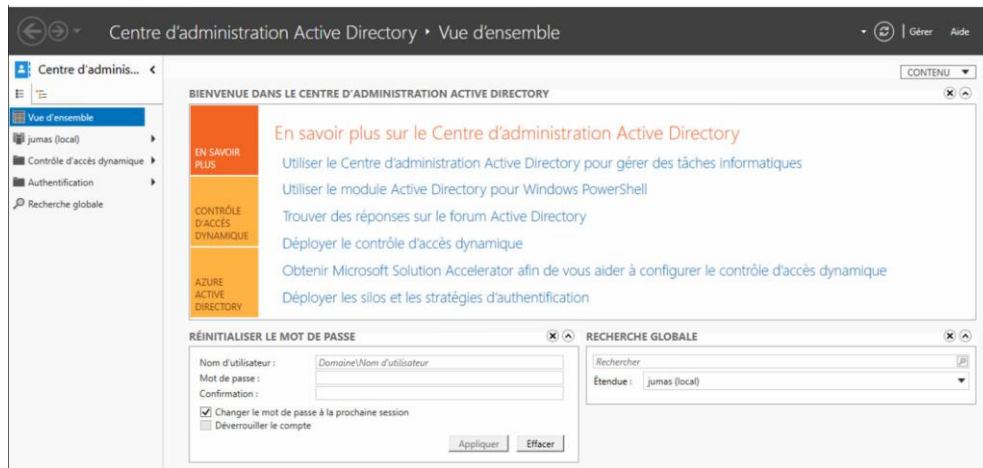
1 – Amélioration de la stratégie de mot de passe.....	1
2 – Désactiver le Print Spooler service	5
3 – Désactiver SMBv1	6
4 – Désactiver LLMNR et Netbios.....	9
4.1 – Désactiver LLMNR via une GPO	9
4.2 – Désactiver NetBIOS via une GPO	10
5 – Protéger le compte krgbt	12

Le hardening de l'Active Directory, ou encore le durcissement de l'Active Directory à pour but d'améliorer la sécurité de celui-ci en désactivant par exemple des protocoles qui sont connues pour ne plus être sur et en renforçant la sécurité via une stratégie de mot de passe forte et des groupes de sécurités.

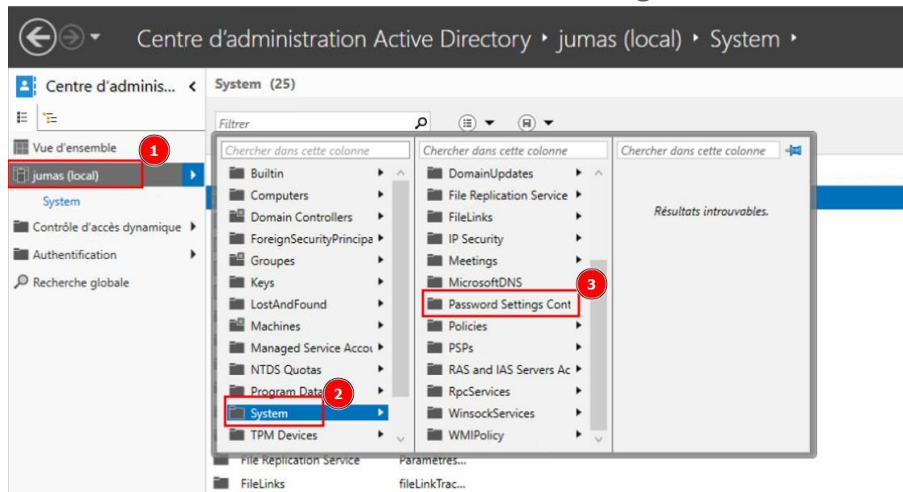
1 – Amélioration de la stratégie de mot de passe

La stratégie de mot de passe par défaut n'est plus suffisante dans un contexte de sécurité comme le connaît actuellement notre société. De ce fait, nous allons améliorer cette stratégie et également bloquer les sessions après un nombre infructueux de tentative de connexion. Cela va notamment servir à éviter les attaques de type Brute force.

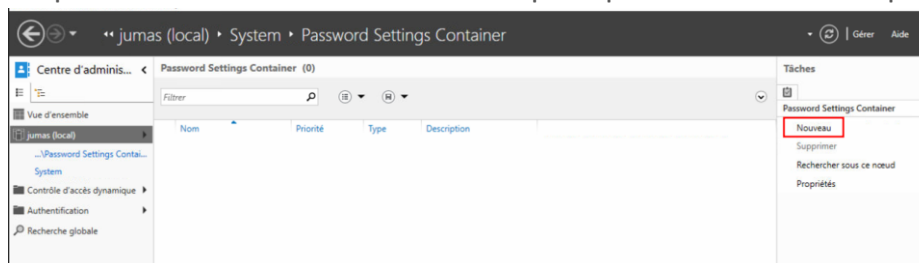
Sur votre contrôleur de domaine, ouvrez le « **Centre d'administration Active Directory** ».



Rendez-vous ensuite dans « **Password Settings Container** »



Cliquez maintenant sur « **Nouveau** » pour pouvoir créer notre politique



Nous allons commencer par donner un nom à notre politique, essayez d'utiliser quelque chose de logique et qui vous permettra de vous y retrouver.

