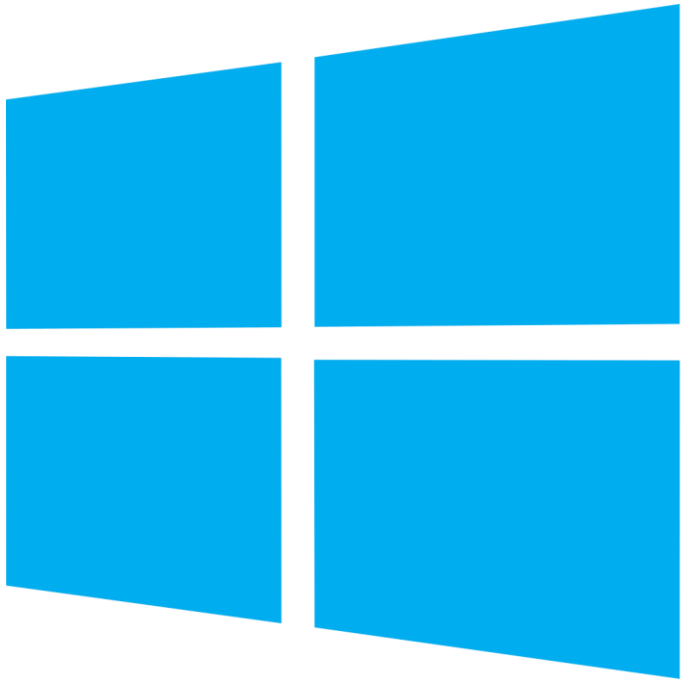


Windows

Environnement de LAB

- SrvDC 192.168.1.10
- SrvFS 192.168.1.11
- SrvBkp 192.168.1.12
- Win10-Clt1 192.168.1.21
- Win10-Clt2 192.168.1.22
- Linux-Clt1 192.168.1.31
- Linux-Clt2 192.168.1.32

- User : Admin
- Password : Pa$$w0rd!
- Domain = sysbas.local
- Hyperviseur = VMWare Workstation Pro

Activation de Windows

Deux méthodes d'activation :

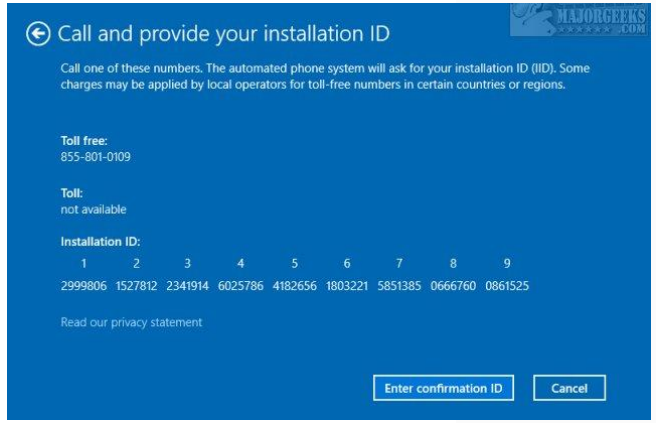
- Clé de produit à 25 caractères XXXX-XXXX-XXXX-XXXX-XXXX
- Licence digitale (lié au hardware et au compte Microsoft)

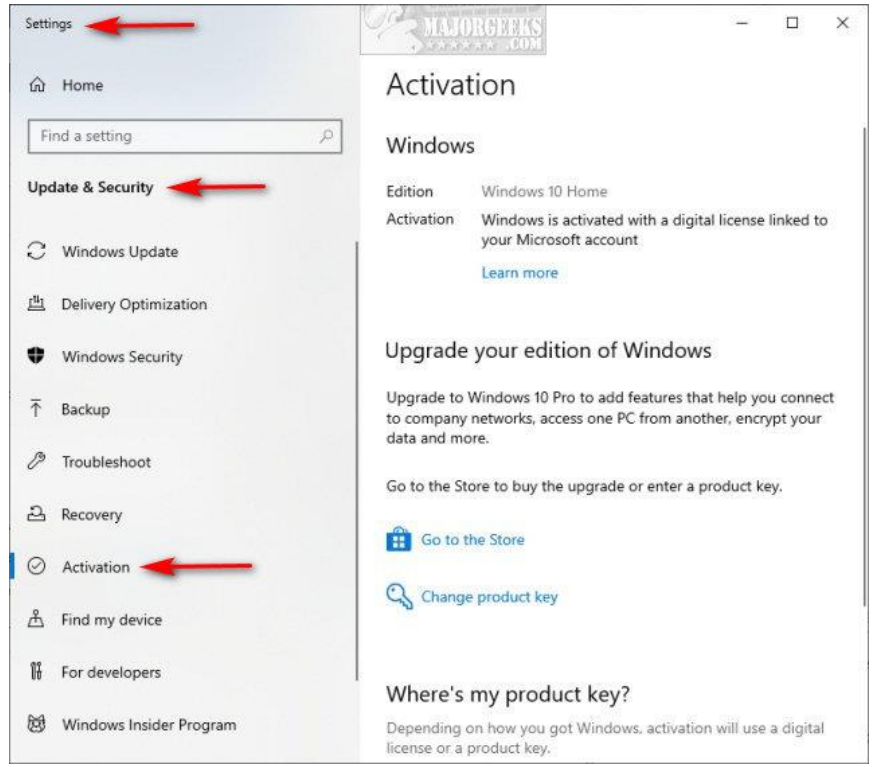
Deux types d'activation :

- Enterprise-level or Volume licensing
  - OEM (Original Equipment Manufacturer) -> Le fabricant inscrit la licence dans le BIOS
  - KMS (Key Management Service) -> Activation via un serveur KMS interne, n'utilise pas internet, une clé peut être utilisée pour plusieurs activations
  - MAK (Multiple Activation Keys) -> Like Consumer keys, but can be enabled multiple times
- Consumer (Achat via Microsoft Store ou n'importe quel revendeur officiel)
  - Activation de la clé à l'installation du système -> Validation par Internet
  - Activation par téléphone ou par chat avec le support Microsoft

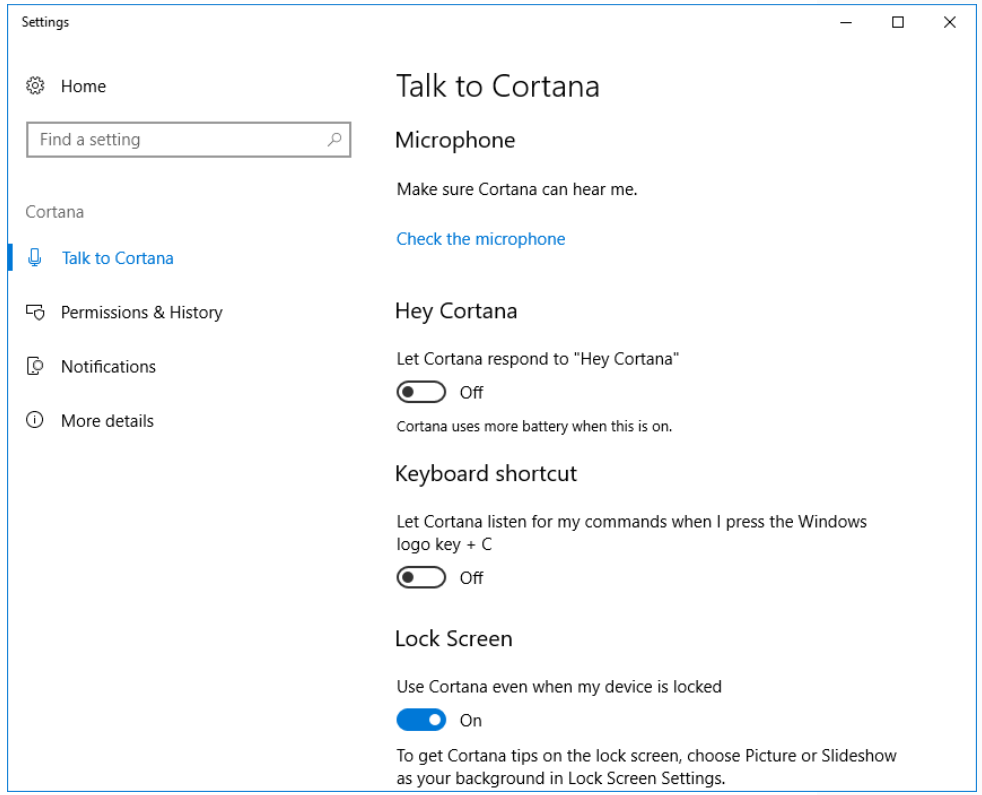
Activation de Windows

- Activate Windows 10 & 11 During Setup
- Activate Windows 10 & 11 in Settings
- Activate Windows 10 & 11 With Activation Troubleshooter
- Activate Windows 10 & 11 in Command Prompt
  Open PowerShell -> command ***slmgr***
- Activate Windows 10 & 11 by Calling Microsoft
  Windows Key + R, type in ***SLUI 4***





Cortana



Cortana est l'assistante de productivité personnelle de Microsoft, qui vous permet de gagner du temps et de concentrer votre attention sur ce qui est important.

Cortana fait partie de Windows 10 dans les paramètres régionaux où Cortana est disponible

Voici quelques-unes des actions que Cortana peut effectuer pour vous :

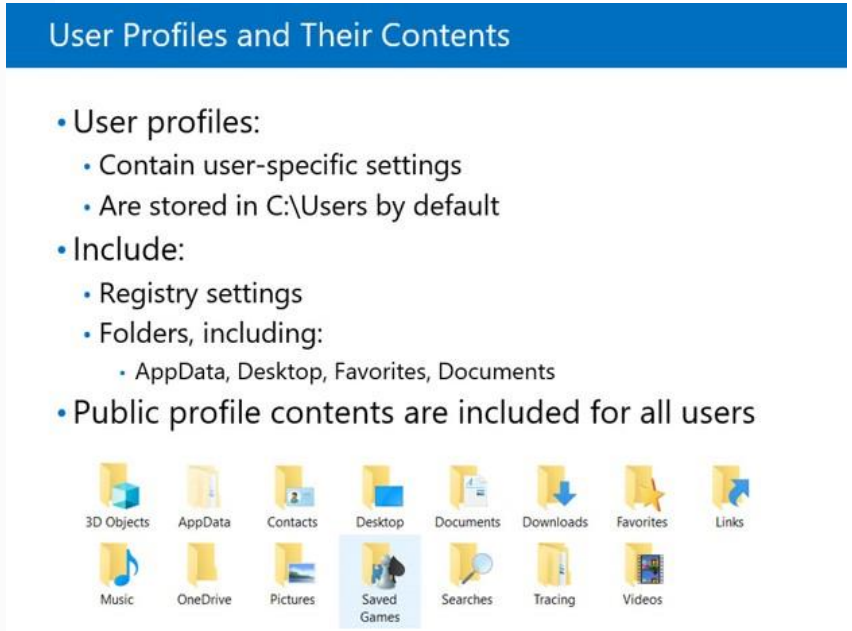
- Gérer votre calendrier et vous tenir informé(e) de votre planning.
- Participer à une réunion dans Microsoft Teams ou découvrir qui participe à votre prochaine réunion.
- Créer et gérer des listes.
- Définir des rappels et des alarmes.
- Rechercher des définitions et des informations.
- Ouvrir les applications sur votre ordinateur.

Profile utilisateur

Le profil utilisateur Windows stocke **les paramètres utilisateurs**
Stock les données tels que les documents, paramètres de Windows (fond d'écran etc), les paramètres des applications, etc. mais également la base de registre.

Le dossier **All Users** est un dossier accessible à tous les utilisateurs et qui permet de stocker des informations qui seront partagées

Le dossier **Default User** stocke le profil par défaut, lorsque vous créez un nouvel utilisateur, ce dernier bénéficiera automatiquement du profil contenu dans Default User.



Migration de profile

User State Migration Tool (USMT) capture les comptes d'utilisateur, les fichiers utilisateur, les paramètres du système d'exploitation et les paramètres d'application, puis les migre vers une nouvelle installation Windows.

L'outil USMT est destiné aux administrateurs qui effectuent des déploiements automatisés à grande échelle. Si vous migrez uniquement les états utilisateur de quelques ordinateurs, vous pouvez utiliser PCmover Express. PCmover n'est pas un utilitaire gratuit. PCmover Express est un outil créé par le partenaire de Microsoft, Laplink.

Lab 1

Scenario

Vous devez remplacer la machine d’un collègue. Il vous demande de copier les paramètres de son ancienne machine (Win10-Clt1) vers la nouvelle (Win10-Clt2). Utilisez USMT pour effectuer la migration

https://learn.microsoft.com/en-us/windows/deployment/usmt/usmt-technical-reference

Comptes utilisateurs

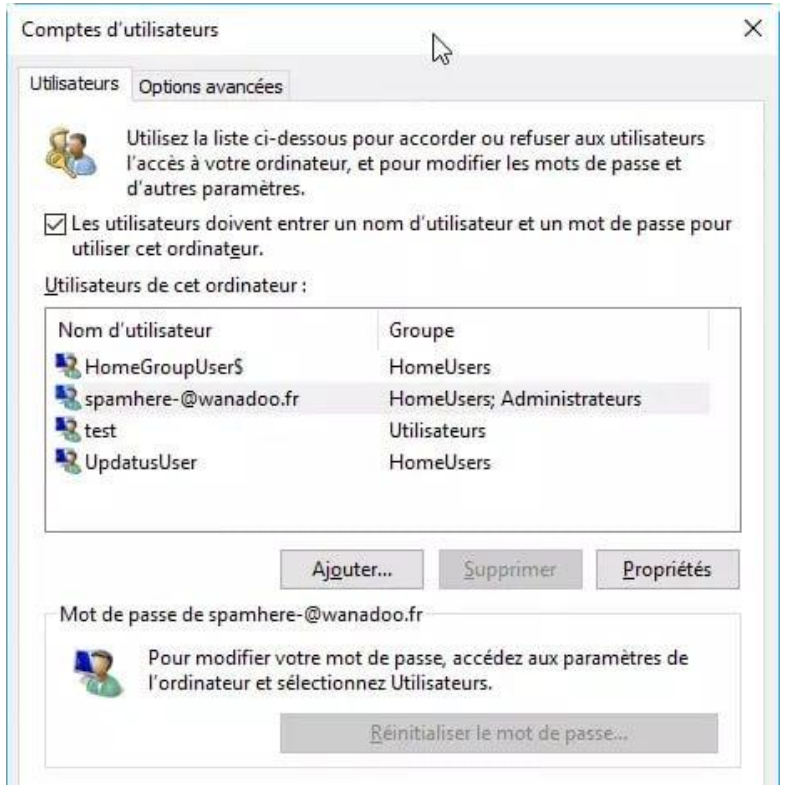
Compte administrateur
C’est le compte qui a le plus de privilège sur le système

Compte administrateur intégré
Désactivé et caché par défaut, n’est pas soumis à l’UAC

Comptes utilisateurs standard
N’ont pas d’accès administrateur et ne peuvent lancer de jetons UAC

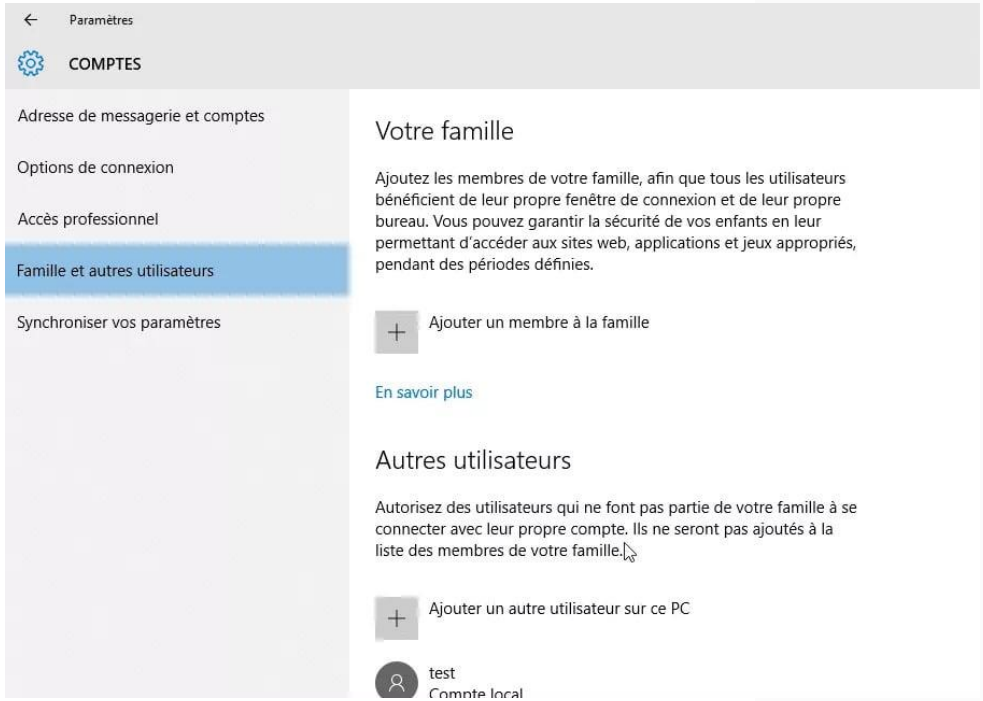
Compte invité
Aucun information n’est stocké sur le compte, tout est détruit lorsque vous fermez la session

Comptes Microsoft
Basés sur une adresse email Microsoft, ils permettent l’utilisation de services Microsoft dans Windows 10 (Outlook.com, Windows Store, OneDrive, etc). Les informations de ces comptes sont stockées, en ligne, dans le Cloud Microsoft. Vos documents du profil utilisateur Windows seront stockés sur OneDrive.



