EXPLOITER UN WINDOWS SERVER

Thèmes abordés : GPO, PSSI, Scripts Batch, AD.

ROUX Axel

Table des matières

Compte rendu technique : Exploiter un Serveur Windows

Problématique : Comment administrer et sécuriser un environnement Windows ?

Matériel :

- 1 hyperviseur de type 2
- 1 VM Windows serveur avec l'ADDS installé
- 1 VM client Windows 11
- 1 PC d'administration

Contexte :

Vous êtes technicien système au sein du service informatique de l'entreprise TechnoData Services. Le responsable sécurité te confie la mission d'appliquer les règles de la PSSI sur le domaine Active Directory.

Les postes utilisateurs doivent être sécurisés et certaines tâches automatisées. Ainsi, vous devrez créer des GPO, configurer des tâches planifiées et automatiser certaines opérations par script Batch afin d'améliorer la sécurité et la productivité du SI.

Les objectifs principaux sont :

- Centraliser l'administration via Active Directory
- Sécuriser les sessions utilisateurs
- Mettre en place des stratégies de groupe (GPO)
- Automatiser des tâches via scripts batch et tâches planifiées
- Garantir la conformité aux règles de sécurité définies par la PSSI

Questions de positionnement :

Rappel GPO :

Q1. Qu'est-ce qu'une GPO ?

Le terme GPO est l'acronyme de Group Policy Object (stratégies de groupe). C'est donc un ensemble de paramètres de configuration sur l'Active Directory (AD) qui seront appliqué à des postes de travails, serveurs, OU, ou des utilisateurs d'un domaine.

Q2. Pourquoi utiliser des GPO ?

Les GPO sont utilisées pour automatiser et sécuriser des configurations. Cela permet de gagner du temps (ne pas manuellement faire une configuration sur chaque poste), de réduire/supprimer des potentielles erreurs humaines, et d'uniformiser l'ensemble du SI.

Q3. Comment configurer une GPO en 4 étapes ? (Créer, Configurer, Lier, Tester)

Créer la GPO :

- Ouvrir la console GPMC (Gestion de stratégie de groupe)
- Clic droit sur « Objet de stratégie de groupe », « Nouveau »
- Donner un nom parlant, par exemple « Interdire_PannelConfig »

Configurer la GPO :

- Clic droit sur la GPO nouvellement créée, puis « Modifier » pour ouvrir l'Éditeur de gestion des stratégies de groupe.
- Aller dans « Configuration ordinateur » ou « Configuration utilisateur », activer et paramétrer les stratégies, puis fermer.

Lier la GPO :

- Dans la GPMC, faire un clic droit sur le site, le domaine ou l'OU cible, puis choisir « Lier un objet de stratégie de groupe existant ».
- Sélectionner la GPO créée dans la liste et valider : un lien apparaît sous l'objet AD choisi, ce qui rend la GPO applicable à ses utilisateurs/ordinateurs.

Tester la GPO :

- Lier la GPO à une OU contenant quelques utilisateurs ou machines représentatifs, puis forcer la mise à jour avec gpupdate /force ou un redémarrage.
- Ouvrir une session avec un compte de test et vérifier que l'effet attendu fonctionne.

Tâches planifiées et scripts Batch :

Q4. Qu'est-ce qu'un fichier Batch ? Précisez son intérêt par rapport à d'autres langage.

Un fichier batch est un script interprété par l'invite de commande de Windows. Il permet de lancer en une fois une série de commandes (copie, suppression, lancement de programmes, etc.). Il prend l'extension .bat ou .cmd.

Par rapport à d'autres langages de script (PowerShell, Python, etc.), son intérêt principal est sa simplicité et sa disponibilité : il fonctionne nativement sur pratiquement toutes les versions de Windows, sans installation supplémentaire.

Q5. Quel outil Windows vous permettrait d'exécuter automatiquement à fréquence programmée votre script batch ?

C'est le Planificateur de tâches permet de lancer automatiquement un programme selon une planification (horaire, journalière, hebdomadaire, au démarrage, à la connexion, etc...) C'est l'outil standard intégré à Windows pour exécuter des scripts à une fréquence programmée, sans intervention manuelle.

PSSI :

Q6. En quoi une tâche planifiée peut améliorer la sécurité d'un système ?

Une tâche planifiée peut grandement améliorer la sécurité d'un système en automatisant des actions de protection. Par exemple, elle peut lancer des sauvegardes régulières, des scans antivirus, ou l'application de mises à jour en dehors des heures de travail, garantissant que ces tâches sont effectuées systématiquement sans risque d'oubli ou d'erreur humaine.

Q7. Pourquoi une PSSI est nécessaire dans une entreprise ?

Une PSSI est nécessaire car elle formalise les règles, les objectifs et les responsabilités en matière de sécurité pour toute l'entreprise. Elle sert de référence pour

protéger les informations critiques, assurer la conformité légale (comme le RGPD) et guider les décisions techniques de manière cohérente.

Q8. Quels sont les décideurs ?

Les décideurs pour une PSSI sont généralement la Direction, qui valide la politique et alloue les budgets, comprenant le Responsable de la Sécurité des Systèmes d'Information (RSSI) et le Directeur des Systèmes d'Information (DSI), qui la rédigent et pilotent sa mise en œuvre technique.

Q9. Citez trois endroits où l'on peut trouver des ACL sur un Système d'Information ?

On trouve ces listes de contrôle d'accès à de nombreux endroits dans un système d'information. On peut citer trois exemples principaux :

- Sur les systèmes de fichiers (ACL NTFS sur Windows) pour contrôler l'accès aux dossiers
- Sur les équipements réseau comme les routeurs et les pares-feux pour filtrer le trafic
- Au sein des annuaires comme Active Directory pour définir les permissions des utilisateurs sur les ressources partagées.

Activité 1 – Administrer Windows

3.1. Préparation du Lab Windows

Une première VM Windows server a été créée sous WS2022 :