Créer Paramètres de mot de passe : Politique_Everyone

Paramètres de mot de passe

Nom : * Politique_Everyone

Priorité : * 1

☒ Appliquer la longueur minimale du mot de passe

Longueur minimale du mot de passe (caractères) : * 7

☒ Appliquer l'historique des mots de passe

Nombre de mots de passe mémorisés : * 24

☒ Le mot de passe doit respecter des exigences de complexité

☐ Stocker le mot de passe en utilisant un chiffrement réversible

☒ Protéger contre la suppression accidentelle

Description :

Options d'âge du mot de passe :

☒ Appliquer l'âge minimal de mot de passe

L'utilisateur ne peut pas changer le mot de passe d... * 1

☒ Appliquer l'âge maximal de mot de passe

L'utilisateur doit changer le mot de passe après (jo...) * 42

☐ Appliquer la stratégie de verrouillage des comptes :

Nombre de tentatives de connexion échouées autoris... *

Réinitialiser le nombre de tentatives de connexion éc... * 30

Le compte va être verrouillé

☒ Pendant une durée de (mins) : * 30

☐ Jusqu'à ce qu'un administrateur déverrouille manuellement le com...

Nous allons maintenant mettre une longueur minimale de mot à 12 caractères (recommandation de la CNIL)

☒ Appliquer la longueur minimale du mot de passe

Longueur minimale du mot de passe (caractères) : * 12

L'historique des mots de passe empêche un utilisateur de réutiliser un ancien mot de passe, la valeur par défaut est correcte nous n'allons donc pas modifier ce paramètre.

☒ Appliquer l'historique des mots de passe

Nombre de mots de passe mémorisés : * 24

Cochez la case afin de respecter les exigences de complexité et SURTOUT ne cochez pas la case permettant un chiffrement réversible (cela signifie que le mot de passe peut être retrouver en clair)

☒ Le mot de passe doit respecter des exigences de complexité

☐ Stocker le mot de passe en utilisant un chiffrement réversible

L'âge minimal de mot de passe représente la durée de vie d'un mot de passe en jour, ce qui permet de changer plusieurs fois d'affilée de mot de passe. La valeur à mettre est en jour.

Options d'âge du mot de passe :

☒ Appliquer l'âge minimal de mot de passe

L'utilisateur ne peut pas changer le mot de passe d... * 30

Désactiver l'application d'un âge maximal afin de respecter les recommandations de l'ANSSI

Nous allons maintenant activer la stratégie de verrouillage des comptes, cela va permettre d'empêcher les attaques de type brute force. Nous allons ainsi verrouiller le compte après 3 échecs et autoriser à nouveau la connexion après 60 min

Ajoutez ensuite le groupe sur lequel vous voulez appliquer cette politique, pour ma part je vais appliquer cette politique sur tous les utilisateurs du domaine

Vous devriez vous retrouver avec une politique ressemblante à l'image ci-dessous

2 – Désactiver le Print Spooler service

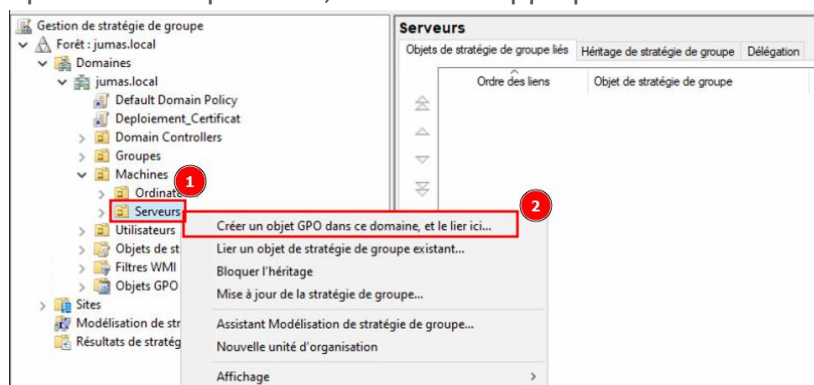
Si ce service est activé sur le contrôleur de domaine, alors il rend celui-ci vulnérable à l'attaque nommée « PrintNightmare » et qui permet d'obtenir les droits SYSTEM, à savoir les droits les plus élevés !

Afin de se prémunir contre cela, il est important de désactiver ce service.

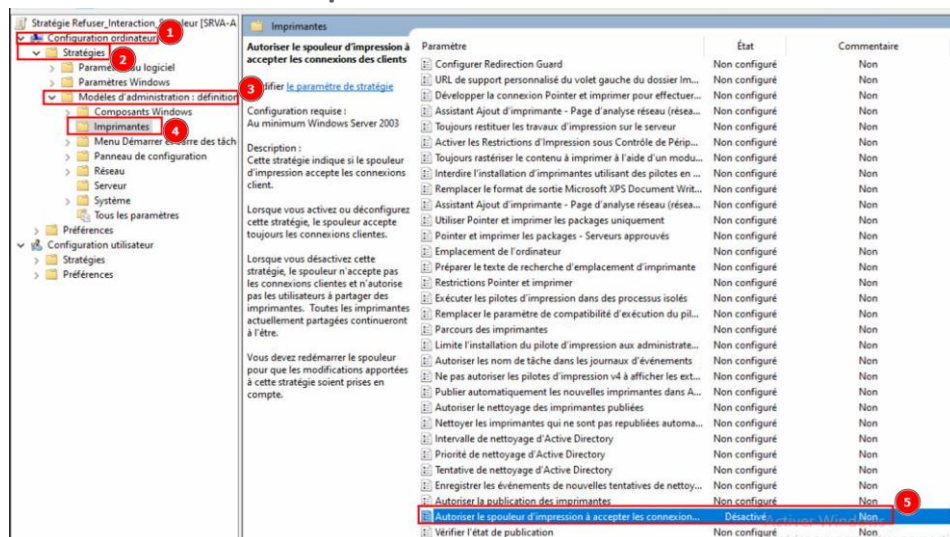
Pour ce faire nous allons utiliser une simple commande PowerShell sur notre contrôleur de domaine