Command : netplwiz

Comptes utilisateurs

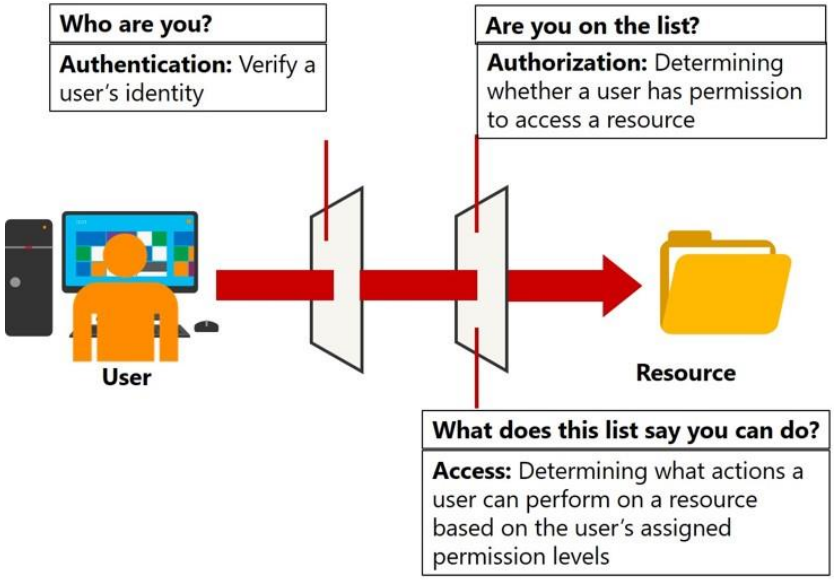


- **Votre famille** : vous créez des comptes et utilisateurs appartenant à votre famille, cela permet de dissocier les comptes adultes et enfants. Les comptes adultes peuvent modifier certains paramètres de contrôle parentaux.
- **Autres utilisateurs** : plutôt à destination des utilisateurs ne faisant pas parti de votre familles.

Comptes utilisateurs

Compte du domaine
Compte géré par Active Directory

Compte Azure AD
Compte géré par Azure Active Directory



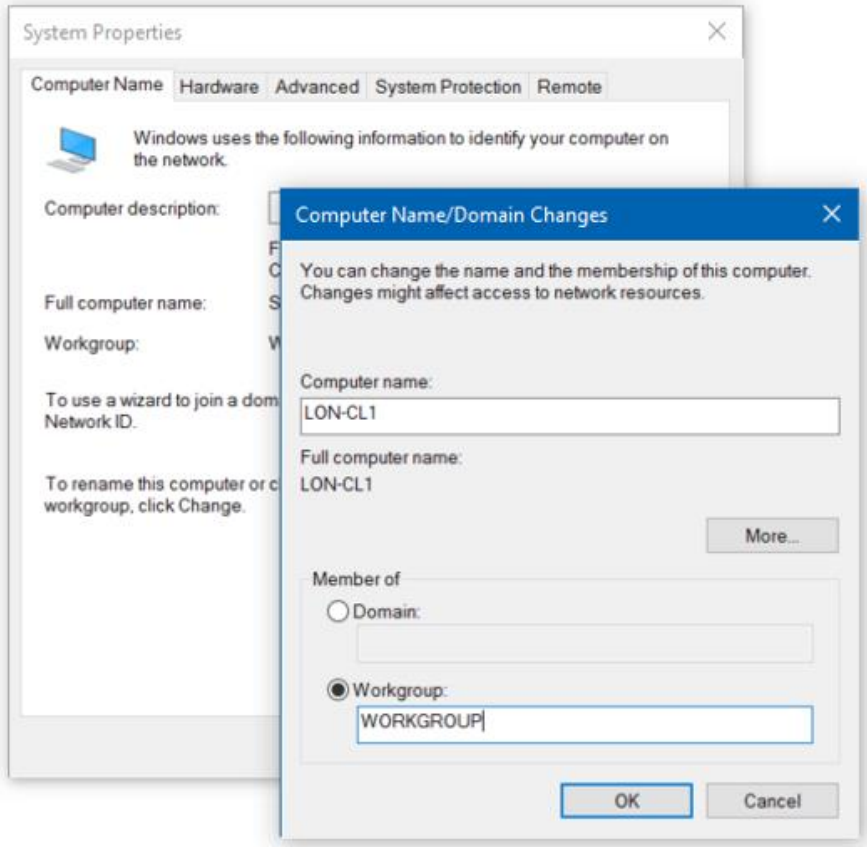
Domains et Workgroups

Workgroup

- Peer-to-peer
- Pas de gestion centralisée
- Max 20 ordinateurs

Domain

- Gestion centralisée
- Hiérarchie
- Evolutif
- Information stockée dans une base de données répliquée



Active Directory Users and Groups

- Active Directory groups
  - Distribution groups
  - Security Groups

Active Directory Overview

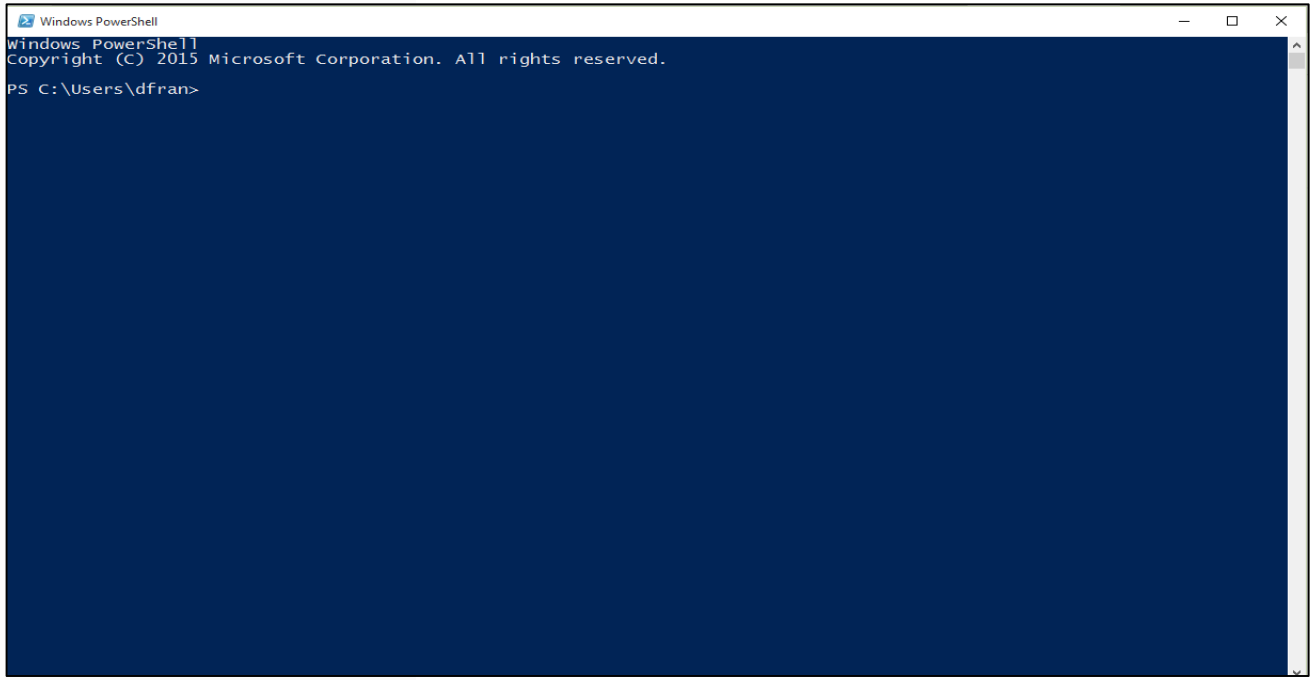
- Active Directory Domain Services (AD DS)
  - Installé sur un serveur Windows domain controller
  - Gestion des utilisateurs et des groupes
  - Fournit l'identité et le service d'authentication pour les périphériques et ressources partagées du domaine

- Azure Active Directory (Azure AD)
  - Cloud-based, aucune infrastructure
  - Gestion des utilisateurs et des groupes
  - Simplifie l'identification et le service d'authentication pour des périphériques du domaine et or domaine
  - Peut s'intégrer avec AD DS

Windows PowerShell

Windows PowerShell est un outil d'administration natif à Windows qui permet :

- L'integration de système d'exploitation
- La gestion de fonctionnalité à distance
- L'execution de script



Windows PowerShell

- Windows PowerShell est un shell command-line développé pour l'administration de système
  - Windows PowerShell fournit l'accès:
    - Système de fichier
    - Base de registre
    - Variables en mémoire
  - Cmdlets:
    - Forma verbe-nom
    - Gère des paramètres d'entrée
    - Exemple:

```
Start-Service –Name “Application Identity”
```

- L'utilisation de PowerShell permet d'effectuer des operations de masse efficace

Remote Commands in Windows PowerShell

- Remoting features of Windows PowerShell are built on Windows Remote Management

- Run an individual command or create a persistent connection or session to run a series of commands

- To enable remoting, use the following procedure:
- Verify the status of the Windows Remote Management service: Winrm quickconfig
- Enable remoting: Enable-PSremoting -force

Lab

- Exercice 1 – Prise en main de PowerShell (cf. Lab Microsoft)
- Exercice 2 – Création de la structure d'entreprise dans l'AD via PowerShell

Créer les comptes, groupes AD ainsi que les OU pour une petite entreprise comprenant les utilisateurs ci-dessous :

Nom	Prenom	Secteur
Mcclane	John	Directeur
Wick	John	Resp. Finance
Murphy	John	Resp. Vente
Doe	John	Resp. IT
Pignon	François	Comptable
Leblanc	Juste	Production

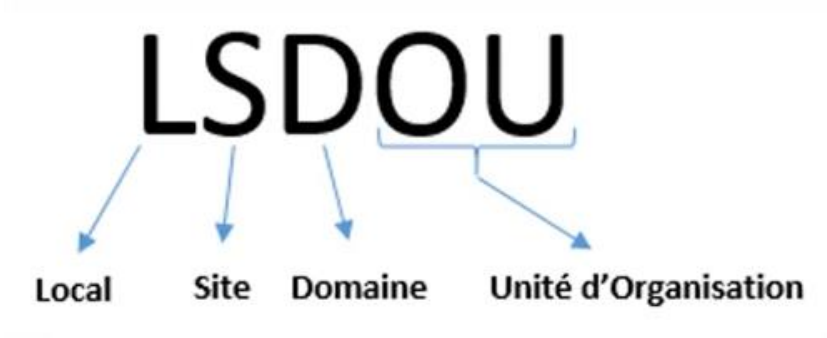
Group Policy Object (GPO)

Le but est de centraliser la gestion de l'environnement utilisateur et la configuration des machines. Cela permet d'appliquer des règles, des configurations ou de faire des déploiements sur un ensemble de postes.

Stratégie locale: Il est possible de configurer des paramètres GPO sur une machine hors domaine (workgroup) mais cela doit être fait machine par machine.

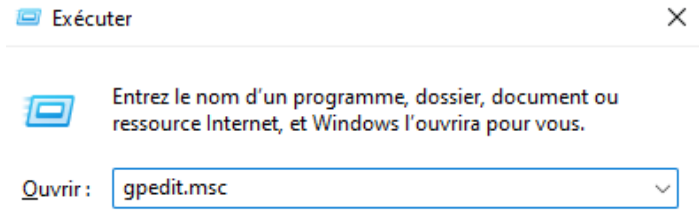
Stratégie Active Directory: Console unique pour gérer différentes GPO à appliquer sur un groupe de machines ou d'utilisateurs.

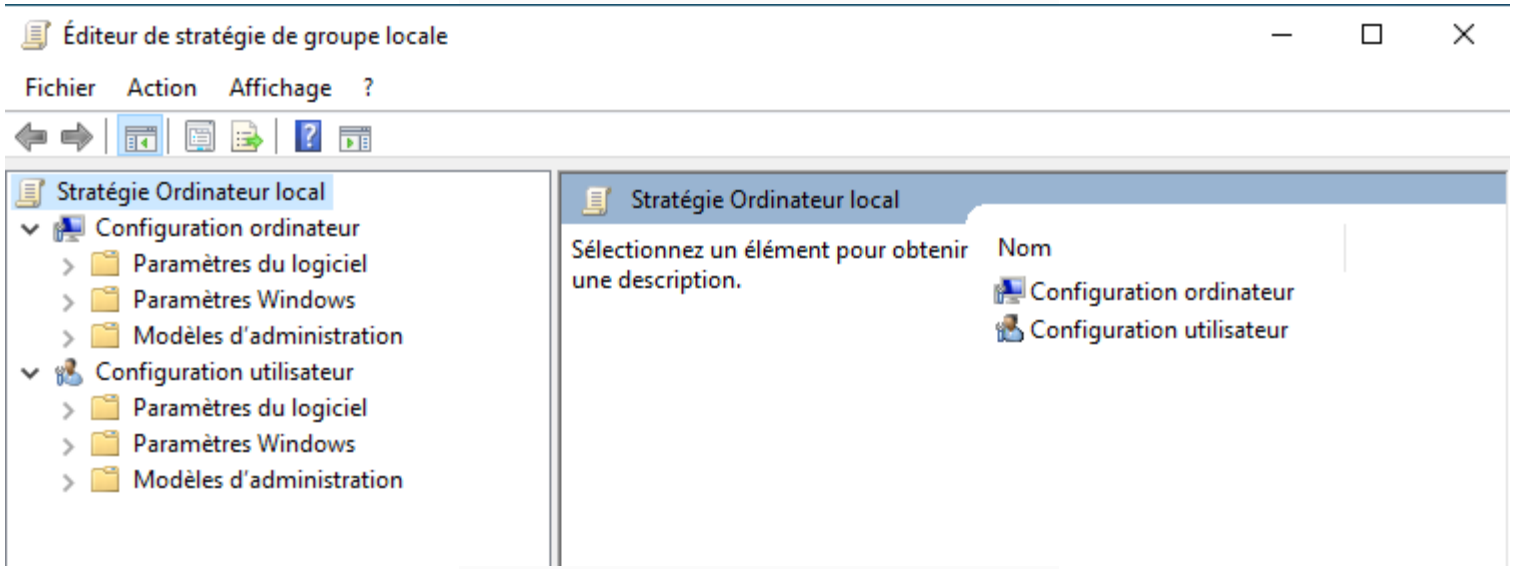
Ordre d'application:



Local Group Policy

La console pour éditer des stratégies locales est la console **GPEDIT.msc**



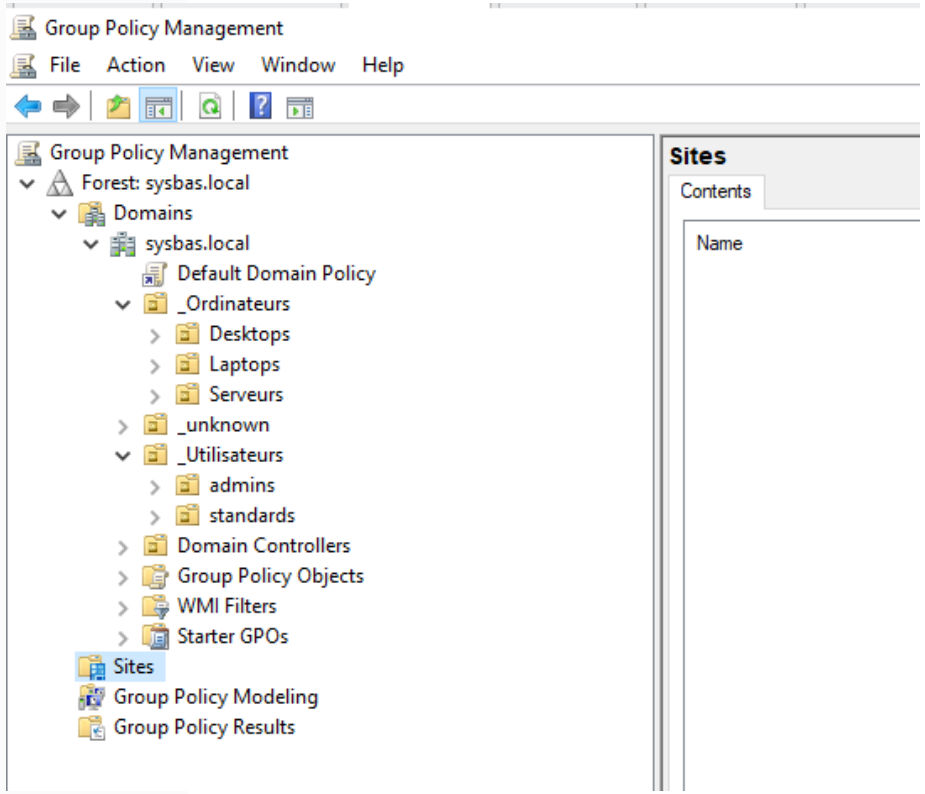


Group Policy Management Console

La console pour éditer des stratégies de groupe est la console **GPMC.msc**

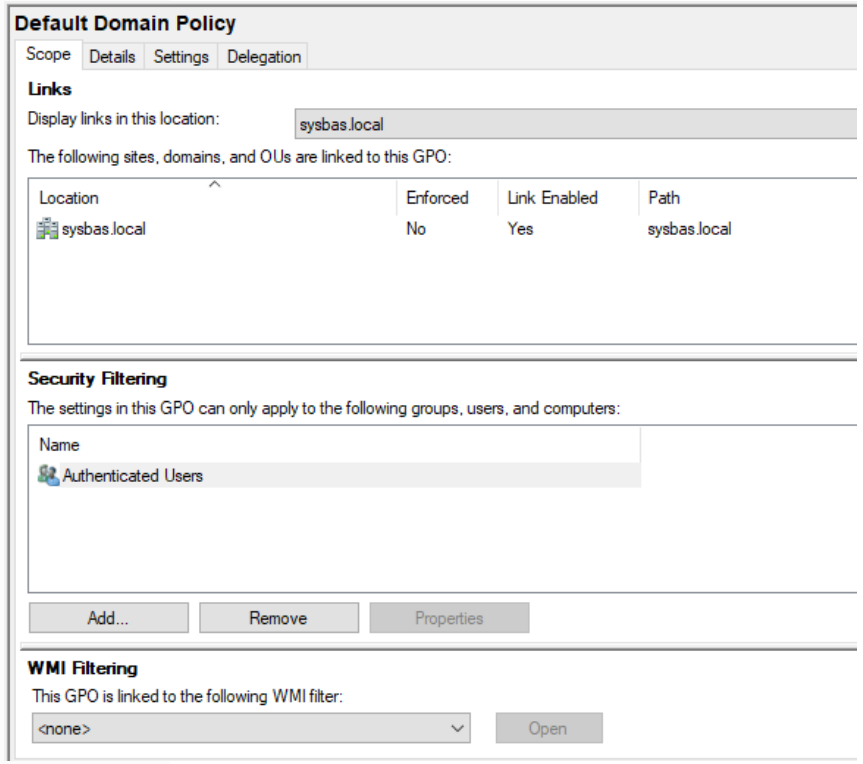
Il est possible d'installer la console GPMC sur un autre serveur ou un poste de travail, puis de se connecter à distance sur votre contrôleur de domaine. Les outils d'administration à distance sont disponibles en téléchargement sur le site de Microsoft, mais d'une version à l'autre le processus d'installation peut varier.

Télécharger RSAT sur le site Microsoft



Group Policy Management Console

- **Scope**: sert à afficher les objets avec lesquels est liée la GPO sélectionnée, ainsi que le filtrage de sécurité et l'éventuel filtre WMI associé. Il est à noter qu'une GPO peut être liée à une OU, sans qu'elle s'applique forcément puisque le lien en lui-même peut être désactivé
- **Details**: affiche la date de création de la GPO, la date de dernière modification, le propriétaire, le numéro de version, l'état de la GPO et sa description si elle existe.
- **Settings**: affiche tous les paramètres configurés au sein de la stratégie de groupe sélectionnée.
- **Delegation**: affiche les autorisations spécifiques sur cet objet GPO en matière d'administration.



Default policies

Default Domain Policy

Contient exclusivement des paramètres de sécurité, et notamment pour la gestion des comptes utilisateurs : stratégie de mot de passe et de verrouillage de compte. **Il est déconseillé de modifier la stratégie de groupe par défaut.**
Si vous souhaitez modifier l'un des paramètres : créez une nouvelle GPO pour le modifier.

Default Domain Controllers Policy

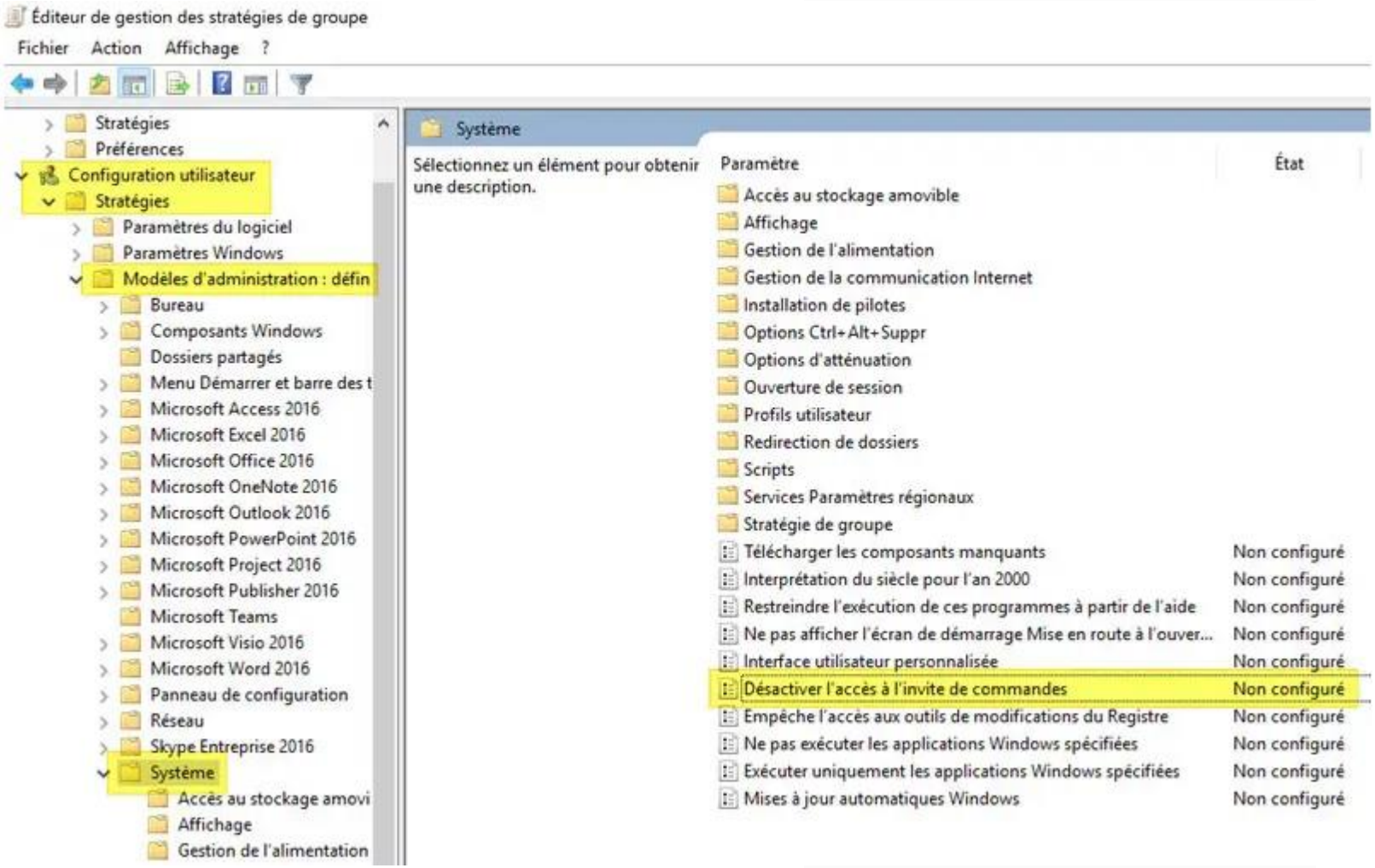
Cette GPO a pour objectif de sécuriser un minimum les serveurs ayant le rôle de contrôleur de domaine. Dès qu'un nouveau contrôleur de domaine est ajouté à votre environnement, il se retrouve dans l'OU "*Domain Controllers*" donc il va hériter des paramètres de sécurité de cette GPO.

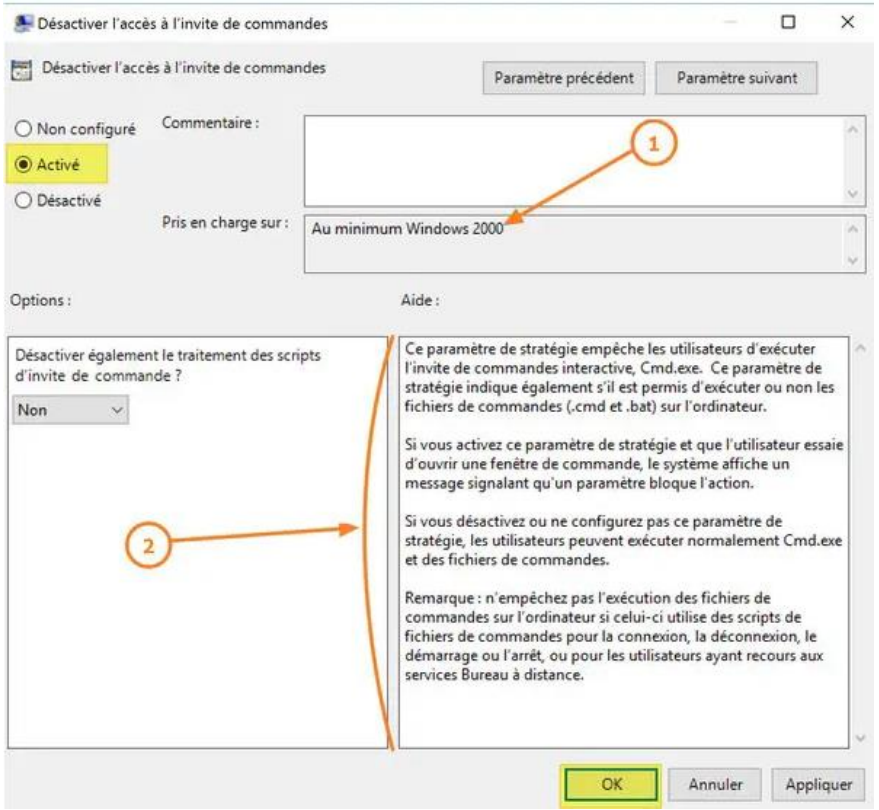
Parmi ces paramètres, nous retrouvons par exemple :
- Qui est autorisé à éteindre le serveur ?
- Qui est autorisé à ouvrir une session locale ?
- Qui est autorisé à modifier l'heure du système ?
- Qui est autorisé à gérer le journal d'audit et de sécurité ?
- Etc...

Lab

- Créer une GPO pour bloquer l’accès à l’invite de commande
- Appliquer la GPO au groupe des utilisateurs standard
- Tester la GPO
- Vérifier les GPO appliquées avec l’outil GPResult

Lab - solution

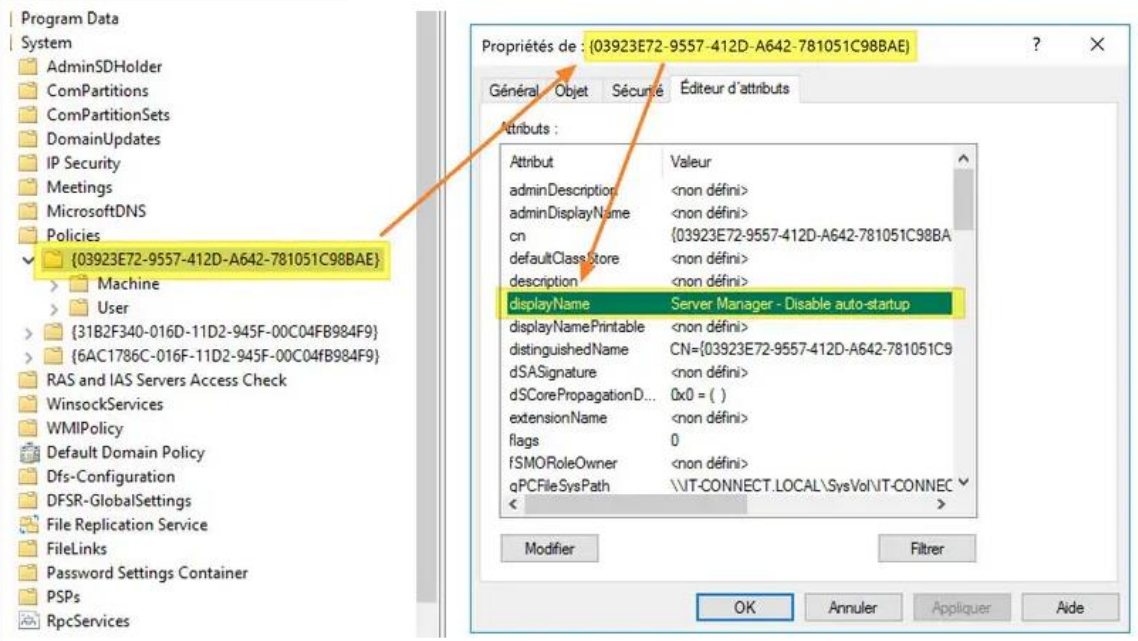




GPC / GPT / registre

Chaque GPO est reliée à un container de stratégie de groupe appelé "*Group Policy Container*" (GPC) stocké directement dans l'Active Directory et un modèle de stratégie de groupe appelé "*Group Policy Template*" (GPT) qui se présente sous la forme d'un ensemble de fichiers stockés dans le répertoire SYSVOL.

- GPC :



GPC / GPT / registre

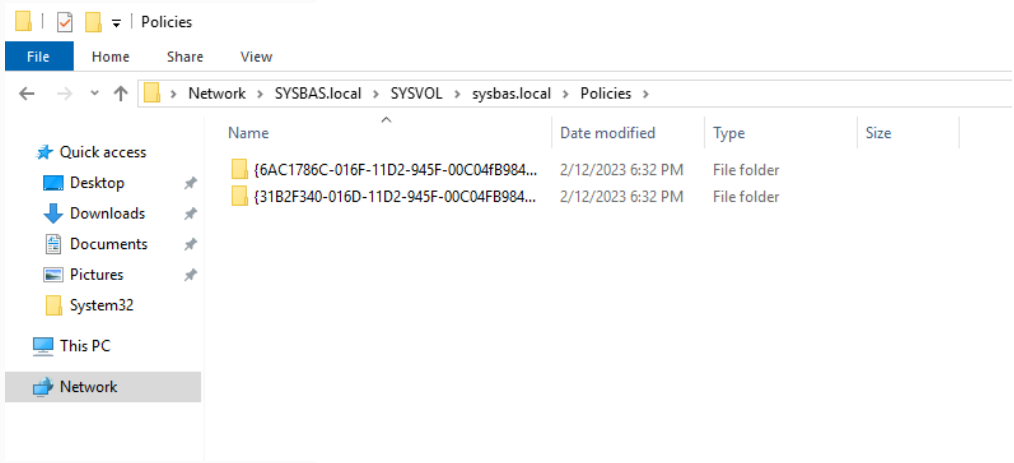
- GPT :

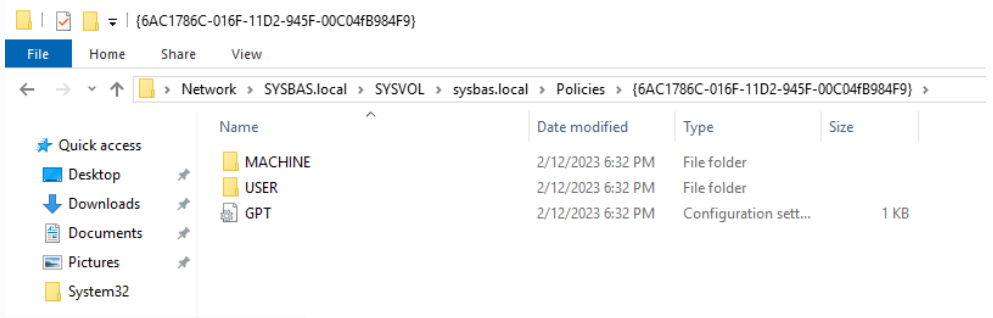
Identifiable avec un identifiant unique (GUID)

Stocké dans le SYSVOL

Utilisé pour stocker les fichiers de config de la GPO

Répliqué au travers de la réplication SYSVOL





- Certaine policy sont directement lié à une valeur dans la base de registre : https://gpsearch.azurewebsites.net/

ADMX / ADML

Les fichiers ADMX sont des template d’administration qui permettent d'ajouter des paramètres supplémentaires à l'éditeur de stratégie de groupe.

Windows Server est livré avec près de 200 fichiers ADMX. Des fichiers ADMX peuvent être importé pour permettre la gestion par GPO d’outils tel que Office, Chrome, etc.

Les fichiers ADML viennent en complément des templates d'administration (ADMX) afin de gérer la partie linguistique. Il s'agit ni plus ni moins que de fichiers de traduction.

Le magasin central

Le magasin central est un dossier qui est utilisé pour stocker les fichiers ADMX et ADML sur un domaine Active Directory.

Le magasin central inclus à Windows Server est stocké à l'emplacement suivant : C:\Windows\PolicyDefinitions, plus précisément il utilise une variable d'environnement : %systemroot%\PolicyDefinitions.