Nom de la VM : SRV-DC

Mot de passe du compte administrateur : MDPadmin44

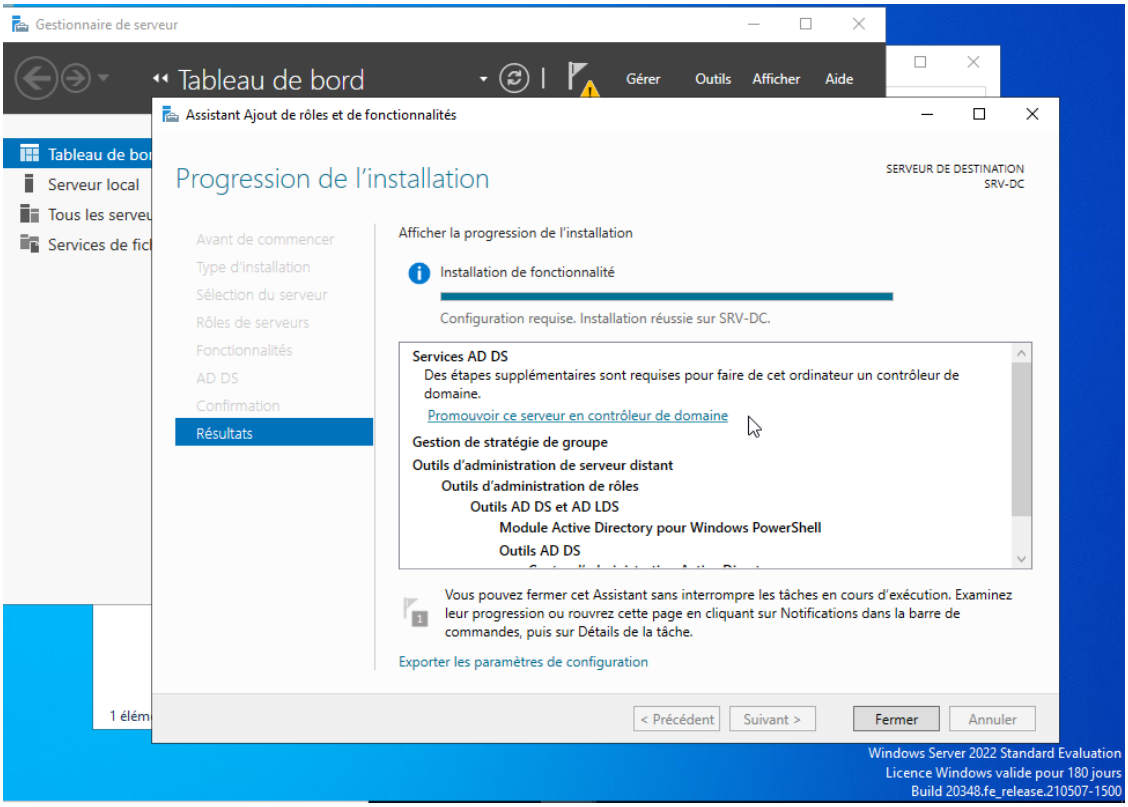
PC renommé SRV-DC

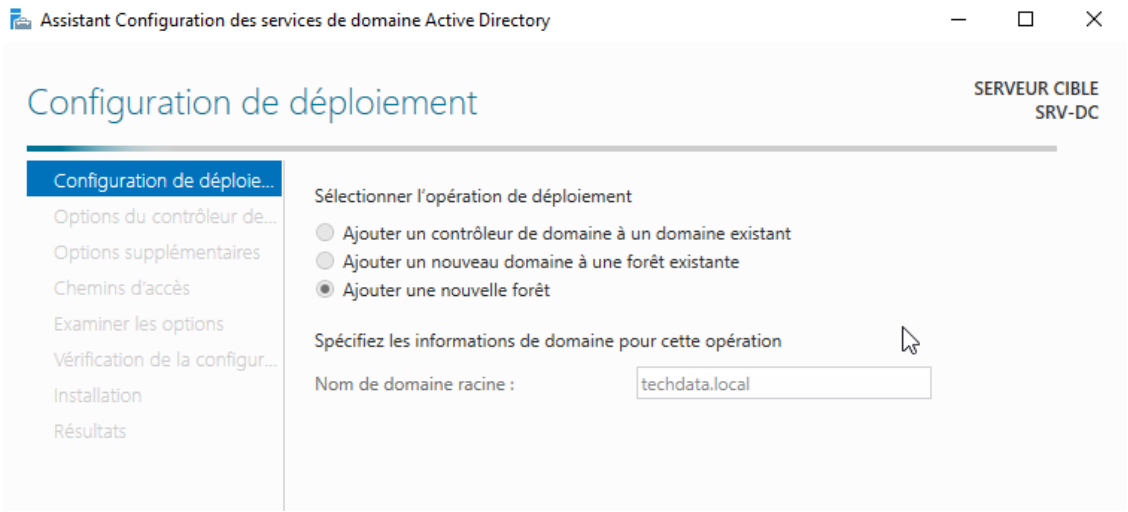
Adresse IP : 172.16.1.2/24

Pour le Windows server, nous aurons uniquement besoin du service AD DS (le service de partage de fichiers sera créé plus tard).

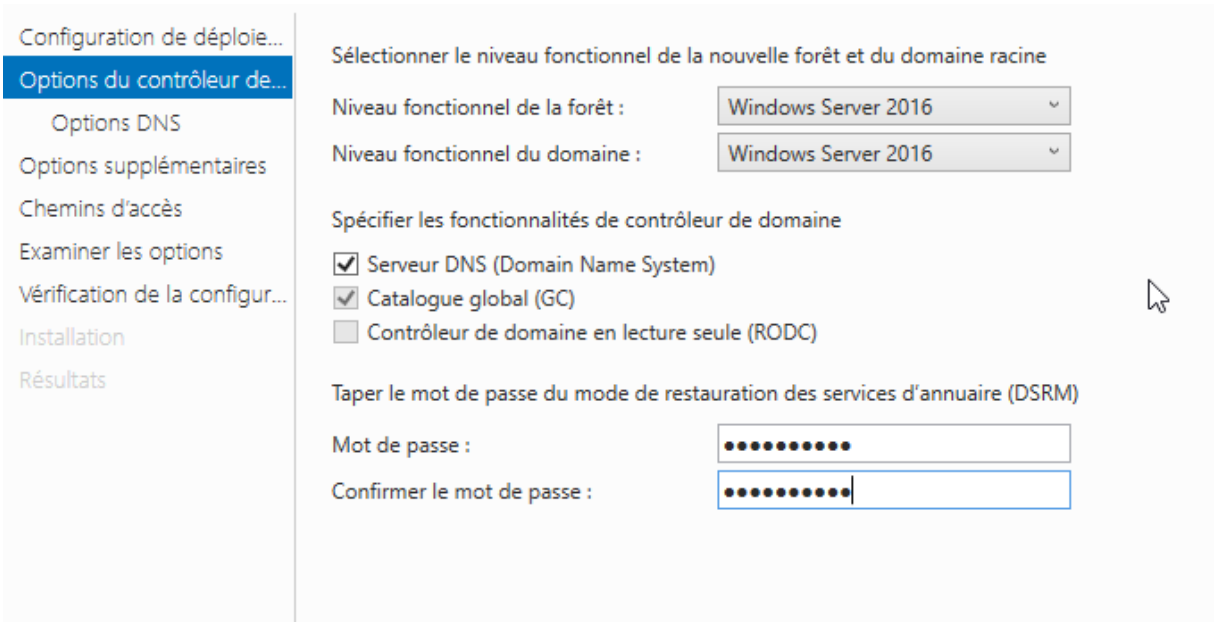
Le serveur a ensuite été promu en contrôleur de domaine avec les paramètres suivants :

- **Nom de domaine :** techdata.local
- **Nom NetBIOS :** TECHDATA





Le mot de passe pour le DSRM sera : MDPadmin44

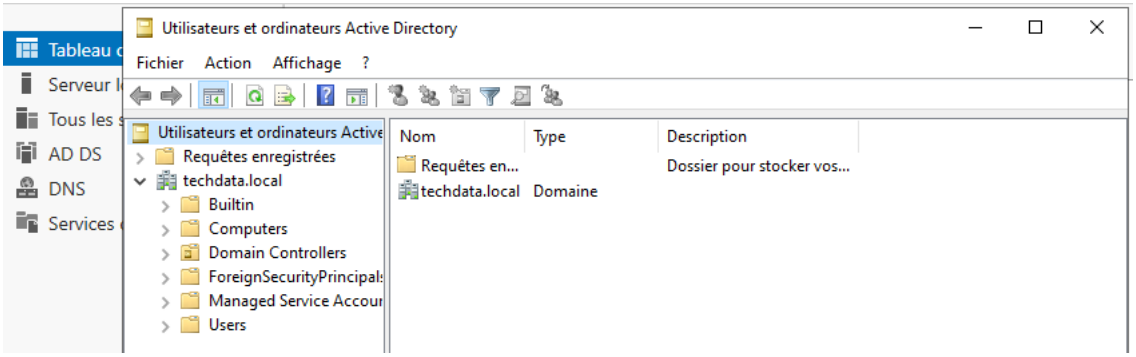


Suivant

Suivant

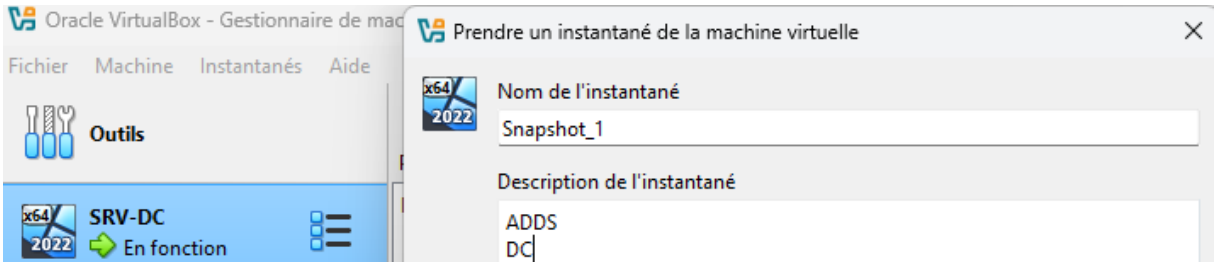
Installer

Après validation des différentes étapes de l'assistant et lancement de l'installation, le service Active Directory a été correctement déployé.
Un redémarrage du serveur a été effectué afin de prendre en compte l'ensemble des modifications apportées au système.