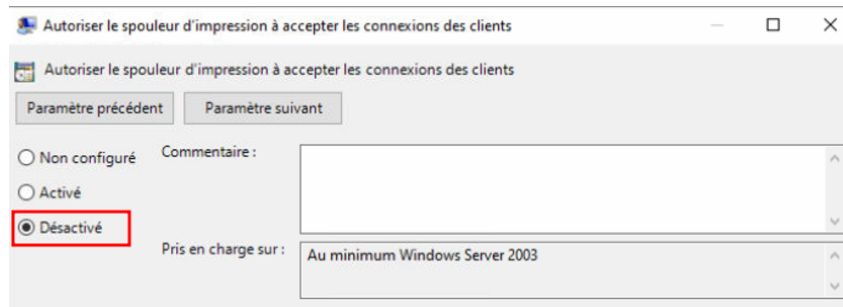
Maintenant, nous allons faire en sorte de bloquer les interactions distantes sur le Spouleur d'impression, il va falloir appliquer cette GPO sur une OU pour vos serveurs



Il va falloir ensuite désactiver la GPO « Autoriser le spouleur d'impression à accepter les connexions des clients » dans Configuration ordinateur -> Stratégies -> Modèles d'administration -> Imprimantes



Mettez cette GPO sur « **Désactivé** »



3 – Désactiver SMBv1

SMBv1 est la toute première version de SMB (Server Message Block) du protocole permettant le partage de ressources. Cette version est vulnérable à la vulnérabilité nommée « **EternalBlue** » qui permet de devenir SYSTEM sur le contrôleur de domaine et tout ordinateur utilisant cette version de SMB en seulement 5 minutes.

Nous allons donc utiliser une GPO qui s'appliquera sur l'ensemble du parc pour interdire l'utilisation de cette version.

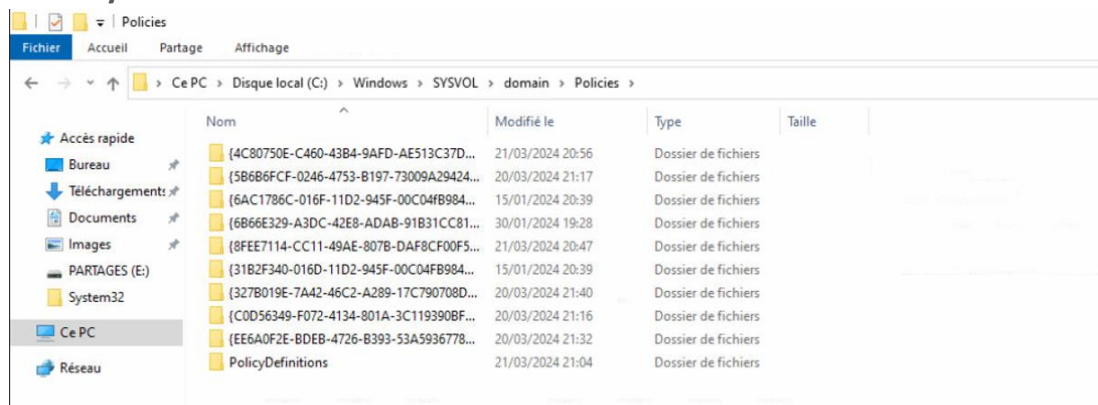
Il va falloir en premier lieu télécharger une GPO dans le magasin [Microsoft](#). Sélectionnez « **Windows 11 Security Baseline.zip** »

☒ Windows 11 Security Baseline.zip 1.2 MB

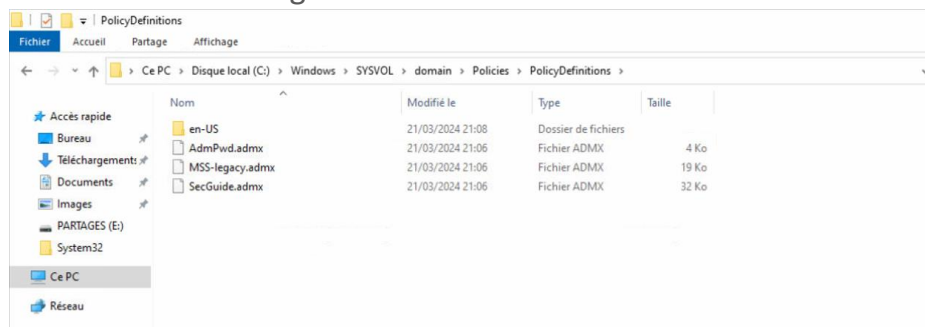
Maintenant, rendez-vous dans le chemin suivant

C:\Windows\SYSTEM32\domain\Polices et créez un nouveau dossier

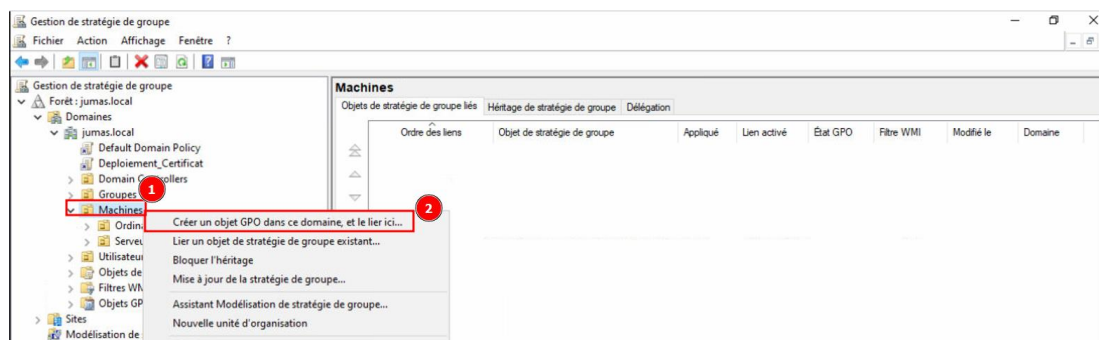
« **PolicyDefinitions** »