Tous les fichiers ADMX et ADML natifs à Windows Server sont stockés à cet endroit. Néanmoins ce dossier est local et il n'est pas répliqué entre les contrôleurs de domaine, il est donc nécessaire de le stocker dans un endroit sûr et répliqué sur tous les contrôleurs de domaine => \\SYSBAS.local\SYSVOL\sysbas.local\Policies\PolicyDefinitions.

Afin de pouvoir stocker les fichiers linguistiques (ADML), je vous invite à créer deux sous-dossiers :

en-US
fr-FR

Le magasin central

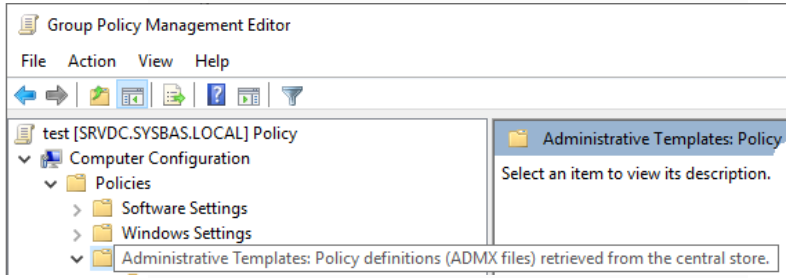
Les templates d'administration pour Windows 10 v1909 sont disponibles sur le site de Microsoft : ADMX Windows 10

Le téléchargement se présente sous la forme d'un fichier MSI, il faut réaliser l'installation sur un PC ou un serveur pour récupérer ensuite les fichiers ADMX et ADML.

Lorsque l'installation est réalisée, les fichiers sont disponibles à l'emplacement suivant :
C:\Program Files (x86)\Microsoft Group Policy\Windows 10 November 2019 Update (1909)\PolicyDefinitions

Copiez tous les fichiers ADMX, ainsi que les deux dossiers de langue "en-US" et "fr-fr" dans le dossier PolicyDefinitions. Pour rappel voici son emplacement :
\\sysbas.local\SYSVOL\ sysbas.local\Policies\PolicyDefinitions

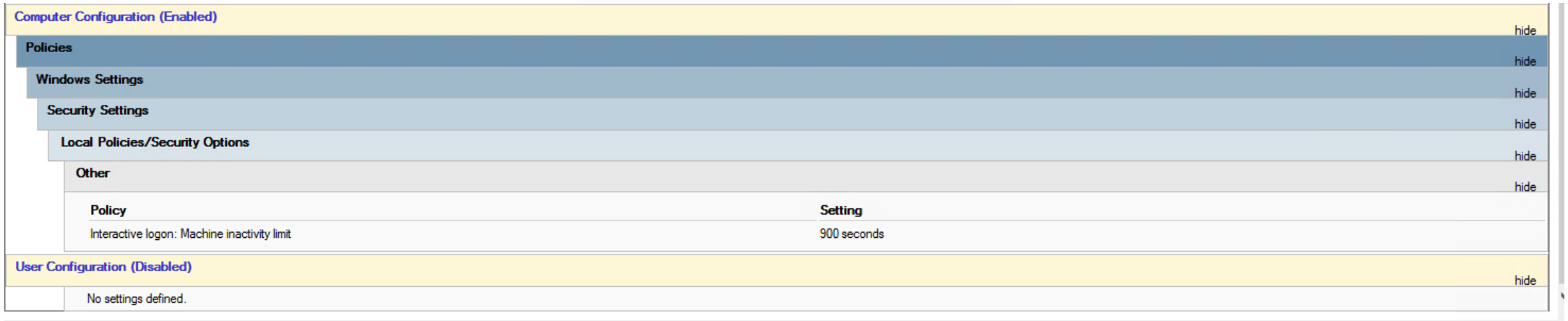
Si l'on déroule la partie "Configuration ordinateur" (ou Configuration utilisateur), on retrouve la partie "Modèles d'administration". Par défaut, dans cette partie nous retrouvons uniquement les modèles natifs et préchargés sur Windows Server. Désormais, dès que vous ajoutez des fichiers ADMX à votre dépôt centralisé, les paramètres de GPO viendront s'ajouter dans cette zone.



Lab

- Lock session after 15min
- Configurer favoris Edge + la page de démarrage
- Configurer favoris Chrome

Lab – Autolock



Lab – Edge (legacy) favorites

User Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

Microsoft Edge

Microsoft Edge/Startup, home page and new tab page

Windows Components/Microsoft Edge

Policy	Setting
Configure Favorites	Enabled

Enter the name of the favorite in the first column and the URL of the favorite in the other column like Contoso http://www.contoso.com/	
CFF	https://www.cff.ch
CPNE	https://www.cpne.ch

Policy	Setting
Configure Open Microsoft Edge With	Enabled
Configure Open Microsoft Edge With	Start page

Policy	Setting
Configure Start pages	Enabled
Use this format: <support.contoso.com><https://support.microsoft.com/>	https://edus2.rpn.ch

Lab – Edge Chromium favorites

Download & install ADMX for Microsoft Edge Chromium (here)

User Configuration (Enabled) hide

Policies hide

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the central store.

Microsoft Edge hide

Policy	Setting	Comment
Configure address bar editing	Enabled	
Configure favorites	Enabled	
Configure favorites	[{"toplevel_name": "Managed Favorites"},{"url": "https://edus2.rpn.ch","name": "EDUS2"},{"url": "https://www.cpne.ch","name": "CPNE"},{"url": "https://www.cff.ch","name": "CFF"},{"name":"Microsoft","children":[{"url": "https://www.microsoft.com","name": "Official website"},{"url": "https://learn.microsoft.com","name": "Learn"}]}]	

Policy	Setting	Comment
Enable favorites bar	Enabled	

Microsoft Edge/Startup, home page and new tab page hide

Policy	Setting	Comment
Action to take on startup	Enabled	
Action to take on startup	Open a new tab	

Policy	Setting	Comment
Configure the home page URL	Enabled	
Home page URL	https://www.edus2.rpn.ch	

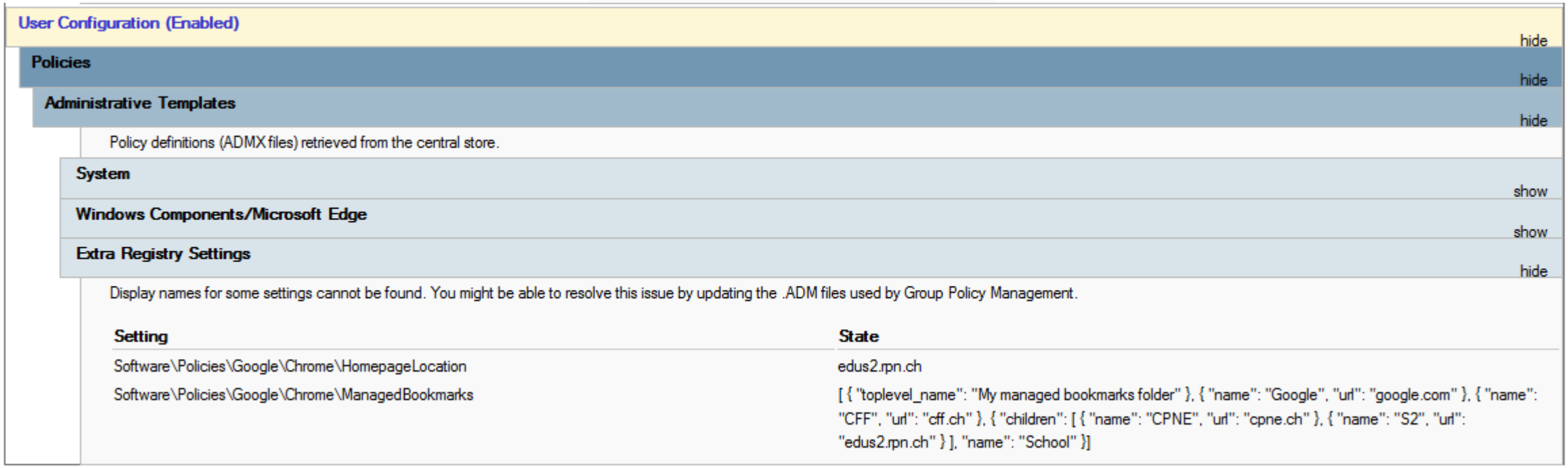
Policy	Setting	Comment
Configure the new tab page URL	Enabled	
New tab page URL	https://www.google.ch	

Policy	Setting	Comment
Show Home button on toolbar	Enabled	
Sites to open when the browser starts	Enabled	

Sites to open when the browser starts
https://www.cpne.ch

Lab – Chrome favorites

- Download and install AMDX files for Chrome in central store



Recap

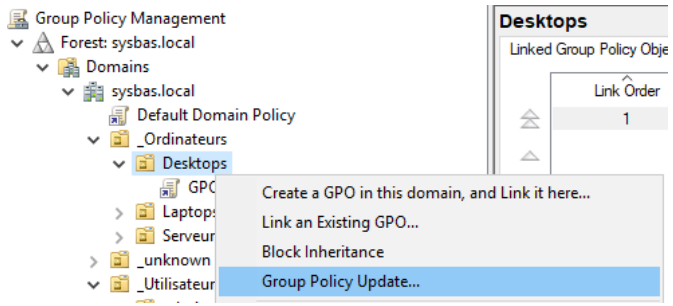
- Redirusr / redircmp
- Qu’est-ce qu’une GPO ?
- Ordre d’application de GPO ?
- Politique par défaut
- GPC / GPT
- Qu’est-ce que le magasin central (central store)

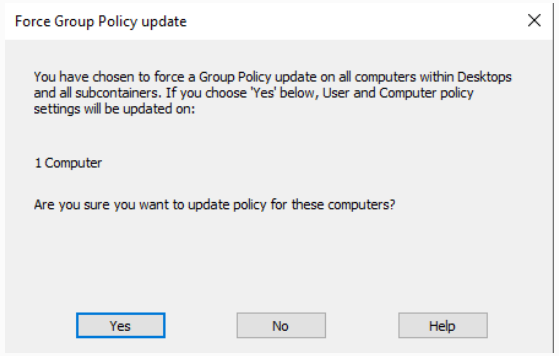
GPUPDATE

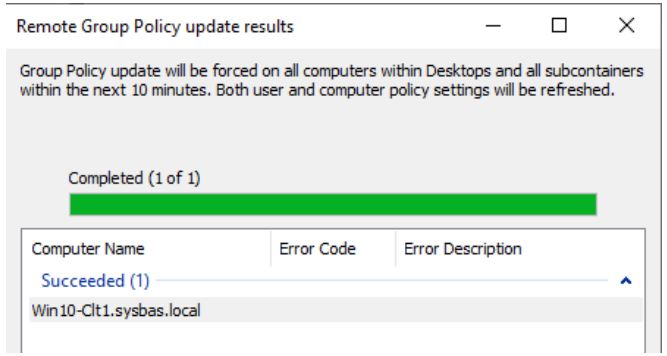
- Via command line : **gpupdate**

  gpupdate /force
  gpupdate /force:user
  gpupdate /force:computer

- Via GPMC :







- Via PowerShell:

```
Invoke-GPUpdate -Computer Win10-Clt1 -RandomDelayInMinutes 0
```

Filtres WMI

WMI : Windows Management Instrument

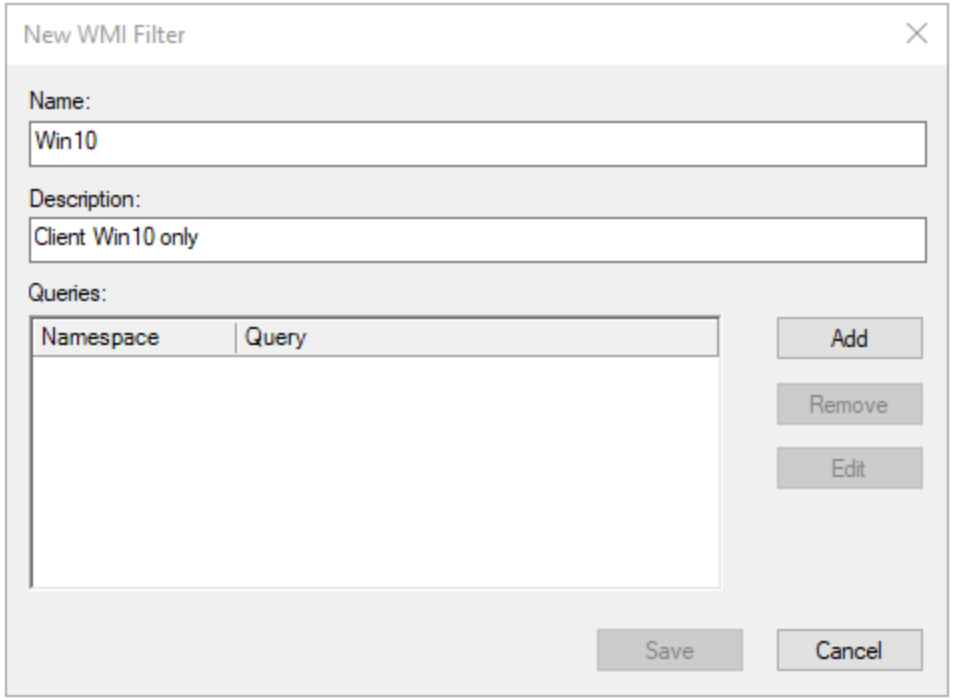
L'objectif est de filtrer les objets sur lesquels appliquer une GPO.
Par exemple : Type du système d'exploitation, type d'architecture (32 ou 64bits), nom de machine, etc.

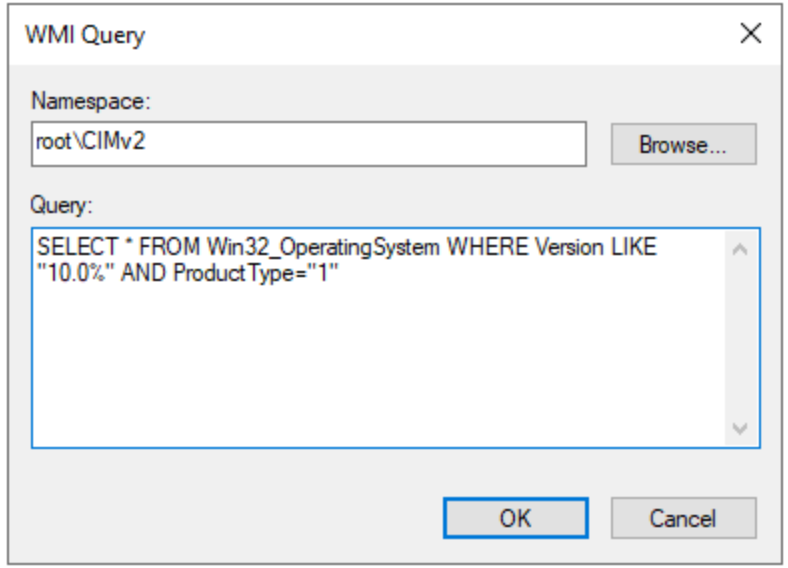
Syntaxe d'une requête WMI:

```
SELECT * FROM <classe WMI> WHERE <propriété> = <valeur>
SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0%" AND ProductType="1"
```

Résultat => Uniquement les clients Windows 10 seront retourné

Filtres WMI

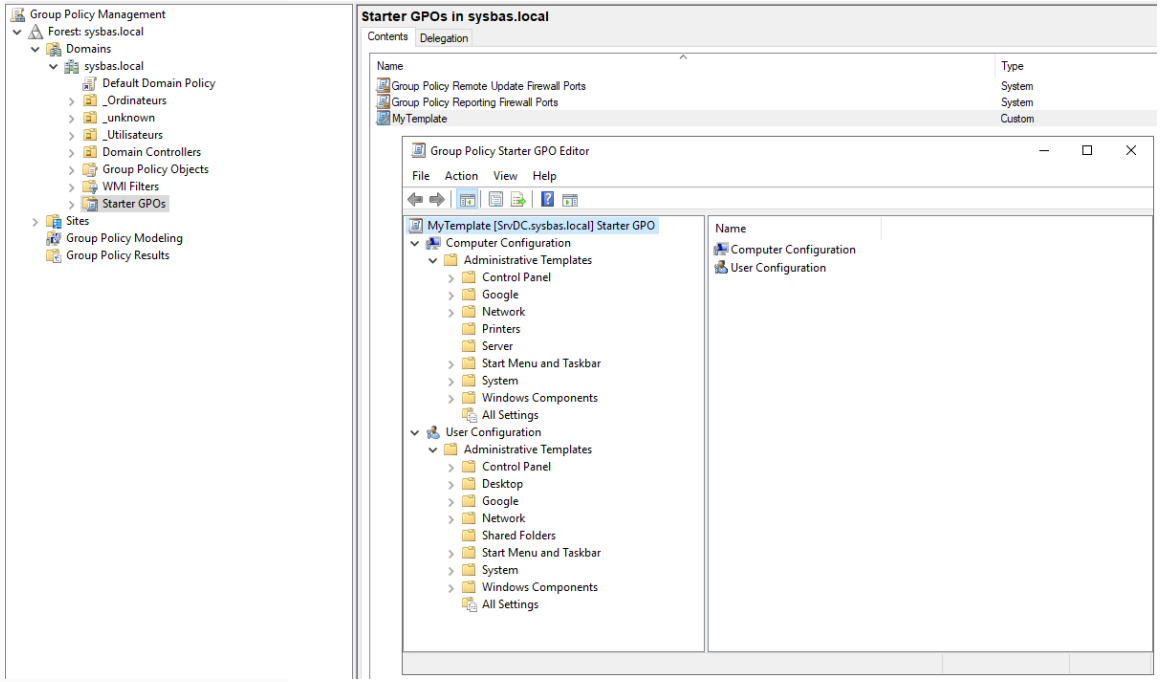

New WMI Filter
Name:
Win10
Description:
Client Win10 only
Queries:
Namespace
Query
Add
Remove
Edit
Save
Cancel


WMI Query
Namespace:
root\CIMv2
Browse...
Query:
SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0%" AND ProductType="1"
OK
Cancel

GPO Starter

Il s'agit d'une GPO qui va servir de point de départ pour créer une ou plusieurs autres GPO ; autrement dit il s'agit d'un template.