Une fois fini, le serveur redémarrera pour prendre en compte l'ensemble des modifications que nous avons apportés.

Par mesure de sécurité et conformément aux bonnes pratiques, un snapshot de la machine virtuelle SRV-DC a été réalisé à l'issue de cette étape. :



Pour la partie Client :

Une seconde machine virtuelle a été créée afin de représenter un poste utilisateur du domaine.

À la suite de tests précédents, le nom CLT01 ainsi que l'adresse IP 172.16.1.100/24 étaient déjà utilisés par une autre machine virtuelle. Le poste client a donc été configuré avec les paramètres suivants :

- Nom de la machine : CLT02
- Adresse IP : 172.16.1.101/24

S'il on poursuit avec l'installation de Windows 11 Pro, nous serons bloqués par Microsoft car nous n'aurons pas la configuration minimale requise pour passer sur Windows 11. Pour éviter cela, une manipulation est nécessaire :

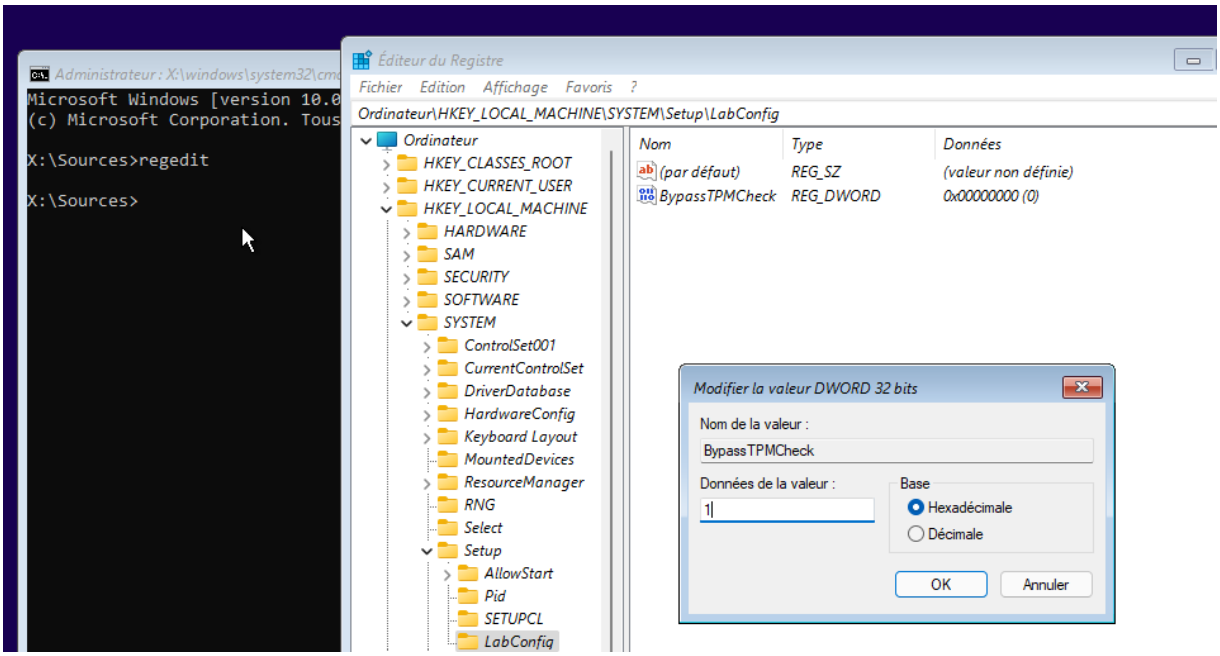
Au moment de faire l'installation lors du premier lancement, il faudra faire SHIFT + F10.

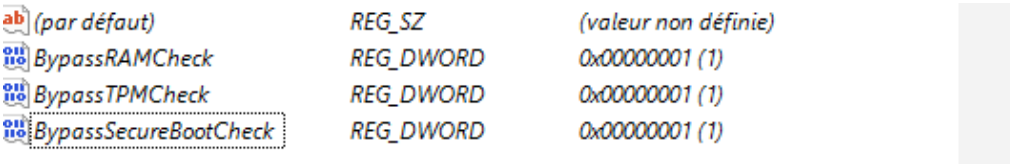
Nous arriverons donc dans une CLI.

En faisant « regedit », le programme ouvre l'éditeur de registre dans lequel nous allons créer une nouvelle clé « LabConfig ».

Dans HKEY_LOCAL_MACHINE\SYSTEM\Setup\LabConfig , 3 valeurs DWORD sont nécessaire au bon fonctionnement de la machine virtuelle. Chacune d'entre elles sera mise à 1 :

- BypassTPMCheck
- BypassRAMCheck
- BypassSecureBootCheck





Cela se verra utile lors de la vérification du matériel requis pour Windows 11.

En validant, nous pouvons à présent quitter et revenir à l'installation de base.

Nom de la VM : CLT02

OS : Windows 11 pro

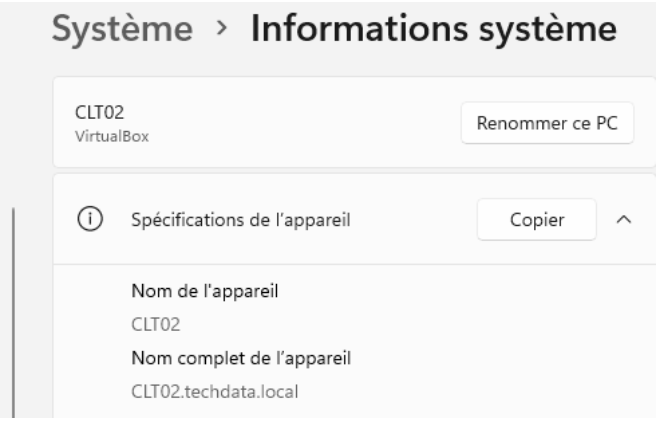
Id : user

Mot de passe : user

Adresse IP : 172.16.1.101/24

Afin d'intégrer le CLT02 au domaine, les deux machines virtuelles ont été placées sur un même réseau interne. Le mode Promiscuous (Allow VMs) a été activé afin d'autoriser les échanges réseau nécessaires.