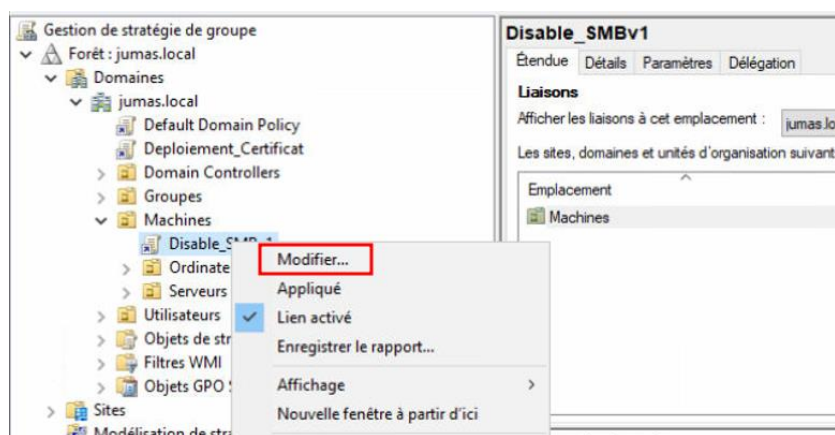
Dans ce dossier, il va falloir mettre les fichiers « admx » présent dans le fichier que nous avons téléchargé



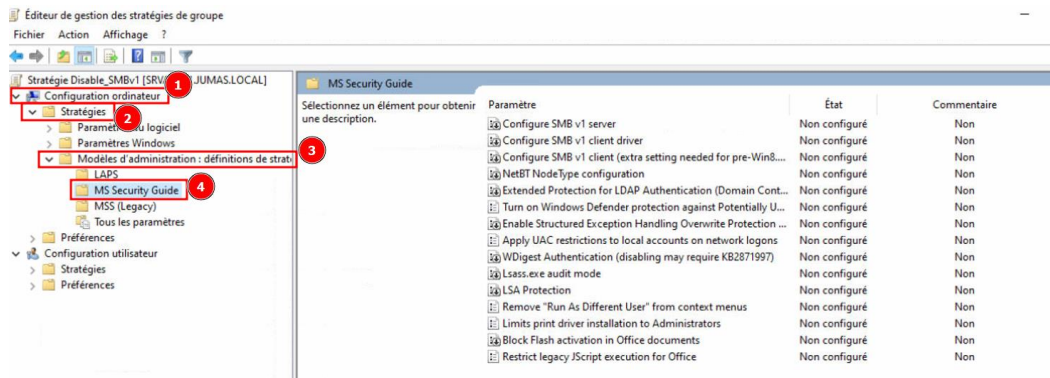
Je vais maintenant créer cette GPO dans mon OU « **Machines** »



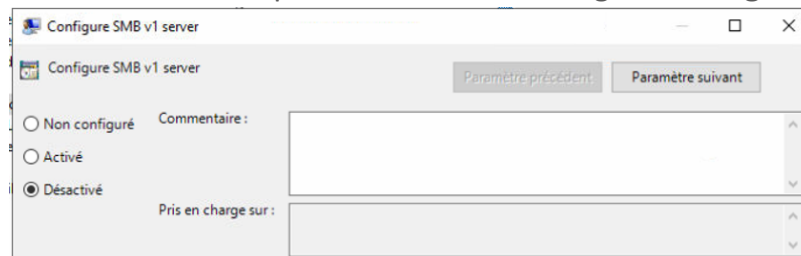
Il va ensuite falloir modifier cette GPO



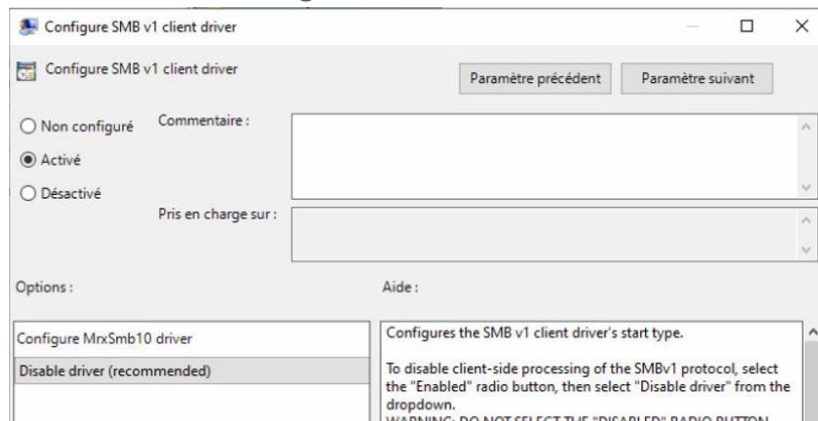
Il va maintenant falloir se rendre dans l'emplacement **Configuration ordinateur -> Stratégies -> Modèles d'administration -> MS Security Guide**



Il faut commencer par désactiver la stratégie « **Configure SMB v1 server** »



Nous allons ensuite désactiver la stratégie « **Configure SMB v1 client driver** ». Pour ce faire activez la stratégie et sélectionner « **Disable driver** »



4 – Désactiver LLMNR et Netbios

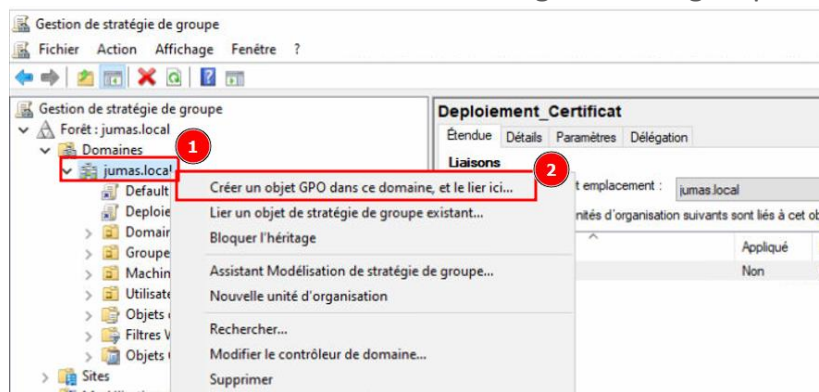
Le protocole LLMNR (Local Link Multicast Name Resolution) permet la résolution de noms localement. Il est utilisé lorsque la résolution DNS échoue.