Note : si l'on utilise une GPO Starter pour créer une GPO, et que l'on modifie ensuite la GPO Starter, cela ne va pas remettre à jour automatiquement toutes les GPO qui ont utilisé ce template



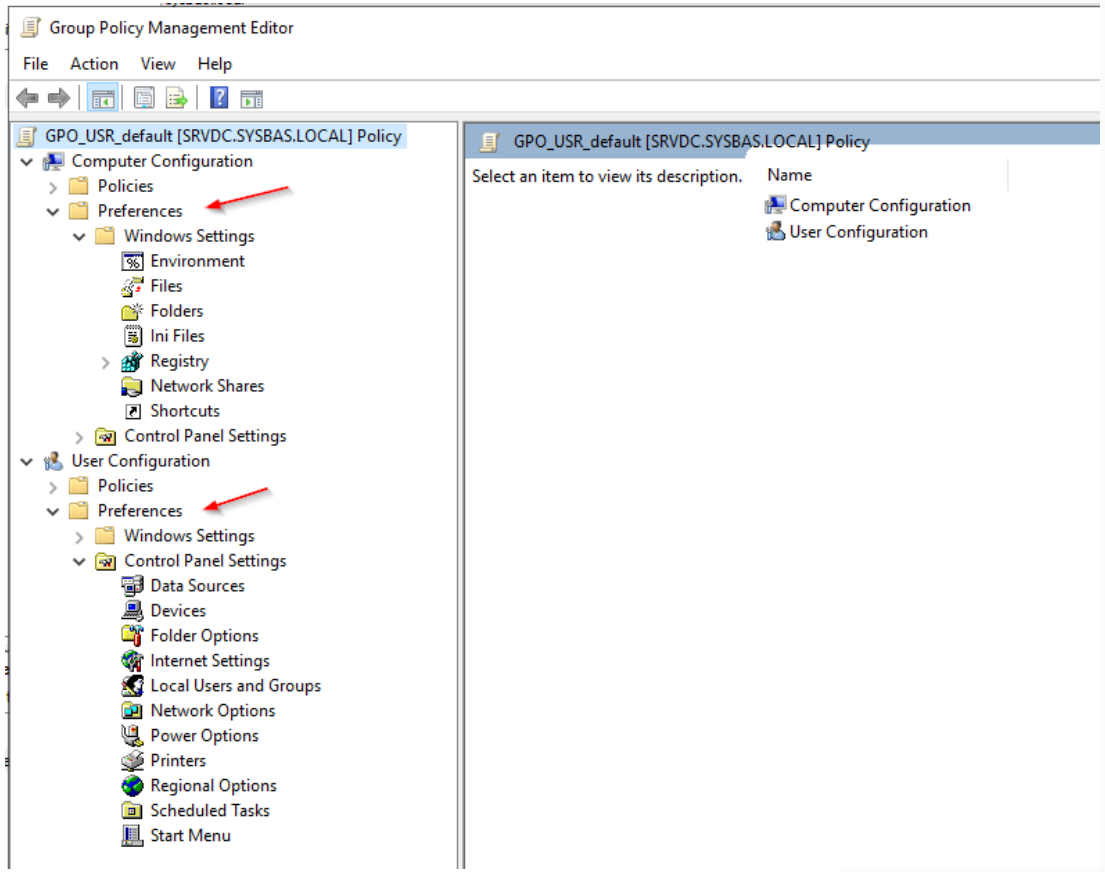
Group Policy Preference (GPP)

Pour rappel, lorsqu'un paramètre est défini dans une GPO et qu'il s'applique sur un utilisateur ou un poste, ce paramètre est forcé et ne peut pas être modifié par l'utilisateur.

Avec les préférences, c'est différent. Ces paramètres sont déployés, mais peuvent être modifiés.

Par défaut, si l'on **supprime une GPP qui s'applique sur un poste**, cela **ne supprime pas la configuration déployée par cette GPP**, contrairement aux paramètres classiques qui reviendraient à leur état initial

Group Policy Preference (GPP)



Voici quelques exemples de GPP :

- Déployer ou supprimer **une imprimante** sur la session d'un utilisateur
- Copier, écraser ou supprimer **un fichier** sur un ordinateur
- Créer un nouveau dossier ou supprimer **un dossier** existant
- Mapper **un lecteur réseau**
- Ajouter, modifier ou supprimer **une clé de registre**
- Créer un **nouveau raccourci** sur la session d'un utilisateur ou sur le "Bureau Public", par exemple
- Gérer **les variables d'environnement**
- Créer, supprimer et modifier **une tâche planifiée**
- Gérer **les utilisateurs et groupes locaux** d'un poste de travail

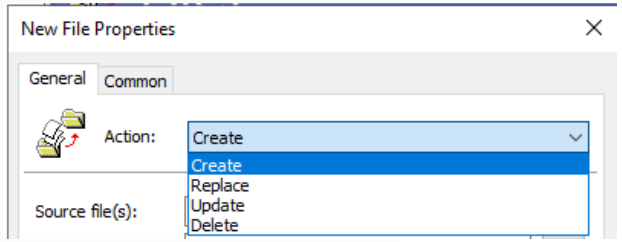
Group Policy Preference (GPP)

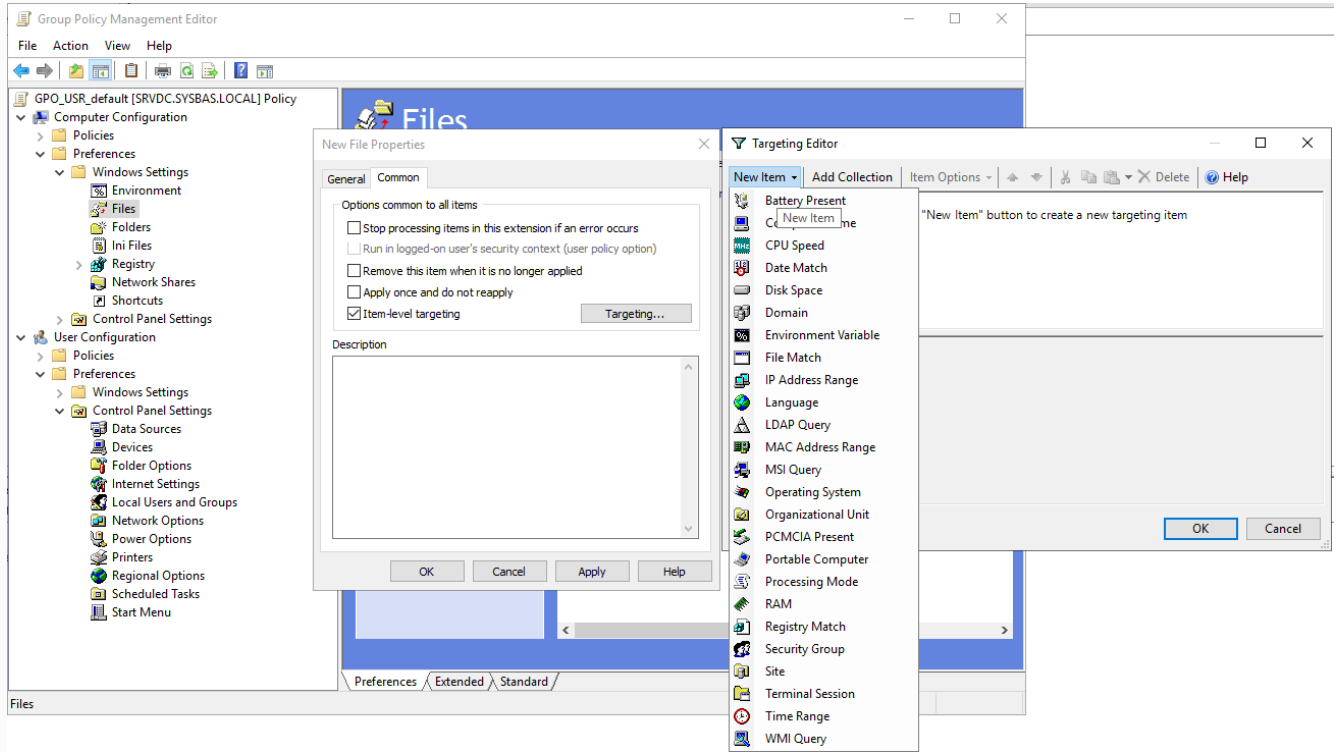
A la création, plusieurs choix sont possible :

- Créer
- Remplacer (supprimer, puis ajoute)
- Mettre à jour (création si pas existant)
- Supprimer

Le ciblage (accessible depuis l'onglet « commun ») permet une granularité bien plus évoluée qu'une GPO standard.

Attention néanmoins à ne pas mettre trop de critère car cela peux affecter les performances à l'utilisation.



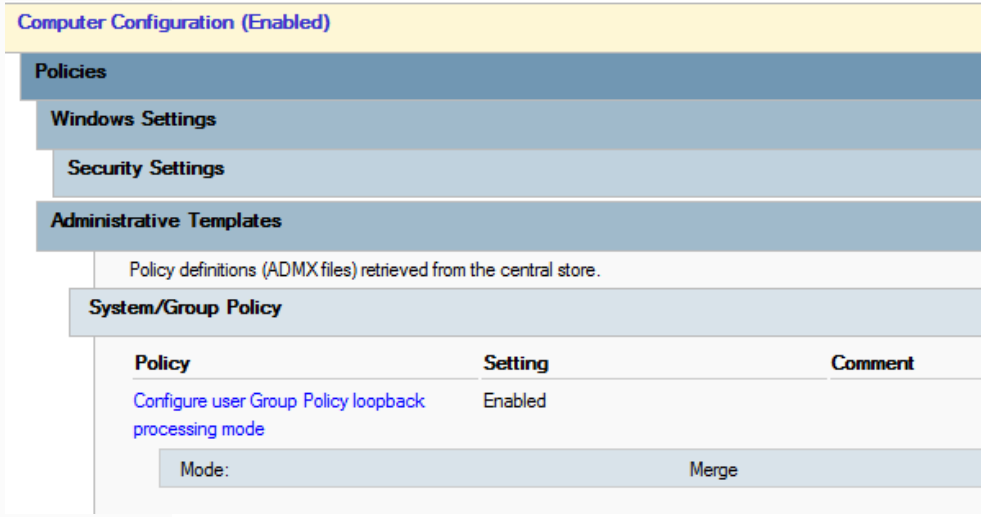


Loopback processing

Le Loopback processing permet de faire en sorte que les paramètres qui s'appliquent sur l'utilisateur ne sont pas ceux appliqués sur l'objet utilisateur directement, mais ceux appliqués au niveau de l'objet ordinateur.

Lorsque l'on active « loopback processing » dans la GPO, il y a deux choix:

- **Remplacer (replace)** : les paramètres "utilisateurs" de la GPO ordinateur remplacent ceux de la GPO utilisateur, complètement.
- **Fusionner (merge)** : les paramètres "utilisateurs" des deux GPO sont fusionnés. S'il y a un conflit, c'est la valeur de la GPO qui s'applique sur l'ordinateur qui l'emporte.

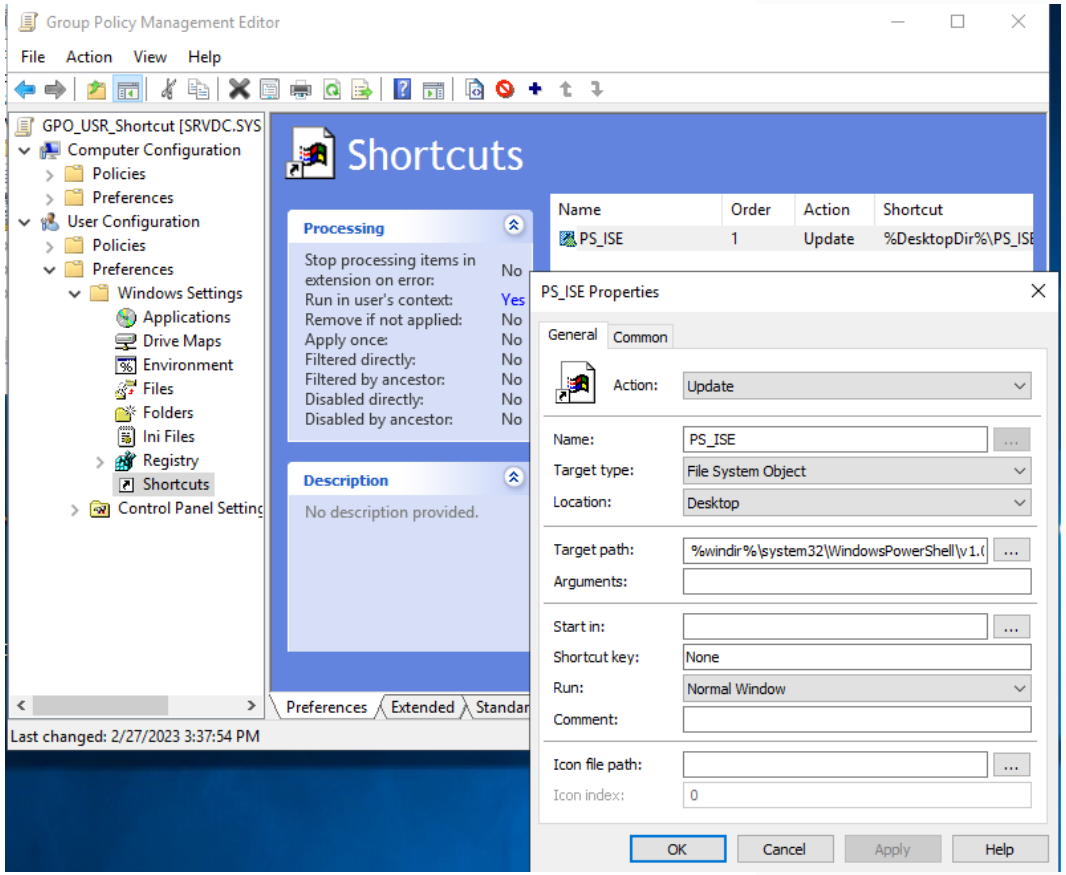


Lab

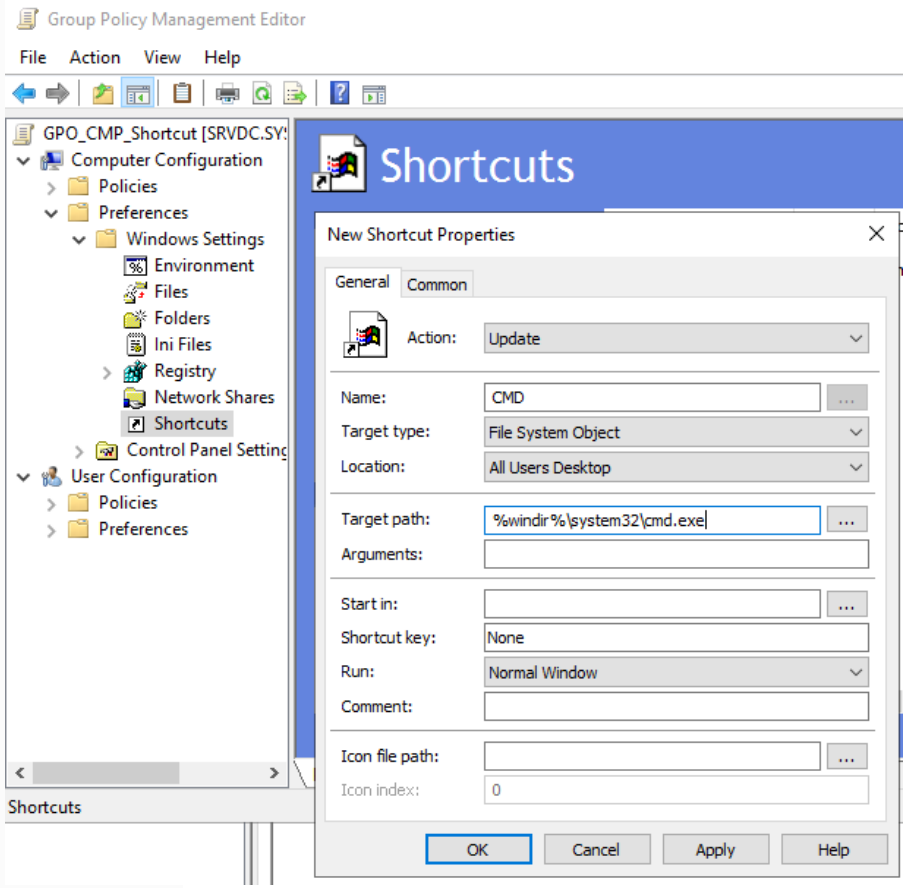
- Déployer un raccourci sur le bureau de l'utilisateur en cours
- Mapper un partage réseau (\\SrvFS\Dept) sur la lettre Z:\
- Retirer l'onglet sécurité des propriétés des fichiers dans l'explorateur de fichier
- Déployer un raccourci sur le bureau pour tous les utilisateurs
- Définir Chrome comme navigateur par défaut
- Eteindre l'ordinateur à 21h
- Désactiver «Server Manager au login»
- Personnaliser le menu démarrer
- Désactiver CTRL+ALT+DEL pour afficher l'écran de login