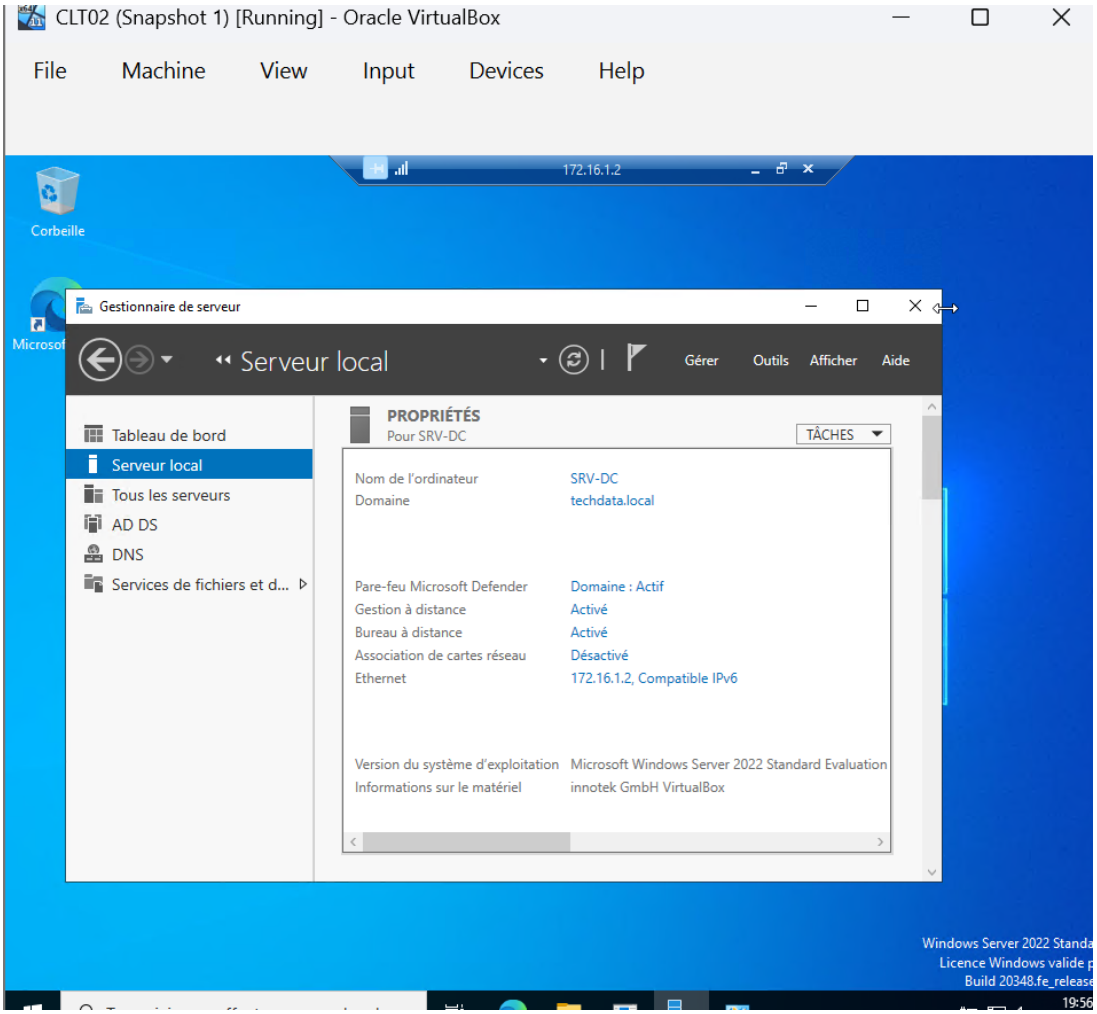
Ajout du client au domaine



3.2. Outils d'administration

L'accès au serveur a été configuré via le Bureau à distance (RDP) afin de permettre une administration centralisée depuis le poste client. Cette fonctionnalité a été activée manuellement sur le serveur.

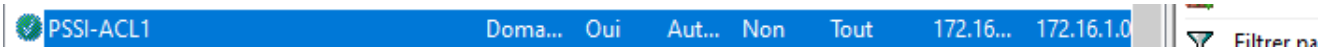
La connexion RDP a ensuite été testée avec succès depuis la machine **CLT02**, confirmant le bon fonctionnement de l'accès distant.



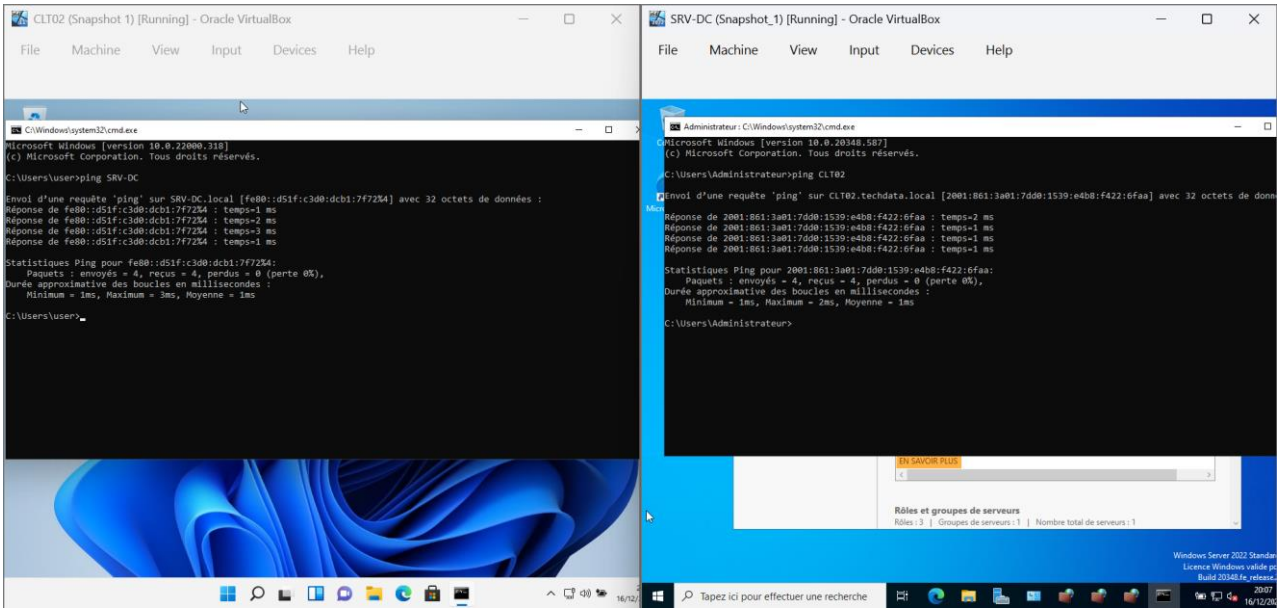
Conformément aux exigences de la PSSI, une règle de pare-feu a été mise en place afin d'autoriser les requêtes ICMPv4 vers le contrôleur de domaine depuis le réseau local.

La règle, nommée **PSSI-ACL1**, a été créée avec les paramètres suivants :

- **Type de règle :** personnalisée
- **Programmes :** tous les programmes
- **Protocole :** ICMPv4
- **Adresse IP locale :** 172.16.1.2/24
- **Adresse IP distante :** 172.16.1.0/24
- **Action :** autoriser
- **Profils :** Domaine et Privé



Test de communication dans les deux sens (avec la règle active) :