Le risque est qu'un attaquant s'étant introduit dans le réseau pourrait empoisonner les paquets en se faisant passer pour le nom recherché.

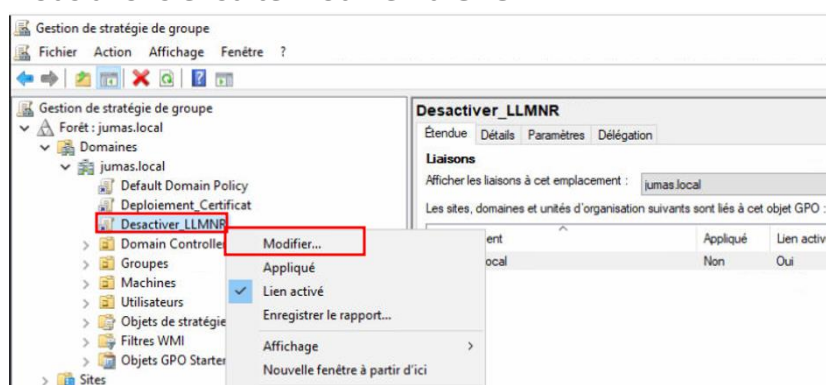
Netbios quant à lui est utilisé pour effectuer la recherche de ressources sur un réseau local. Ce protocole est aussi vulnérable à l'empoisonnement de paquet, un attaquant pourrait se faire passer pour une ressource réseau et tenter de récupérer le hash NTLM d'une machine avec des outils comme Responder.

4.1 – Désactiver LLMNR via une GPO

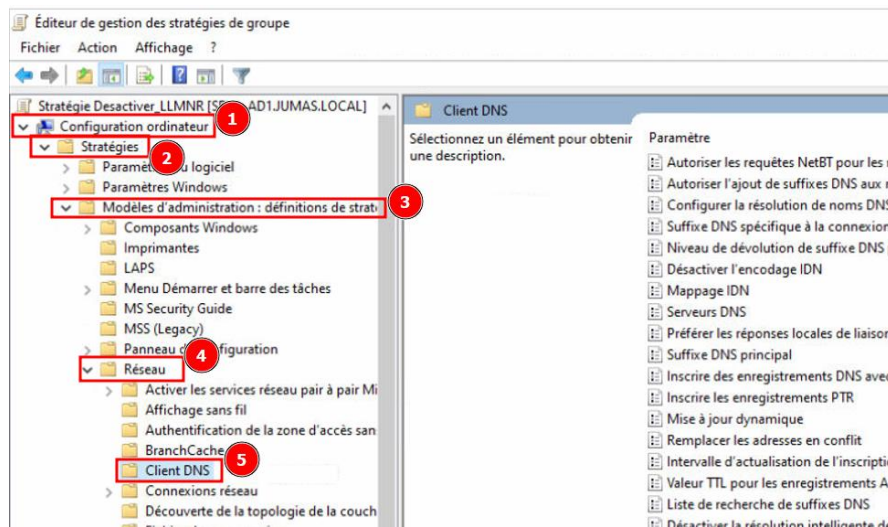
Nous allons créer une stratégie de groupe qui sera liée à la racine du domaine. Pour ce faire, rendez-vous dans la console de gestion de groupe et créer une GPO à la racine



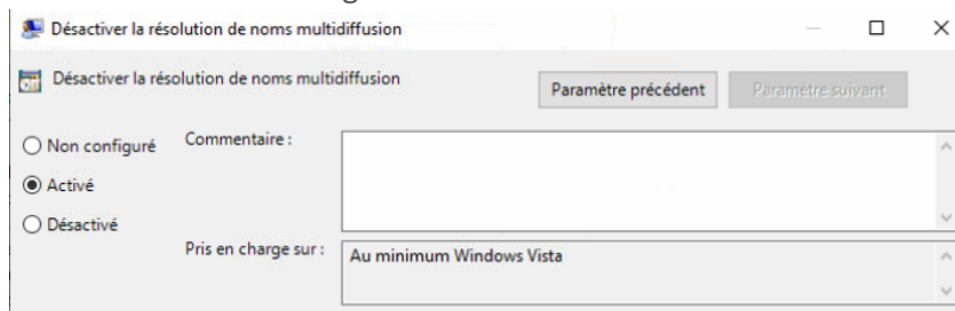
Nous allons ensuite modifier la GPO



Rendez-vous dans **Configuration ordinateur -> Stratégies -> Modèles d'administration -> Réseau -> Client DNS**



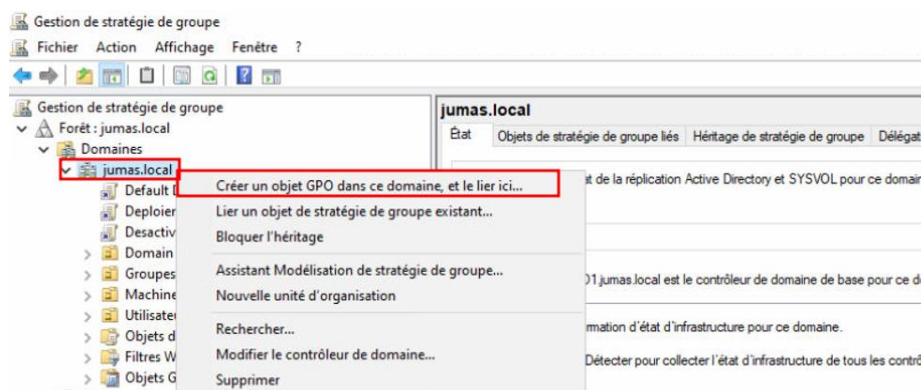
Activez ensuite la stratégie « **Désactiver la résolution de noms multidiffusion** »