Lab - Shortcuts

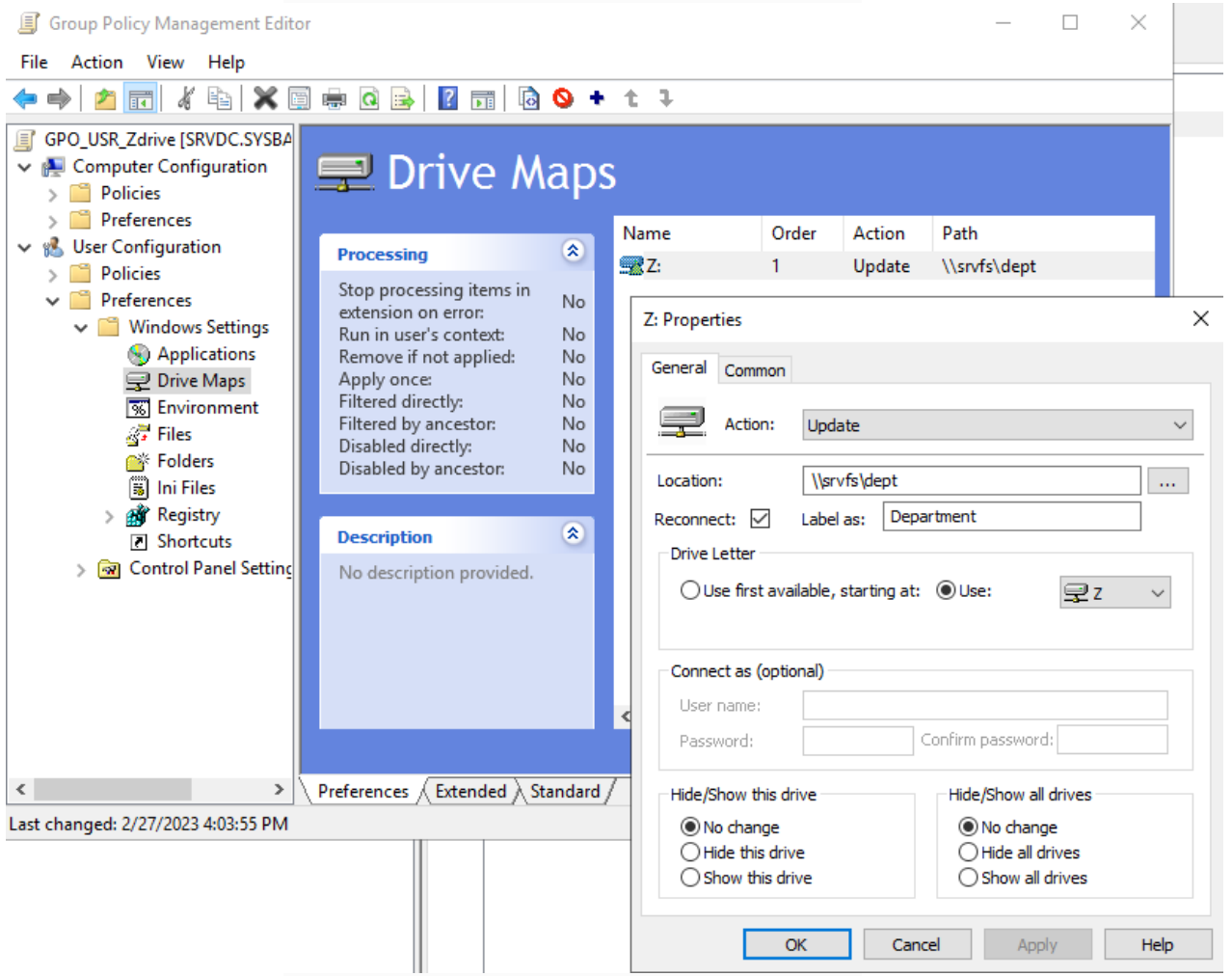
GPO User :



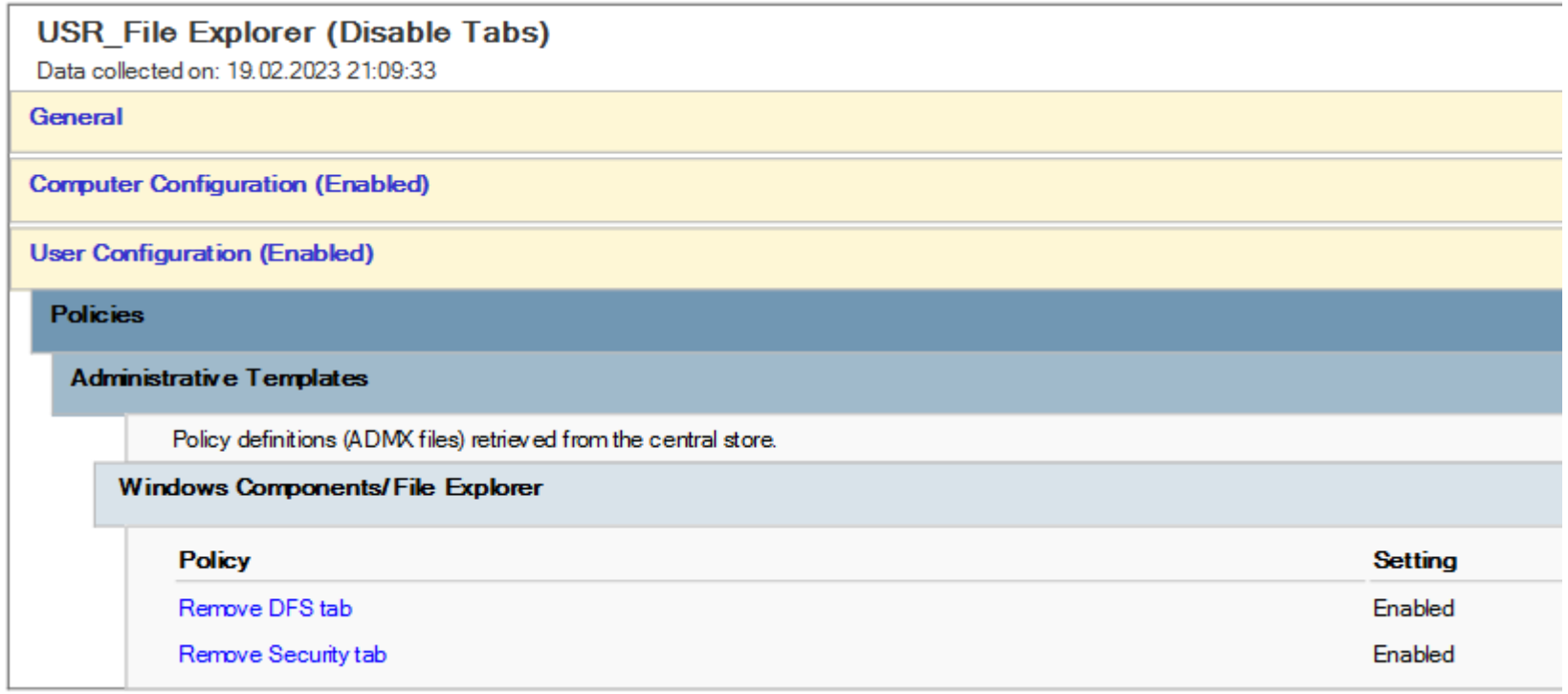
GPO Computer :



Lab – Mapped drive



Lab – Remove tabs



USR_File Explorer (Disable Tabs)

Data collected on: 19.02.2023 21:09:33

General

Computer Configuration (Enabled)

User Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

Windows Components/File Explorer

Policy	Setting
Remove DFS tab	Enabled
Remove Security tab	Enabled

Lab – Chrome by default

Créer un fichier XML d'association d'extension (template disponible sur internet)

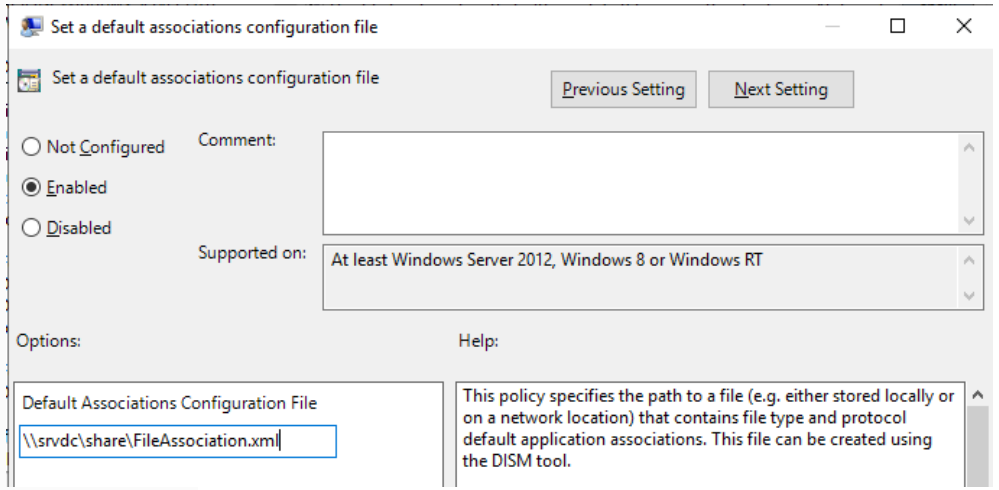
```
<?xml version="1.0" encoding="UTF-8"?>
<DefaultAssociations>
<Association Identifier=".htm" ProgId="ChromeHTML" ApplicationName="Google Chrome"/>
<Association Identifier=".html" ProgId="ChromeHTML" ApplicationName="Google Chrome"/>
<Association Identifier="http" ProgId="ChromeHTML" ApplicationName="Google Chrome"/>
<Association Identifier="https" ProgId="ChromeHTML" ApplicationName="Google Chrome"/>
</DefaultAssociations>
```

Enregistrer le fichier dans un partage (lecture seule)

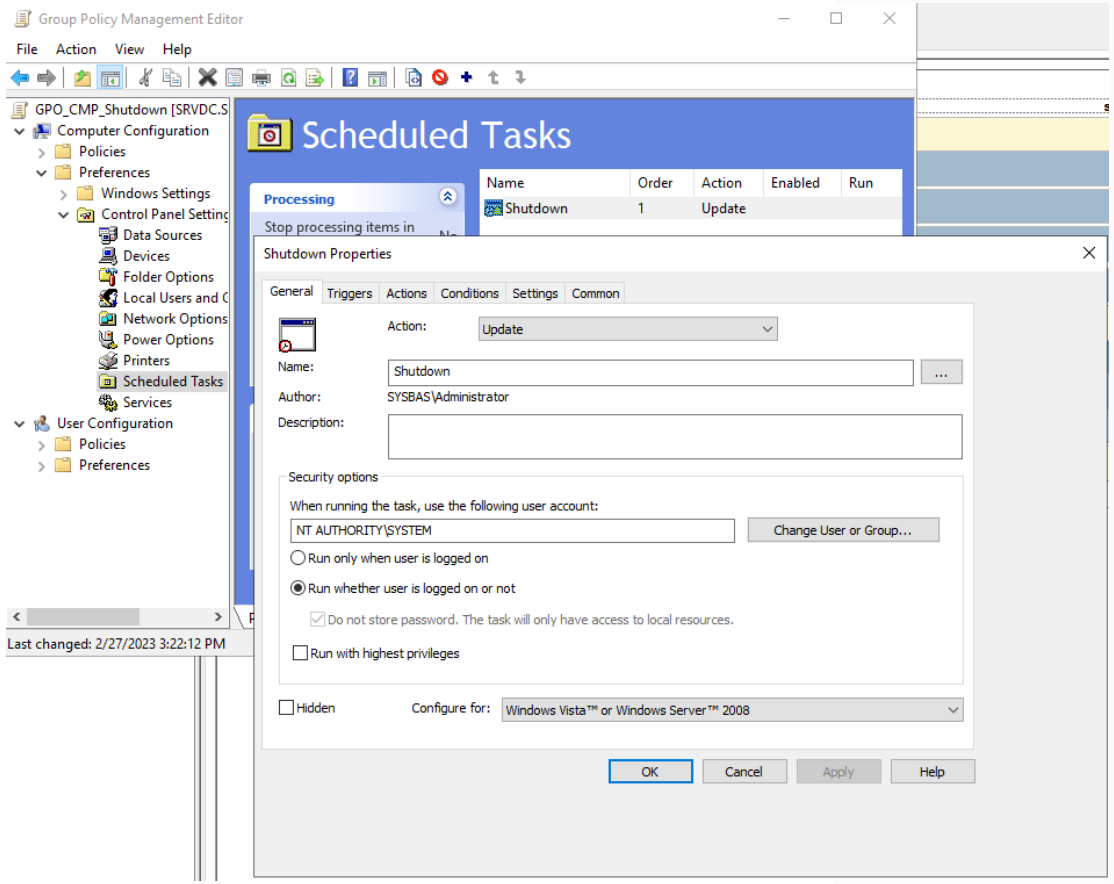
Créer la GPO :

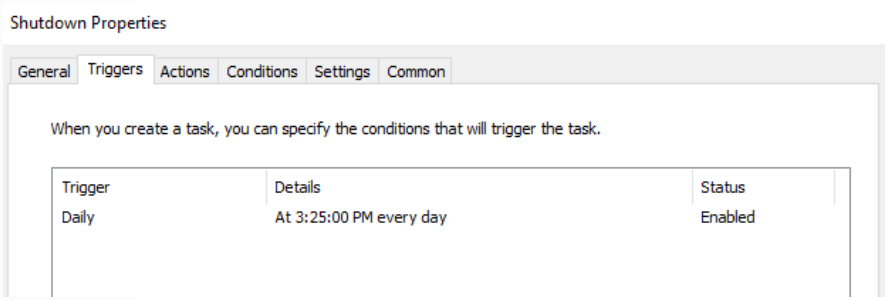
Computer configuration -> Policies -> Administrative Templates
-> Windows Components -> File Explorer
-> Set a default associations configuration file

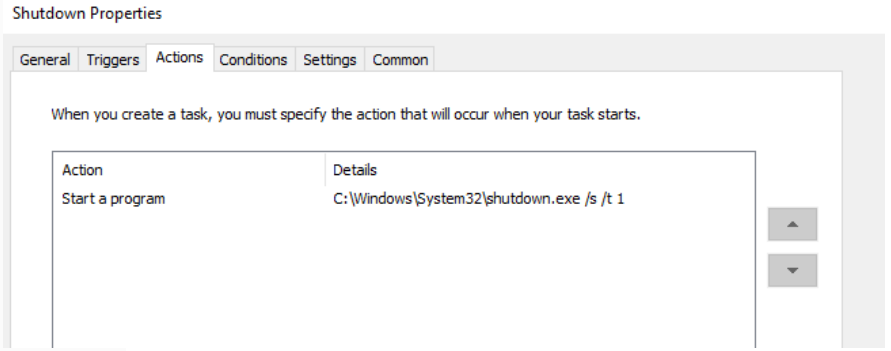
Reboot (Computer GPO)



Lab - Shutdown







Lab – Customize Server

CMP_Configuration (SRV)

Data collected on: 19.02.2023 21:10:33

General

Computer Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

System/ Server Manager

Policy	Setting
Do not display Server Manager automatically at logon	Enabled

Windows Components/Data Collection and Preview Builds

Policy	Setting
Allow Diagnostic Data	Enabled
	Diagnostic data off (not recommended)