Snapshot DC & Client

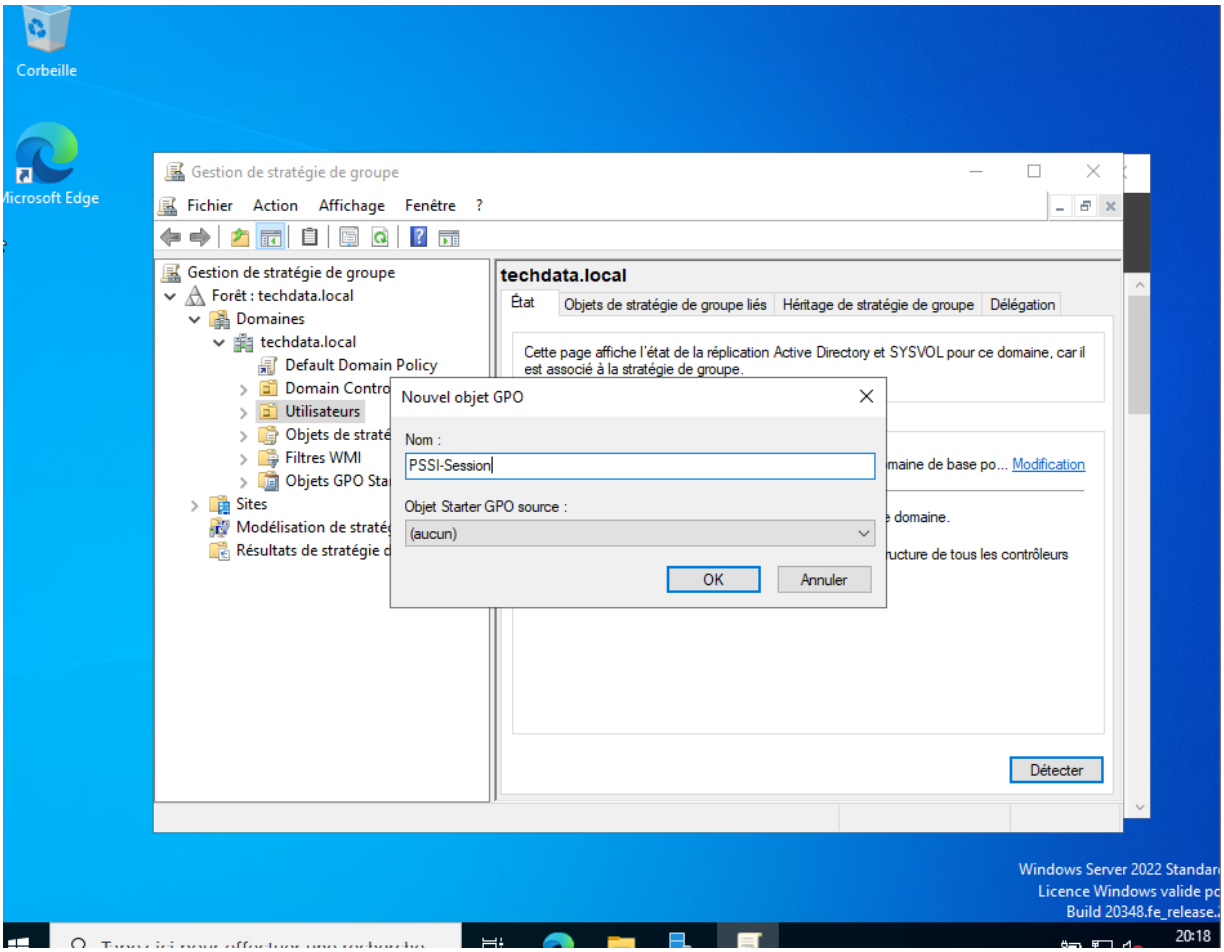
Activité 2 – Créer des GPO de sécurisation des sessions

3.1. Étapes à réaliser : GPO 1

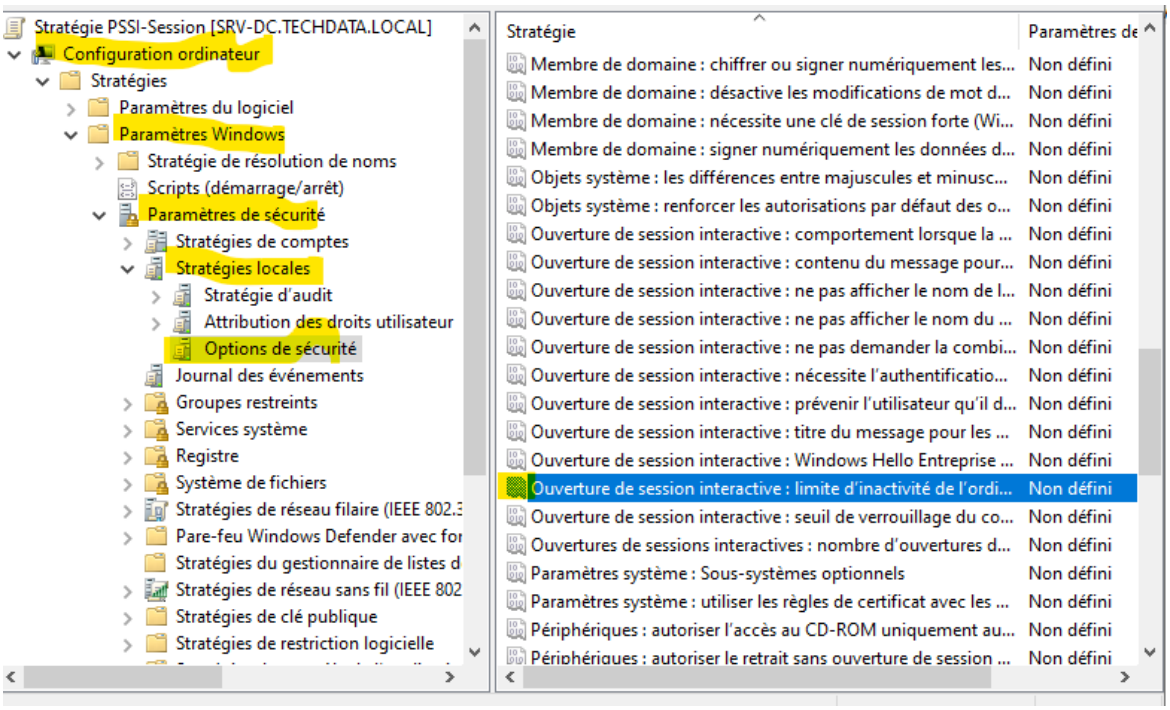
Avant d'entamer la création d'une GPO, nous allons d'abord crée un OU « Utilisateurs » dans lequel nous allons placer notre utilisateur « test », ainsi que l'OU « Ordinateurs » dans lequel il y a le CLT02.

Ensuite, nous pouvons créer une stratégie de groupe (GPO) « PSSI-Session ». Cette GPO déconnectera la session d'un utilisateur inactif depuis plus de 15 minutes et bloquera l'accès au panneau de contrôle.

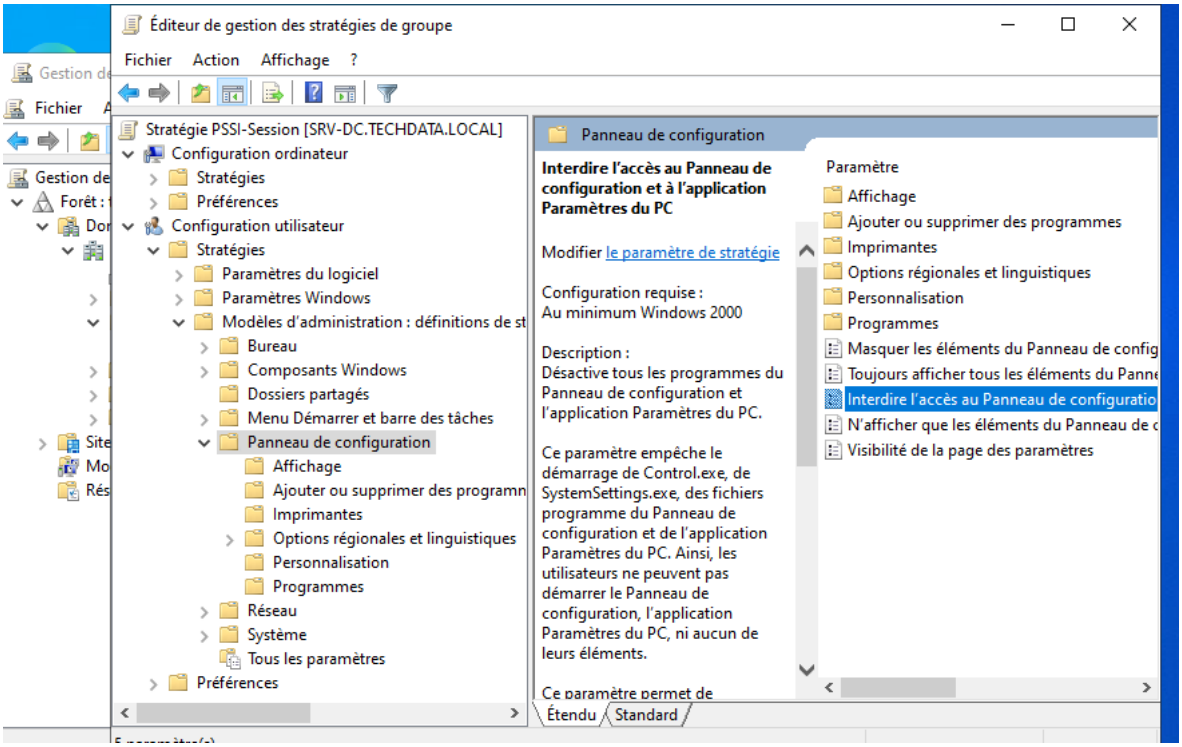
On ouvre donc la console Group Policy Management (gpmc.msc), puis on créé une GPO Utilisateurs.