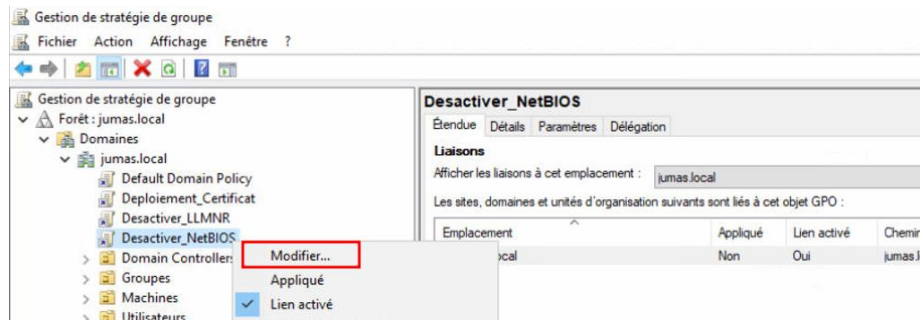
4.2 – Désactiver NetBIOS via une GPO

Afin de désactiver NetBIOS il va falloir jouer sur les clés de registre. Nous allons utiliser un script PowerShell déjà existant et faire en sorte qu'il s'exécute sur les machines.

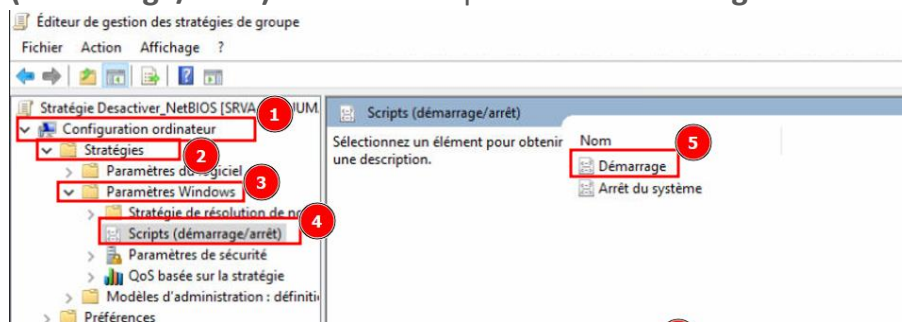
Créez une GPO à la racine de votre domaine



Modifiez cette GPO



Rendez-vous dans **Configuration ordinateur -> Paramètres Windows -> Scripts (démarrage/arrêt)** et double cliquez sur « Démarrage »

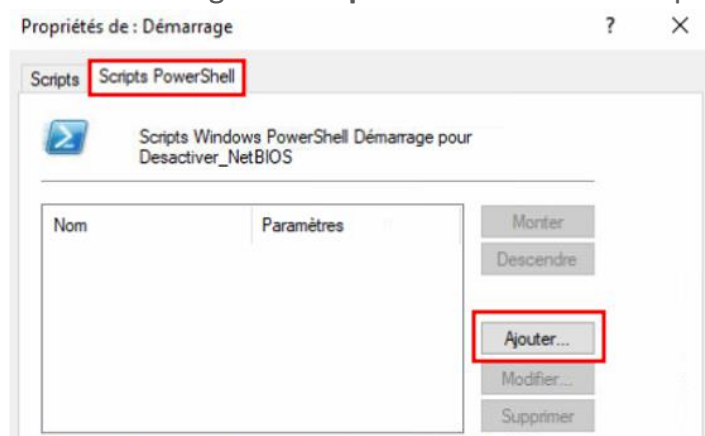


Rendez-vous dans le chemin suivant

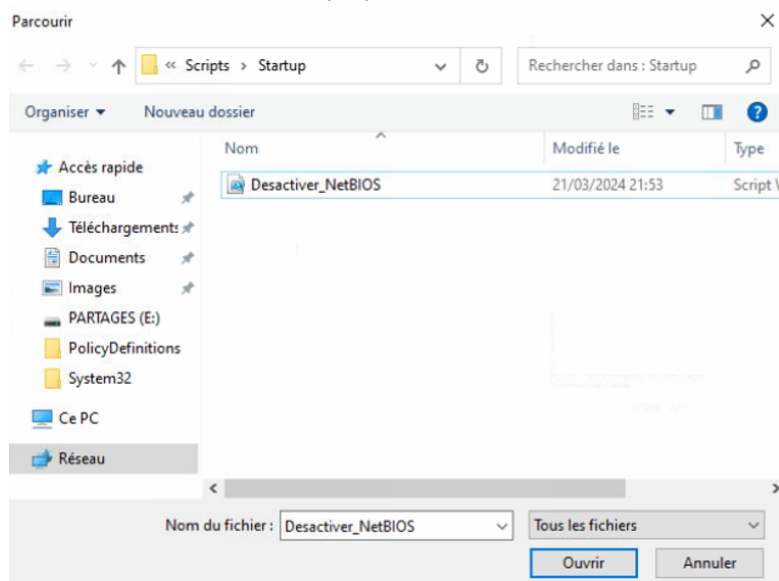
« \\domaine\\SysVol\\domaine\\Politiques\\{C838EA2B-8B69....}\\Machine\\Scripts\\Startup », créez un fichier PowerShell et collez le script suivant :

```
Set-ItemProperty -Path
'HKLM:\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\Interfaces\tcpip_*'
-Name NetbiosOptions -Value 2 -Verbose
```

Allez dans l'onglet « **Scripts PowerShell** » et cliquez sur « **Ajouter** »



Sélectionnez votre script précédemment créé



Une fois ajouté, ce script s'exécutera à chaque démarrage de toutes les machines.