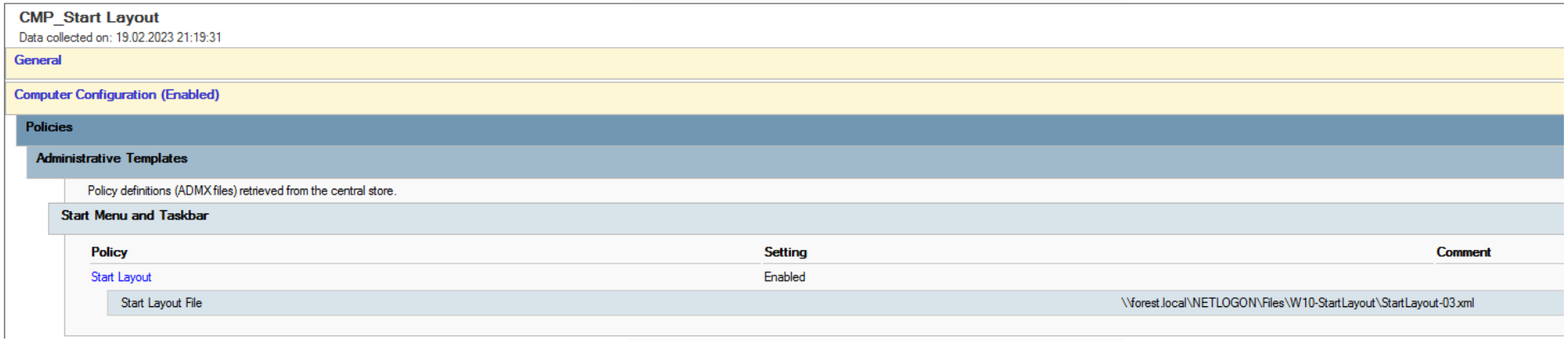
Policy	Setting
Do not show feedback notifications	Enabled

Windows Components/Windows Error Reporting

Policy	Setting
Disable Windows Error Reporting	Enabled

User Configuration (Enabled)

Lab – Start layout



CMP_Start Layout

Data collected on: 19.02.2023 21:19:31

General

Computer Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

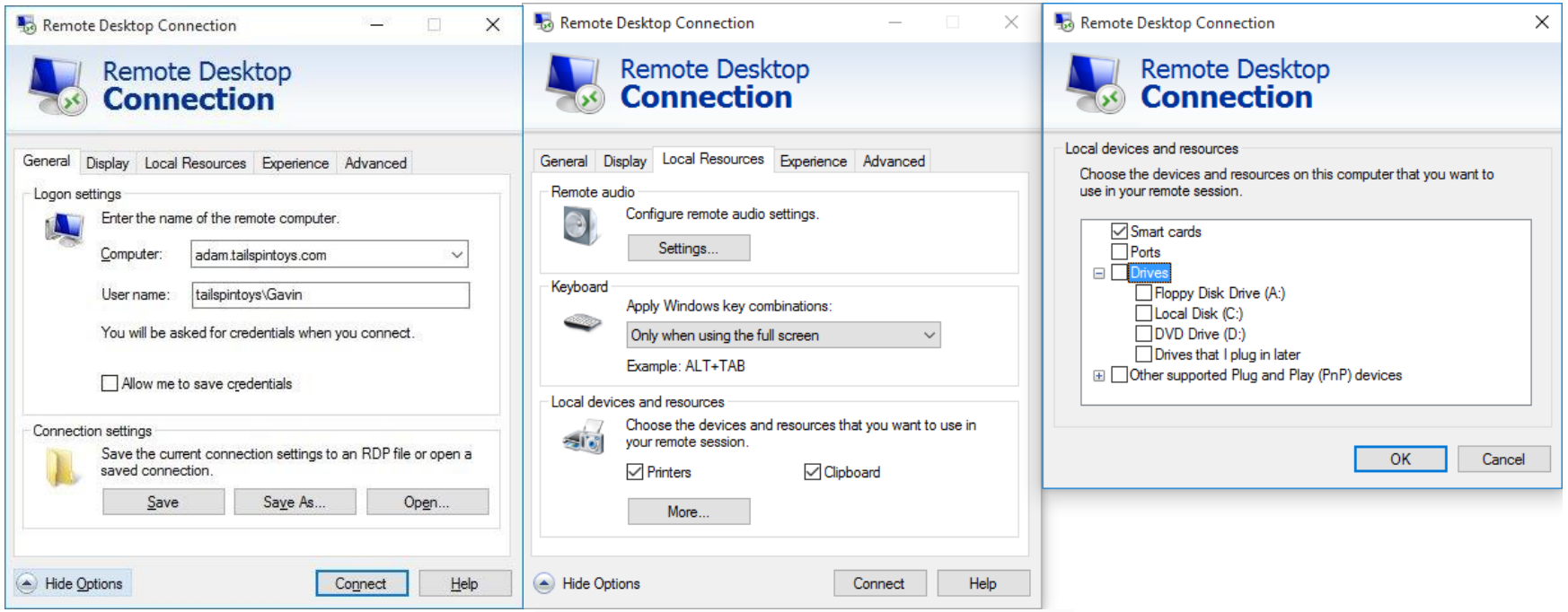
Start Menu and Taskbar

Policy	Setting	Comment
Start Layout	Enabled	
Start Layout File	\\forest.local\NETLOGON\Files\W10-StartLayout\StartLayout-03.xml	

```
<LayoutModificationTemplate xmlns:defaultlayout="http://schemas.microsoft.com/Start/2014/FullDefaultLayout"
xmlns:start="http://schemas.microsoft.com/Start/2014/StartLayout" Version="1"
xmlns="http://schemas.microsoft.com/Start/2014/LayoutModification">
 <LayoutOptions StartTileGroupCellWidth="6" />
 <DefaultLayoutOverride LayoutCustomizationRestrictionType="OnlySpecifiedGroups">
  <StartLayoutCollection>
   <defaultlayout:StartLayout GroupCellWidth="6">
    <start:Group Name="">
     <start:DesktopApplicationTile Size="2x2" Column="0" Row="0" DesktopApplicationID="Microsoft.Windows.Computer" />
    </start:Group>
   </defaultlayout:StartLayout>
  </StartLayoutCollection>
 </DefaultLayoutOverride>
</LayoutModificationTemplate>
```

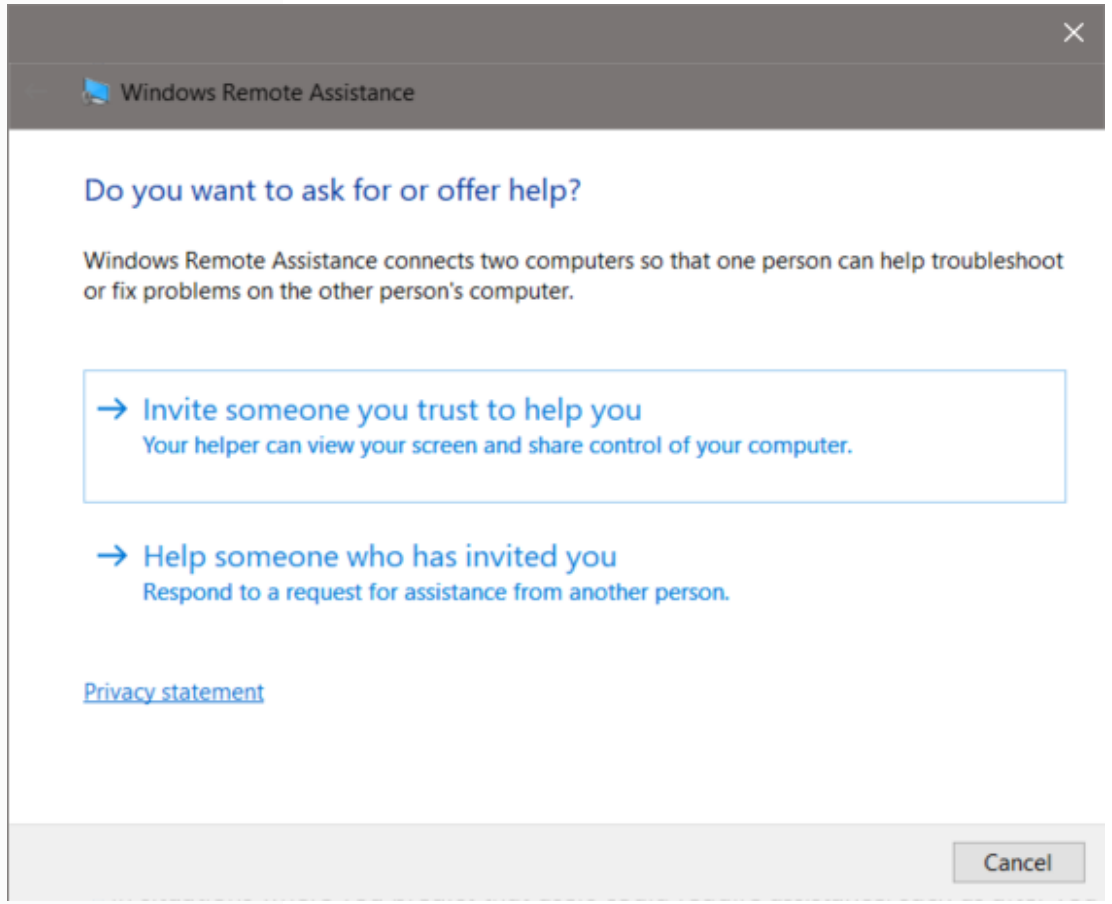
Remote Desktop

- Solution native à Windows pour permettre de se connecter à des ordinateurs distant via le protocol RDP (Remote Desktop Protocol) sur le port TCP 3389
- Utilisé par les administrateurs pour se connecter à distance à des fins d'administration



Remote Assistance

- Remote Assistance permet :
  - Visualiser l’écran à distance
  - Créer une session chat
  - Contrôler l’ordinateur distant



Lab – Exemples

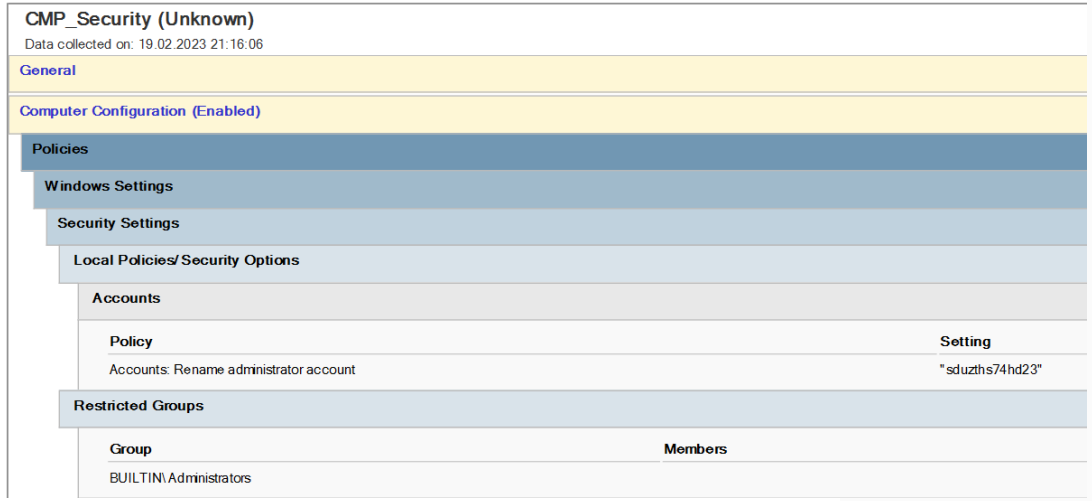
Exercice 1 : Isoler des machines suspecte
Créer une OU « Isolation »
Créer une GPO pour activer le firewall et bloquer tout le traffic entrant/sortant
Créer une GPO pour changer l'admin local

Exercice 2 : Configure RDP on Win10 clients

Exercice 3 : Remote Desktop Server
Bloquer l'accès au panneau de contrôle

Lab – isolate PC

- Enable Firewall
- Block all traffic (inbound/outbound)
- Rename administrator account



CMP_Security (Unknown)

Data collected on: 19.02.2023 21:16:06

General

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

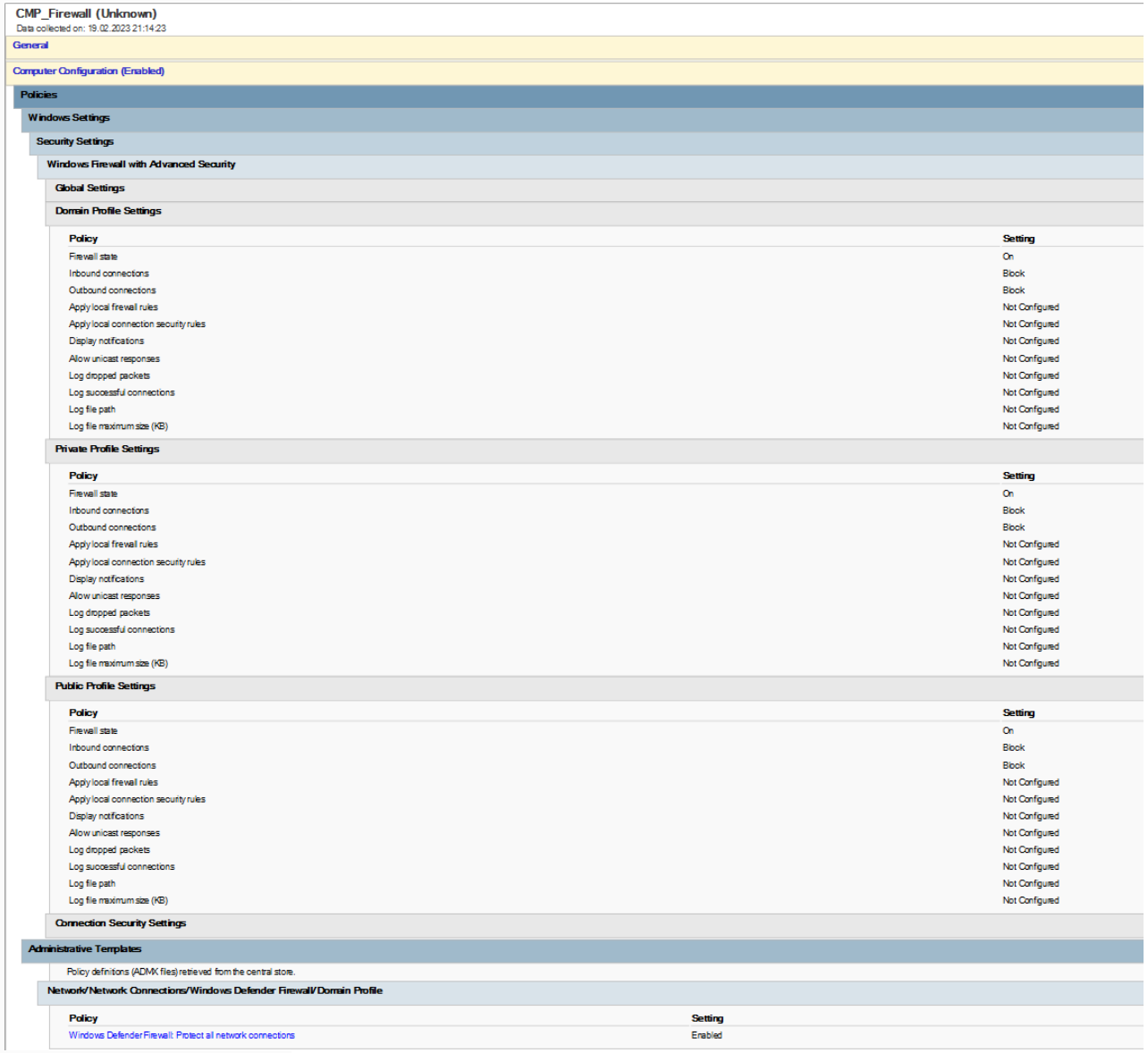
Local Policies/Security Options

Accounts

Policy	Setting
Accounts: Rename administrator account	"sduzths74hd23"

Restricted Groups

Group	Members
BUILTIN\Administrators	



CMP_Firewall (Unknown)

Data collected on: 19.02.2023 21:14:23

General

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Windows Firewall with Advanced Security

Global Settings

Domain Profile Settings

Policy	Setting
Firewall state	On
Inbound connections	Block
Outbound connections	Block
Apply local firewall rules	Not Configured
Apply local connection security rules	Not Configured
Display notifications	Not Configured
Allow unicast responses	Not Configured
Log dropped packets	Not Configured
Log successful connections	Not Configured
Log file path	Not Configured
Log file maximum size (KB)	Not Configured

Private Profile Settings

Policy	Setting
Firewall state	On
Inbound connections	Block
Outbound connections	Block
Apply local firewall rules	Not Configured
Apply local connection security rules	Not Configured
Display notifications	Not Configured
Allow unicast responses	Not Configured
Log dropped packets	Not Configured
Log successful connections	Not Configured
Log file path	Not Configured
Log file maximum size (KB)	Not Configured

Public Profile Settings

Policy	Setting
Firewall state	On
Inbound connections	Block
Outbound connections	Block
Apply local firewall rules	Not Configured
Apply local connection security rules	Not Configured
Display notifications	Not Configured
Allow unicast responses	Not Configured
Log dropped packets	Not Configured
Log successful connections	Not Configured
Log file path	Not Configured
Log file maximum size (KB)	Not Configured