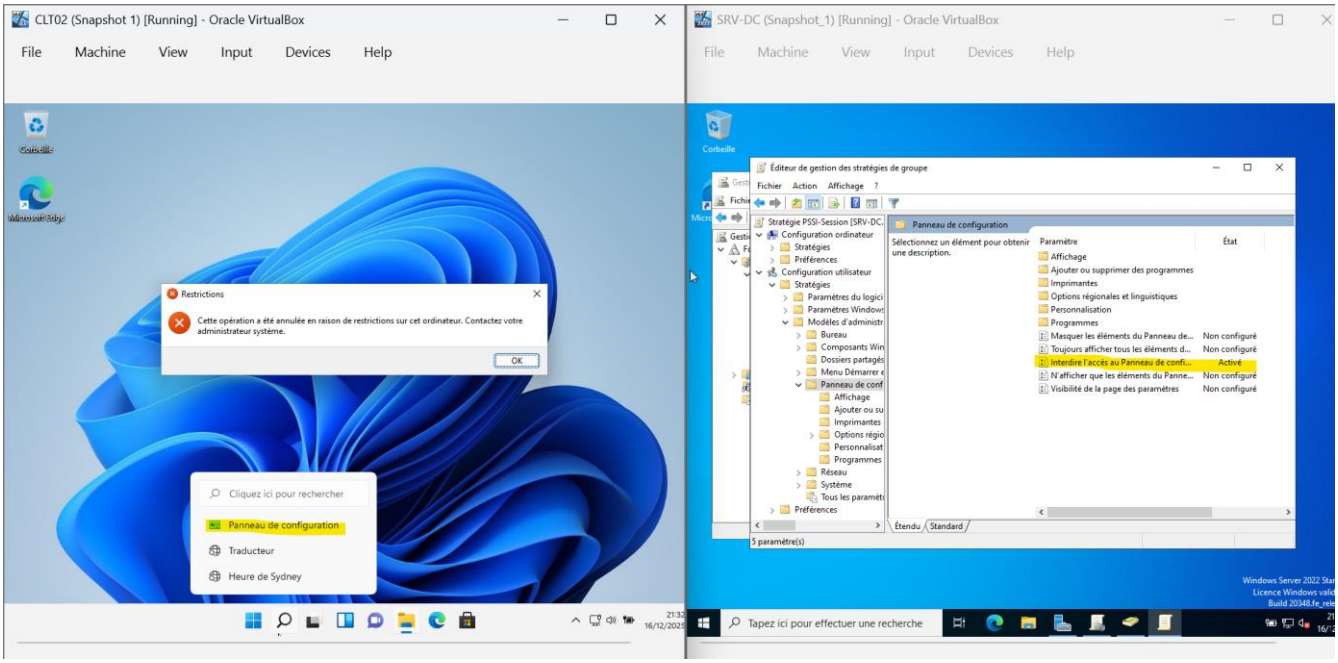
Selon la PSSI-AUTH3, un utilisateur inactif depuis plus de 15 minutes doit être déconnecté. On fixe donc la limite à 900 secondes.



Concernant la restriction au panneau de configurations, il faut activer l'option « interdire l'accès au Panneau de configurations »

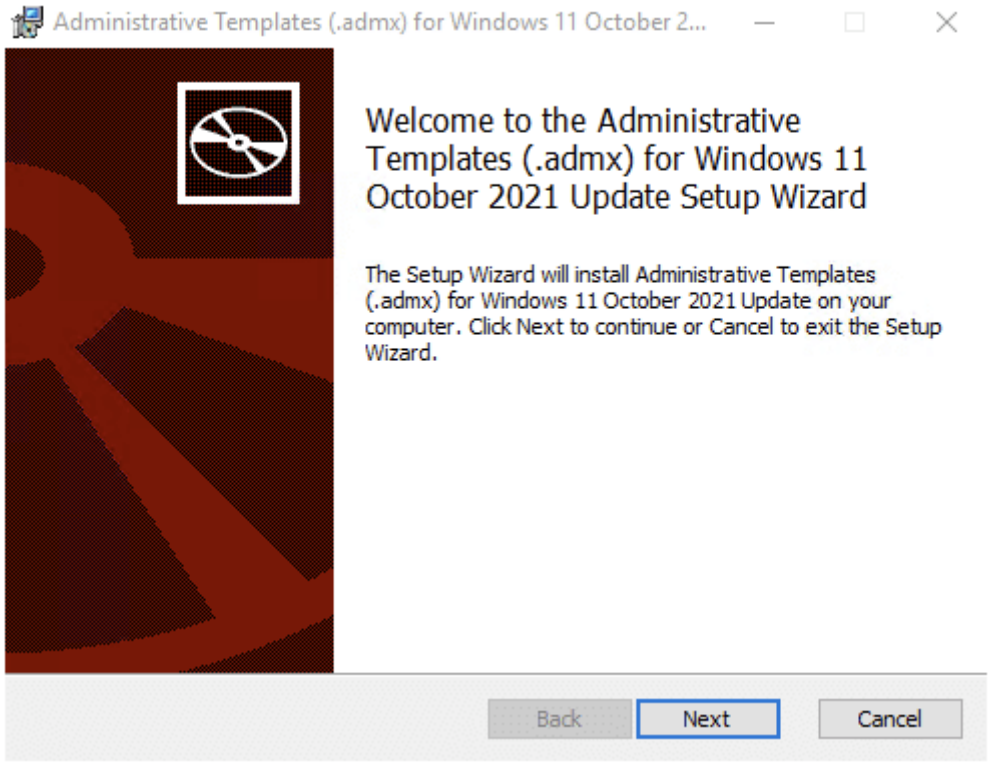


Pour vérifier le bon fonctionnement des GPO, on effectue sur la VM client un gpupdate/force , puis on essaie d'accéder au panneau de configurations :



3.2. Étapes à réaliser : GPO 2

Afin d'installer les templates pour Windows 11, il faut se rendre sur https://www.microsoft.com/en-us/download/details.aspx?id=103507 télécharger et ouvrir l'application dans le Domain Controller.