5 – Protéger le compte krgbt

Le compte krgbt est sujet à des attaques de type « Golden Tickets ». Ce type d'attaque va permettre à un attaquant d'avoir accès à toutes les ressources du domaine en exploitant les vulnérabilités du protocole Kerberos.

Afin de se prémunir contre ce type d'attaque, il faut réinitialiser le mot de passe de ce compte 2 fois, car Windows garde un historique de 2 mots de passe. De plus, l'ANSSI recommande de changer le mot de passe de compte tous les ans.

Il va falloir suivre une méthode précise afin de ne pas perturber le bon fonctionnement de l'Active Directory. Il va falloir réinitialiser le mot de passe une première fois, puis attendre 10 heures avant de réinitialiser à nouveau le mot de passe afin de s'assurer que tous les tickets en cours récupèrent bien le mot de passe.

Pour mener à bien tout cela, nous allons utiliser un script publié par Microsoft.

Nous allons commencer par le télécharger à l'aide de PowerShell

```
# Temporarily allow TLS1.2
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12

# Download the script.
Invoke-WebRequest https://raw.githubusercontent.com/microsoft/New-KrbtgtKeys.ps1/master/New-KrbtgtKeys.ps1 -O ./New-KrbtgtKeys.ps1
```


Insérez maintenant votre nom de domaine

```

+++ RESET KRBTGT ACCOUNT PASSWORD FOR RWDCs/RODCs +++

[2024-03-21 22:25:03] : * BLOG: http://jorgequestforknowledge.wordpress.com/ *
[2024-03-21 22:25:03] : * v2.5, 2020-02-17 *
[2024-03-21 22:25:03] : * ***** *
[2024-03-21 22:25:03] :
[2024-03-21 22:25:03] : Do you want to read information about the script, its functions, its behavior and the impact? [YES | NO]: NO
[2024-03-21 22:25:06] : --> Chosen: NO
[2024-03-21 22:25:06] :
[2024-03-21 22:25:06] : -----
[2024-03-21 22:25:06] : LOADING REQUIRED POWERSHELL MODULES...
[2024-03-21 22:25:06] :
[2024-03-21 22:25:13] : PoSH Module 'ActiveDirectory' Has Been Loaded...
[2024-03-21 22:25:13] :
[2024-03-21 22:25:16] : PoSH Module 'GroupPolicy' Has Been Loaded...
[2024-03-21 22:25:16] :
[2024-03-21 22:25:16] : -----
[2024-03-21 22:25:16] : SELECT THE MODE OF OPERATION...
[2024-03-21 22:25:16] : Which mode of operation do you want to execute?
[2024-03-21 22:25:16] : - 1 - Informational Mode (No Changes At All)
[2024-03-21 22:25:16] : - 2 - Simulation Mode (Temporary Canary Object Created, No Password Reset!)
[2024-03-21 22:25:16] : - 3 - Simulation Mode - Use KrbTgt TEST/BOGUS Accounts (Password Will Be Reset Once!)
[2024-03-21 22:25:16] : - 4 - Real Reset Mode - Use KrbTgt PROD/REAL Accounts (Password Will Be Reset Once!)
[2024-03-21 22:25:16] :
[2024-03-21 22:25:16] : - 8 - Create TEST KrbTgt Accounts
[2024-03-21 22:25:16] : - 9 - Cleanup TEST KrbTgt Accounts
[2024-03-21 22:25:16] :
[2024-03-21 22:25:16] : - 0 - Exit Script
[2024-03-21 22:25:16] :
[2024-03-21 22:25:16] : Please specify the mode of operation: 4
[2024-03-21 22:25:16] : --> Chosen Mode: Mode 4 - Real Reset Mode - Use KrbTgt PROD/REAL Accounts (Password Will Be Reset Once!)...
[2024-03-21 22:25:16] : -----
[2024-03-21 22:25:16] : SPECIFY THE TARGET AD FOREST...
[2024-03-21 22:25:16] : For the AD forest to be targeted, please provide the FQDN or press [ENTER] for the current AD forest: jumas.local