Connection Security Settings

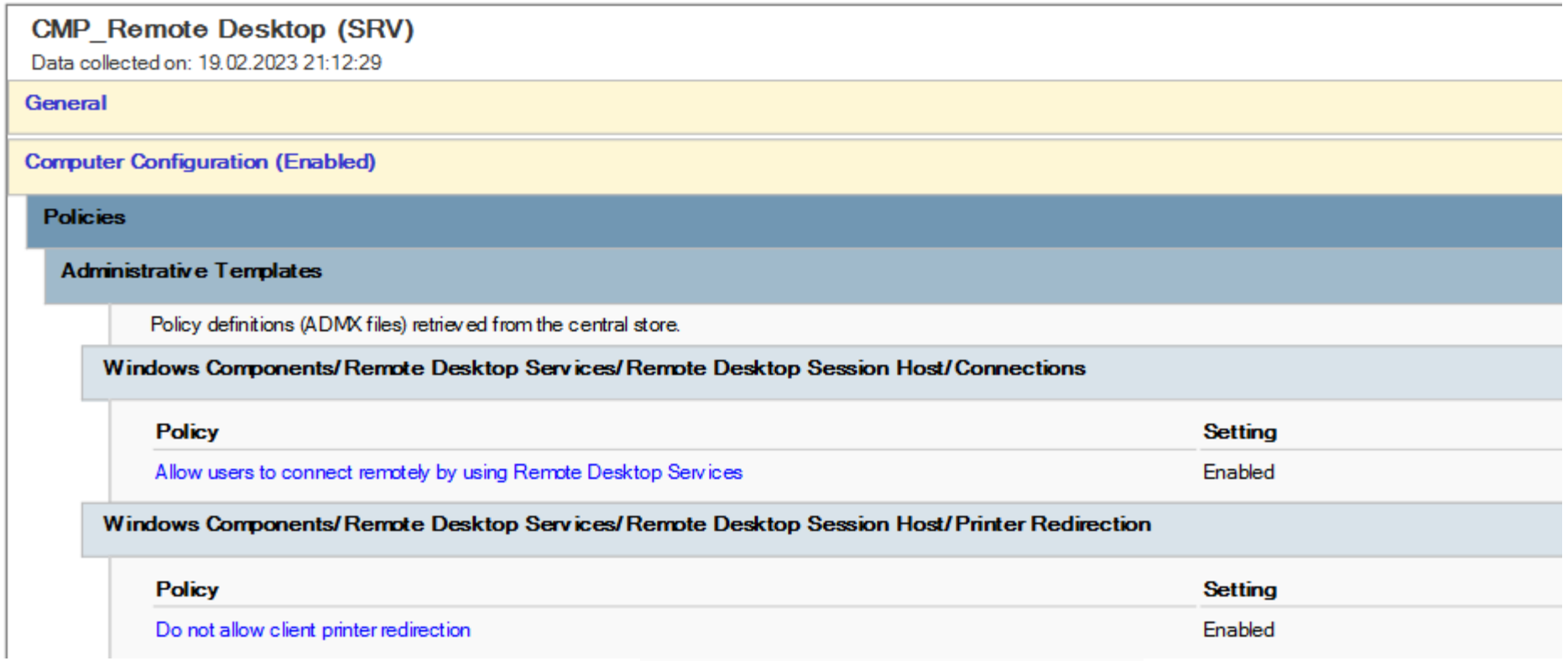
Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

Network/Network Connections/Windows Defender Firewall/Domain Profile

Policy	Setting
Windows Defender Firewall: Protect all network connections	Enabled

Lab – Remote Desktop



CMP_Remote Desktop (SRV)

Data collected on: 19.02.2023 21:12:29

General

Computer Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

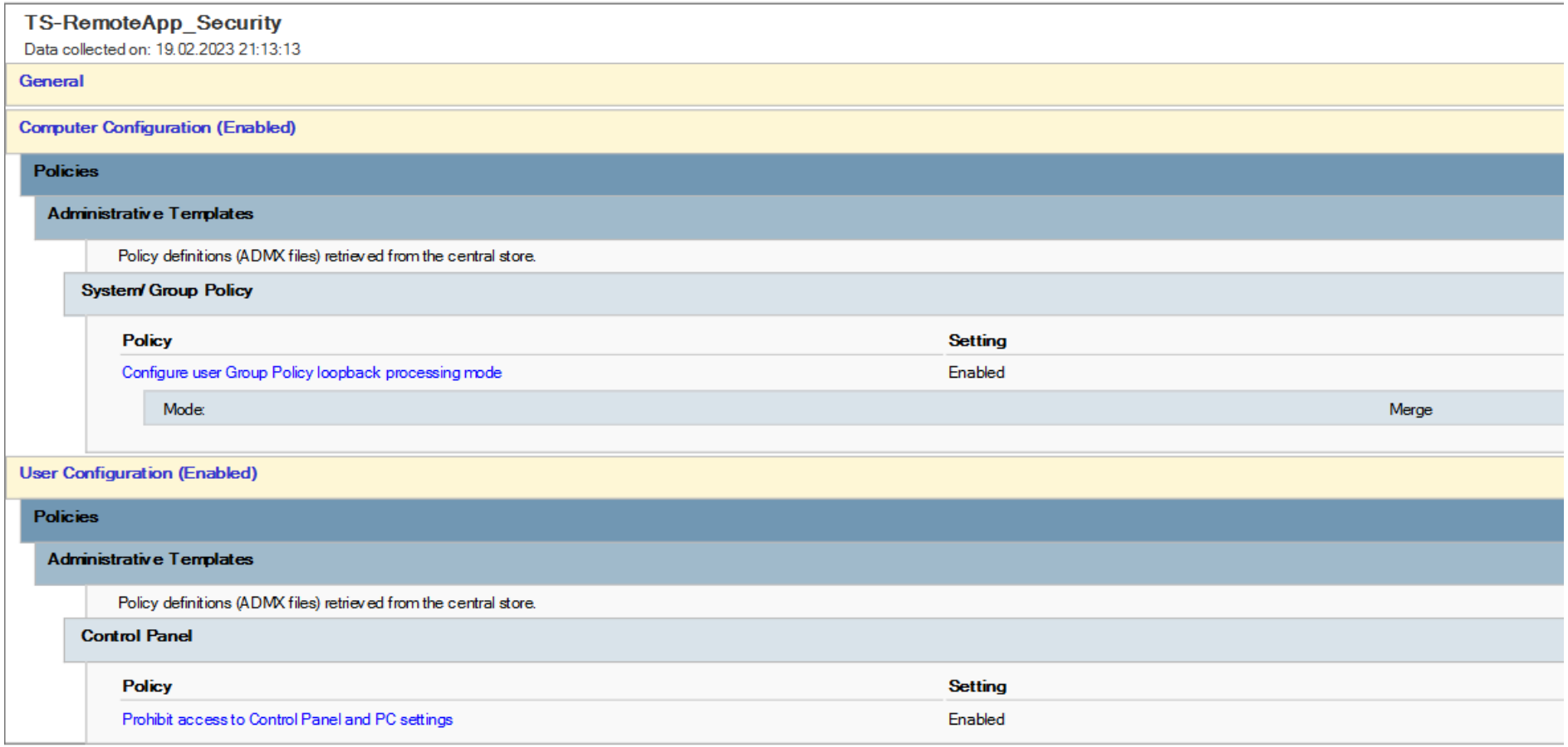
Windows Components/Remote Desktop Services/Remote Desktop Session Host/Connections

Policy	Setting
Allow users to connect remotely by using Remote Desktop Services	Enabled

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Printer Redirection

Policy	Setting
Do not allow client printer redirection	Enabled

Lab – RDS (example for loopback)



TS-RemoteApp_Security

Data collected on: 19.02.2023 21:13:13

General

Computer Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

System/ Group Policy

Policy	Setting
Configure user Group Policy loopback processing mode	Enabled
Mode:	Merge

User Configuration (Enabled)

Policies

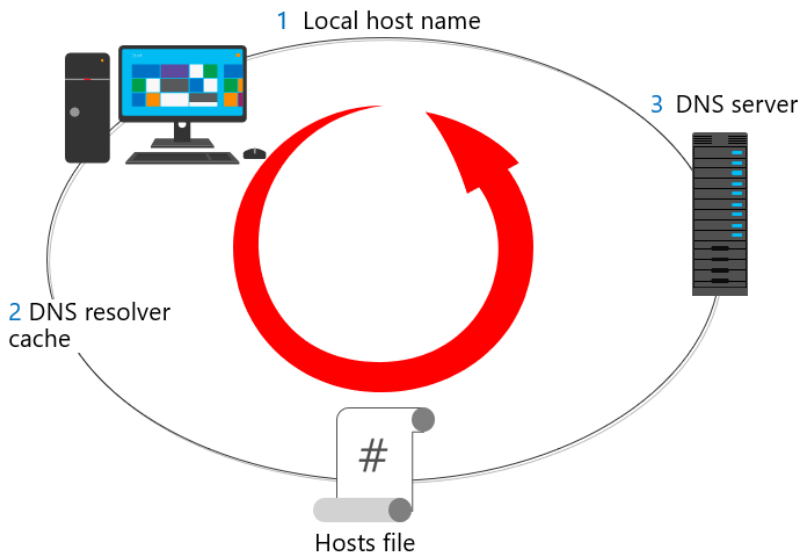
Administrative Templates

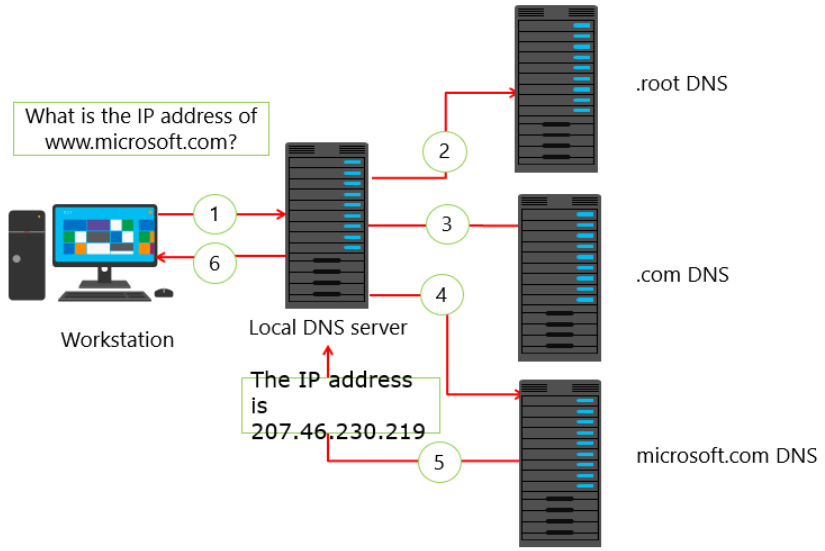
Policy definitions (ADMX files) retrieved from the central store.

Control Panel

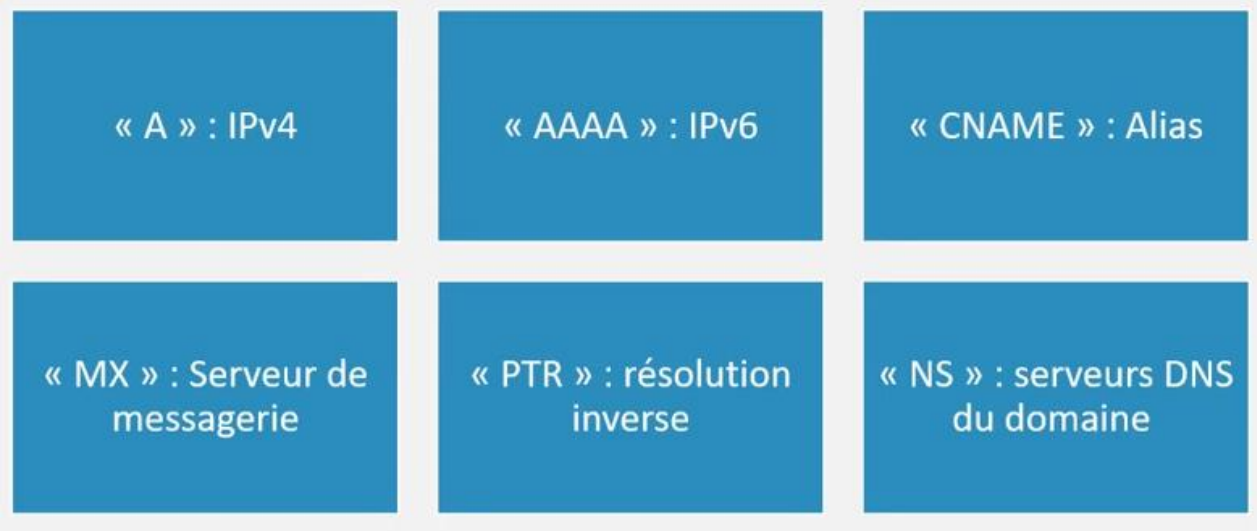
Policy	Setting
Prohibit access to Control Panel and PC settings	Enabled

Résolution de nom





Entrée DNS


« A » : IPv4
« AAAA » : IPv6
« CNAME » : Alias
« MX » : Serveur de messagerie
« PTR » : résolution inverse
« NS » : serveurs DNS du domaine

Lab

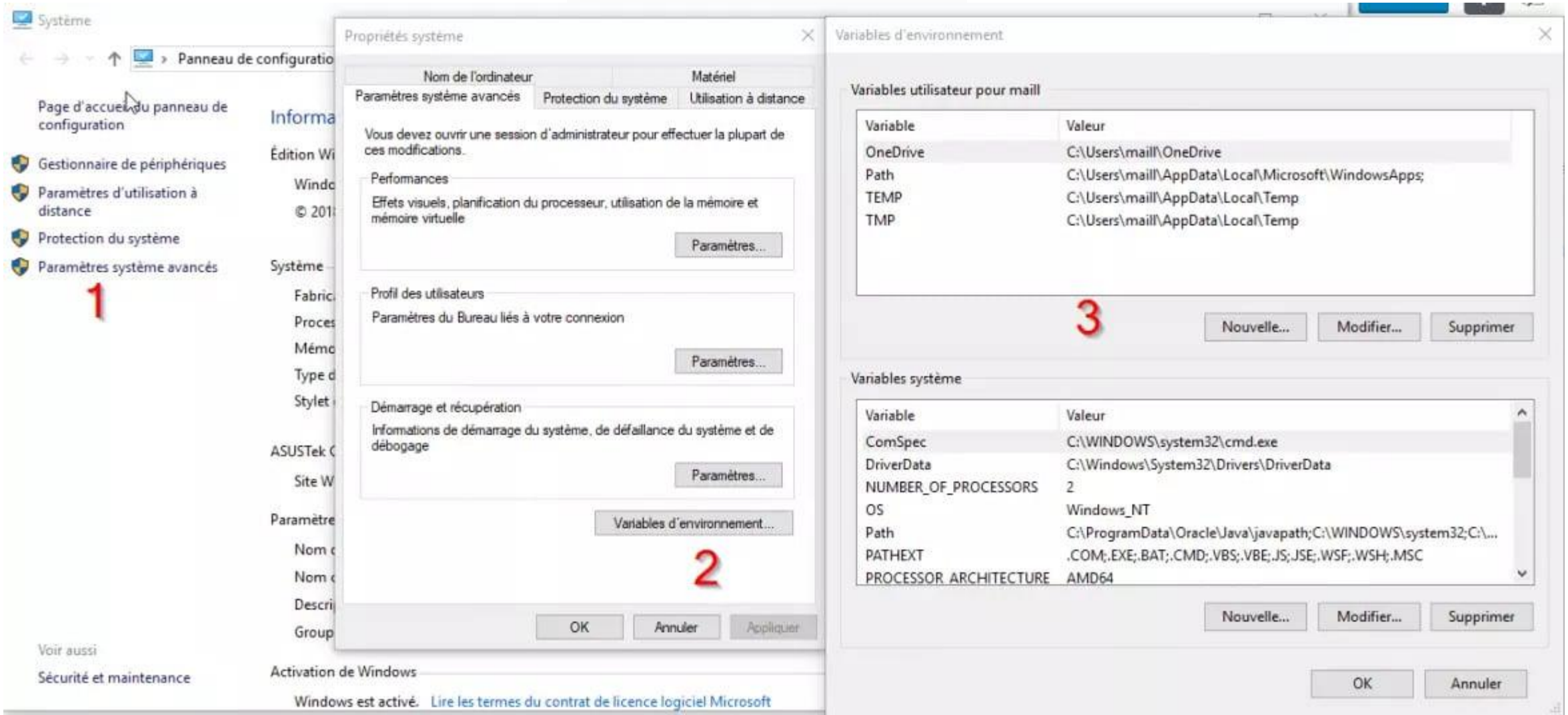
- Troubleshoot name resolution:

- Vider le cache DNS
- Vérifier la connectivité via l'adresse IP
- Vérifier la connectivité via le nom d'hôte
- Si le nom d'hôte n'est pas résolu, ajouter une entrée dans le fichier host
- Répéter le point 3
- Supprimer l'entrée du fichier host + vider le cache
- Ajouter le serveur DNS dans les configurations reseau
- Vérifier la resolution du nom d'hôte avec les commandes suivante :

Nslookup.exe Win-Clt1.sysbas.local

Resolve-dnsname win-clt1

Variables d’environnement



Base de registre

La base de registre Windows ou registre Windows est une base de données structurées où sont stockées un grand nombre d'informations.

Ces informations sont utilisées par Windows et ses composants ainsi que les programmes installés par l'utilisateur pour sauvegarder des informations utiles à leurs fonctionnements.

Cette base de données est invisible à l'utilisateur et est utilisée en arrière plan par Windows.