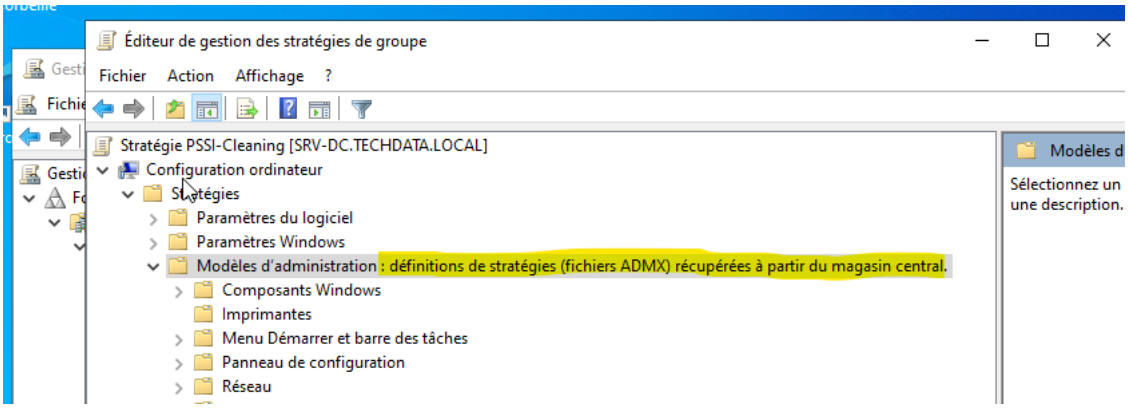


Une vérification a permis de confirmer leur présence dans le répertoire suivant : C:\Program Files (x86)\Microsoft Group Policy\Windows 11 October 2021 Update (21H2)\PolicyDefinitions

L'ensemble du contenu a ensuite été copié dans le dossier centralisé : C:\Windows\SYSVOL\sysvol\techdata.local\Policies\PolicyDefinitions

Cette centralisation permet la synchronisation automatique des fichiers ADMX entre tous les contrôleurs de domaine, garantissant une cohérence des stratégies.

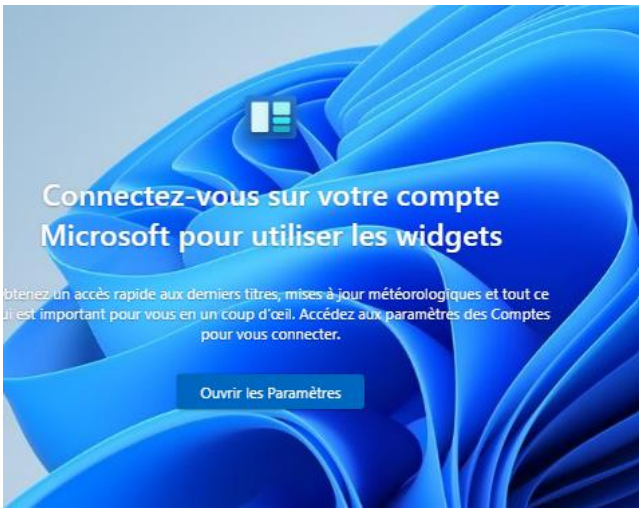
Maintenant, nous pouvons vérifier qu'il a bien été pris en compte :



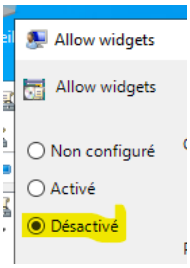
Une nouvelle stratégie de groupe a été configurée afin de **désactiver les widgets Windows 11**, fonctionnalité non essentielle dans un environnement professionnel et susceptible de générer des distractions ou des flux réseau inutiles. Le paramètre à désactiver se situe sur ce chemin :

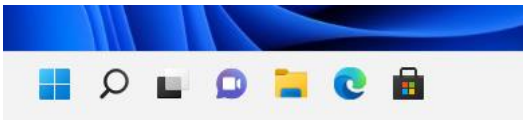
Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Widgets

Avant la modification :



Après la modification :



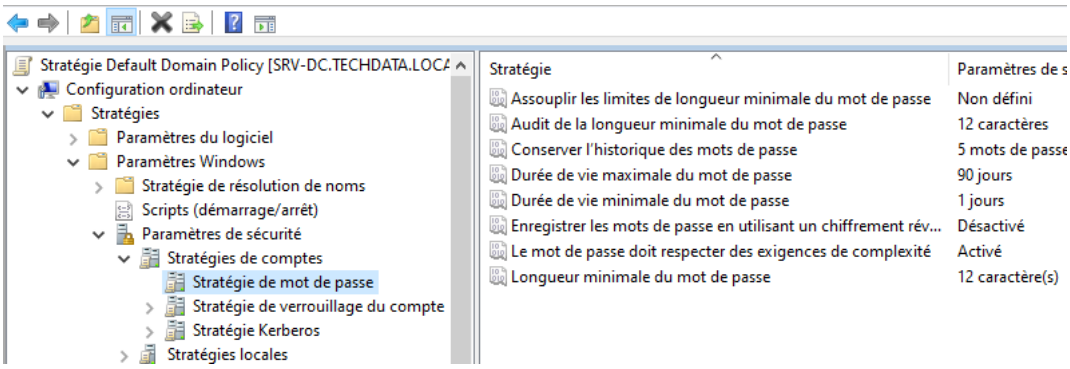


Il n'apparait plus dans la barre des tâches et n'est plus accessible.

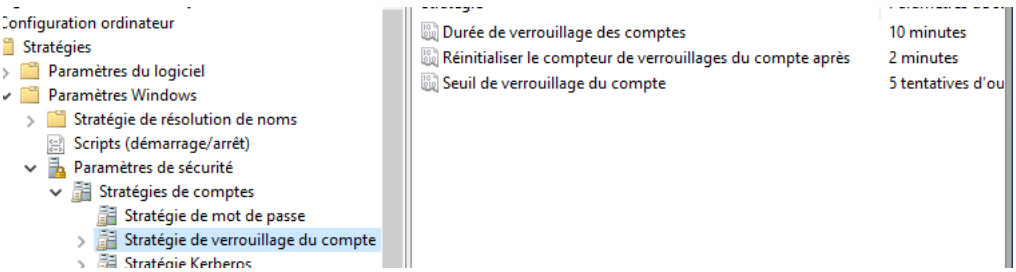
Snapshot DC & Client

Activité 3 – Politique de mot de passe conforme à la PSSI

Dans la stratégie 'Default Domain Policy', il y a une stratégie de mot de passe personnalisable. Modification des paramètres :

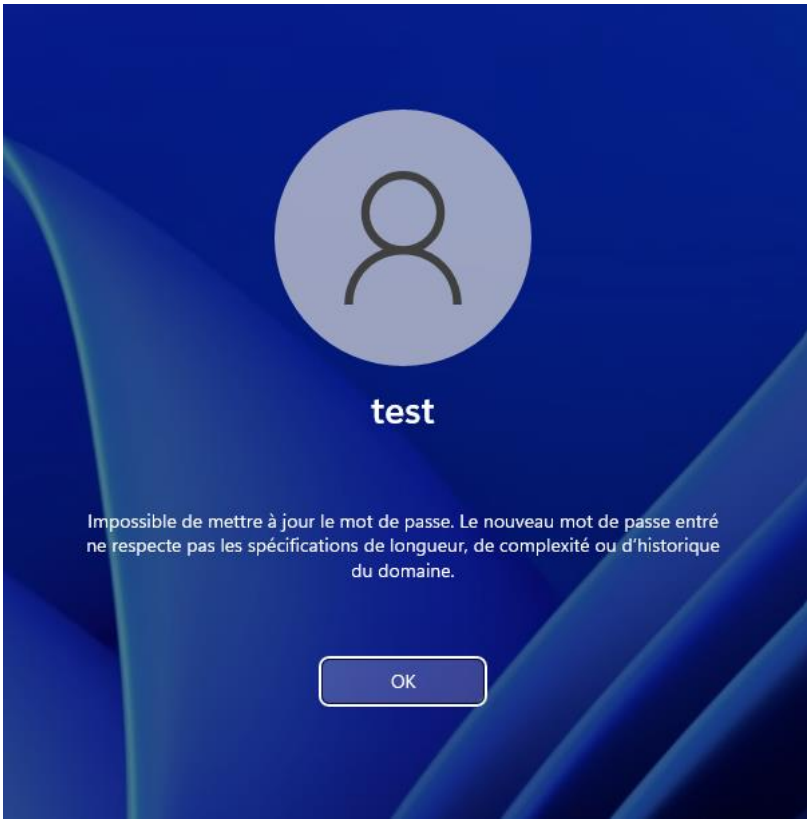


Par soucis de sécurité et de pédagogie, le PSSI-AUTH2 a également été mise en place :