```

Sélectionnez maintenant l'option 1

```

+++ RESET KRBTGT ACCOUNT PASSWORD FOR RWDCs/RODCs +++

SRVA-AD1.jumas.local True Default-First-Site-Name Read/Write krbtgt 2024-01-15 20:40:03 RWDc Demoted 2024-01-15 20:40:03 2 192.168.10.251 Windows Server 20
SRVA-AD2.jumas.local False Default-First-Site-Name Read/Write krbtgt 2024-01-15 20:40:03 RWDc Demoted 2024-01-15 20:40:03 2 192.168.10.252 Windows Server 20

[2024-03-21 22:28:07] :
[2024-03-21 22:28:07] : REMARKS:
[2024-03-21 22:28:07] : - 'N.A.' in the columns 'Source RWDc FQDN' and 'Source RWDc DSA' means the RWDc is considered as the master for this script.
[2024-03-21 22:28:07] : - 'RWDc Unreachable' in the columns 'Source RWDc FQDN' and 'Source RWDc DSA' means the RODC cannot be reached to determine its replic
[2024-03-21 22:28:07] :   RWDc/DSA. The unavailability can be due to firewalls/networking or the RODC actually being down.
[2024-03-21 22:28:07] : - 'Unknown' in various columns means that an RODC was found that may not be a true Windows Server RODC. It may be an appliance acting
[2024-03-21 22:28:07] : - 'RWDc Demoted' in the column 'Org RWDc' means the RWDc existed once, but it does not exist anymore as it has been decommissioned in
[2024-03-21 22:28:07] :   This is normal.
[2024-03-21 22:28:07] : - 'No Such Object' in the columns 'Pwd Last Set', 'Org RWDc', 'Org Time' or 'Ver' means the targeted object was not found in the AD d
[2024-03-21 22:28:07] :   Although this is possible for any targeted object, this is most likely the case when targeting the KrbTgt TEST/BOGUS accounts and
[2024-03-21 22:28:07] :   do not exist yet. This may also occur for an appliance acting as an RODC as in that case no KrbTgt TEST/BOGUS account is created.
[2024-03-21 22:28:07] :
[2024-03-21 22:28:07] : --> Found [2] Real DC(s) In AD Domain...
[2024-03-21 22:28:07] : --> Found [2] RWDc(s) In AD Domain...
[2024-03-21 22:28:07] : --> Found [2] Reachable RWDc(s) In AD Domain...
[2024-03-21 22:28:07] : --> Found [0] UnReachable RWDc(s) In AD Domain...
[2024-03-21 22:28:07] :
[2024-03-21 22:28:07] : --> Found [0] RODC(s) In AD Domain...
[2024-03-21 22:28:07] : --> Found [0] Reachable RODC(s) In AD Domain...
[2024-03-21 22:28:07] : --> Found [0] UnReachable RODC(s) In AD Domain...
[2024-03-21 22:28:07] : --> Found [0] Undetermined RODC(s) In AD Domain...
[2024-03-21 22:28:07] :
[2024-03-21 22:28:07] : -----
[2024-03-21 22:28:07] : SELECT THE SCOPE OF THE KRBTGT ACCOUNT(S) TO TARGET...
[2024-03-21 22:28:07] : Which KrbTgt account do you want to target?
[2024-03-21 22:28:07] : - 1 - Scope of KrbTgt in use by all RWDcs in the AD Domain
[2024-03-21 22:28:07] : - 2 - Scope of KrbTgt in use by specific RODC - Single RODC in the AD Domain
[2024-03-21 22:28:07] : - 3 - Scope of KrbTgt in use by specific RODC - Multiple RODCs in the AD Domain
[2024-03-21 22:28:07] : - 4 - Scope of KrbTgt in use by specific RODC - All RODCs in the AD Domain
[2024-03-21 22:28:07] :
[2024-03-21 22:28:07] : - 0 - Exit Script
[2024-03-21 22:28:07] :
[2024-03-21 22:28:07] : Please specify the scope of KrbTgt Account to target: 1,

```


Le script va ensuite réinitialiser le mot de passe

```

+++ RESET KRBtgt ACCOUNT PASSWORD FOR RWDCs/RODCs +++

[2024-03-21 22:29:08] : --> Previous Password Set Date/Time.....: '2024-01-15 20:40:03'
[2024-03-21 22:29:08] : --> New Password Set Date/Time.....: '2024-03-21 22:29:08'
[2024-03-21 22:29:08] : --> Previous Originating RWDc.....: 'RWDc Demoted'
[2024-03-21 22:29:08] : --> New Originating RWDc.....: 'SRVA-AD1.jumas.local'
[2024-03-21 22:29:08] : --> Previous Originating Time.....: '2024-01-15 20:40:03'
[2024-03-21 22:29:08] : --> New Originating Time.....: '2024-03-21 22:29:08'
[2024-03-21 22:29:08] : --> Previous Version Of Attribute Value....: '2'
[2024-03-21 22:29:08] : --> New Version Of Attribute Value.....: '3'
[2024-03-21 22:29:08] : --> The new password for [CN=krbtgt,CN=Users,DC=jumas,DC=local] HAS BEEN SET on RWDc [SRVA-AD1.jumas.local]!...
[2024-03-21 22:29:08] :
[2024-03-21 22:29:08] : ***** CHECK 1 *****
[2024-03-21 22:29:08] : - Contacting DC in AD domain ...[SRVA-AD1.JUMAS.LOCAL]...(SOURCE RWDc)
[2024-03-21 22:29:08] :   * DC is Reachable...
[2024-03-21 22:29:08] :   * The new password for Object [CN=krbtgt,CN=Users,DC=jumas,DC=local] exists in the AD database
[2024-03-21 22:29:08] : - Contacting DC in AD domain ...[SRVA-AD2.JUMAS.LOCAL]...
[2024-03-21 22:29:08] :   * DC is Reachable...
[2024-03-21 22:29:08] :   * The new password for Object [CN=krbtgt,CN=Users,DC=jumas,DC=local] now does exist in the AD database
[2024-03-21 22:29:09] :
[2024-03-21 22:29:09] : --> Start Time.....: 2024-03-21 22:29:08
[2024-03-21 22:29:09] : --> End Time.....: 2024-03-21 22:29:09
[2024-03-21 22:29:09] : --> Duration.....: 0,42 Seconds
[2024-03-21 22:29:09] :
[2024-03-21 22:29:09] : List Of DCs In AD Domain 'jumas.local' And Their Timing...
[2024-03-21 22:29:09] :
[2024-03-21 22:29:09] :
Host Name      PDC Site Name      DS Type      IP Address      Reachable Source RWDc FQDN      Time
-----
SRVA-AD1.jumas.local True Default-First-Site-Name Read/Write 192.168.10.251 True N.A. 0
SRVA-AD2.jumas.local False Default-First-Site-Name Read/Write 192.168.10.252 True SRVA-AD1.jumas.local 0,42

[2024-03-21 22:29:09] :
[2024-03-21 22:29:09] :
[2024-03-21 22:29:09] : Log File Path...: C:\Users\Administrateur\Documents\2024-03-21_22.27.35_SRVA-AD1_ResetKrbtgtPasswordForRWDCsAndRODCsLog.txt
[2024-03-21 22:29:09] :
[2024-03-21 22:29:09] :

```

Il faudra ensuite refaire cette opération après 10h car comme je l'ai dit précédemment, windows garde en historique 2 mots de passe.

Par la suite, ces étapes seront à réalisées tous les ans afin de maintenir un niveau de sécurité optimale en conformité avec les recommandations de l'ANSSI.

Fin de la procédure.