Stratégie testée sur CLT02 :

Le mot de passe testé était : @Azertyuiop

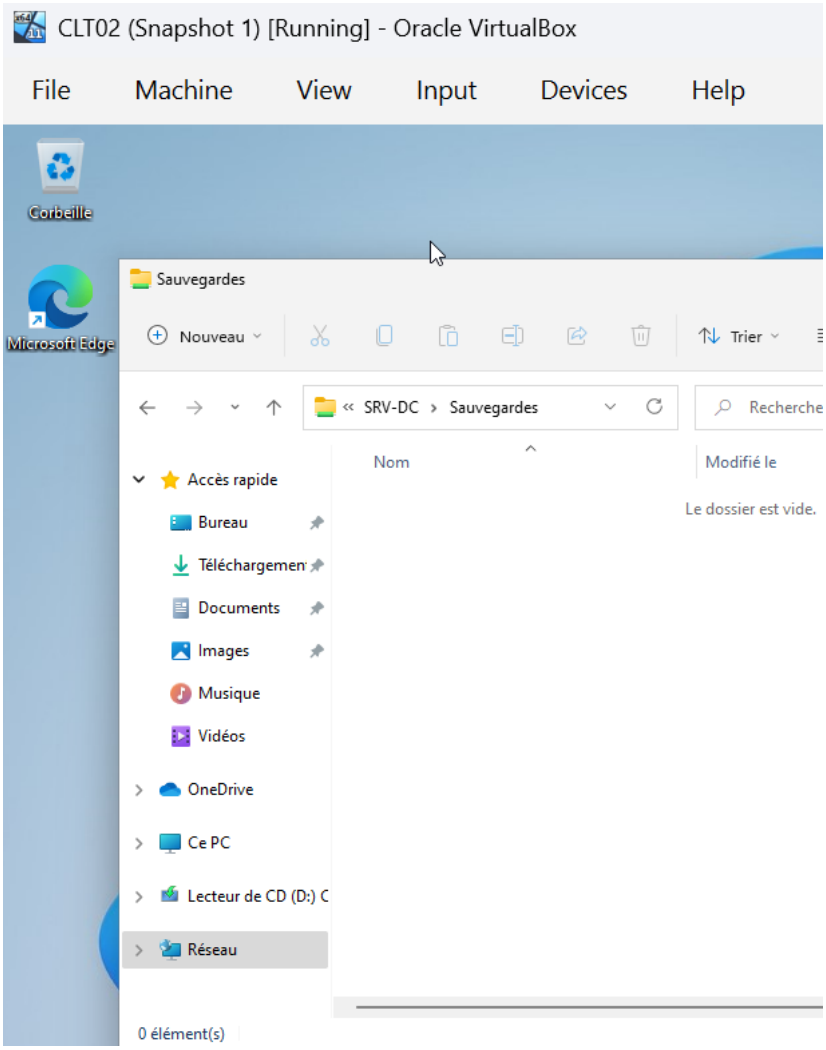


L'utilisateur est bien restreint par la réglementation des mots de passes.

Activité 4 – Automatisation et tâches planifiées avec script Batch

Création d'un dossier partagé « Sauvegardes » sur le contrôleur de domaine.

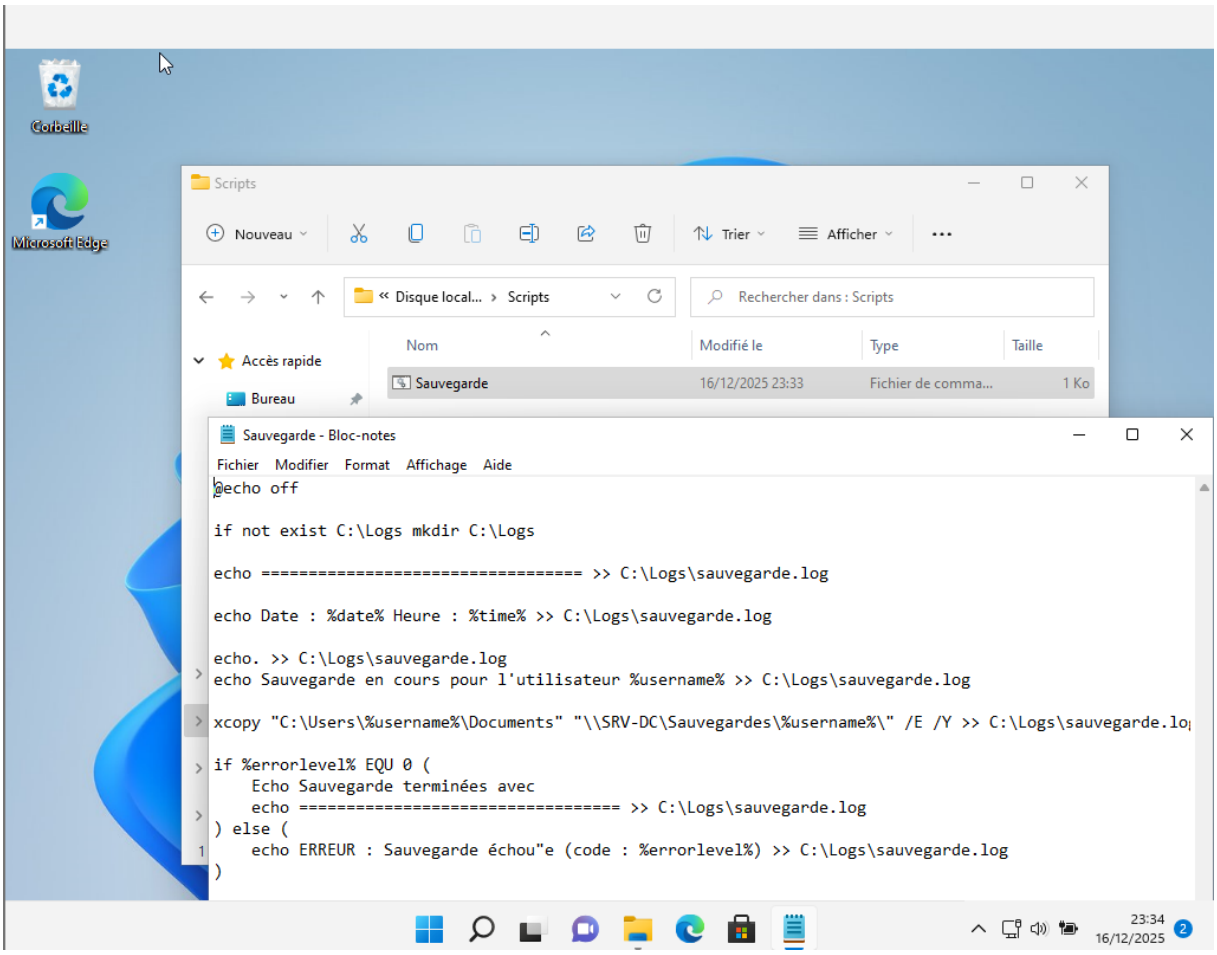
Vérification de l'accessibilité du partage effectuée depuis le poste client **CLT02**, confirmant que les droits d'accès et la connectivité réseau sont correctement configurés.



Un script Batch a été développé afin d'automatiser la copie de fichiers depuis le poste client vers le partage réseau de sauvegarde.

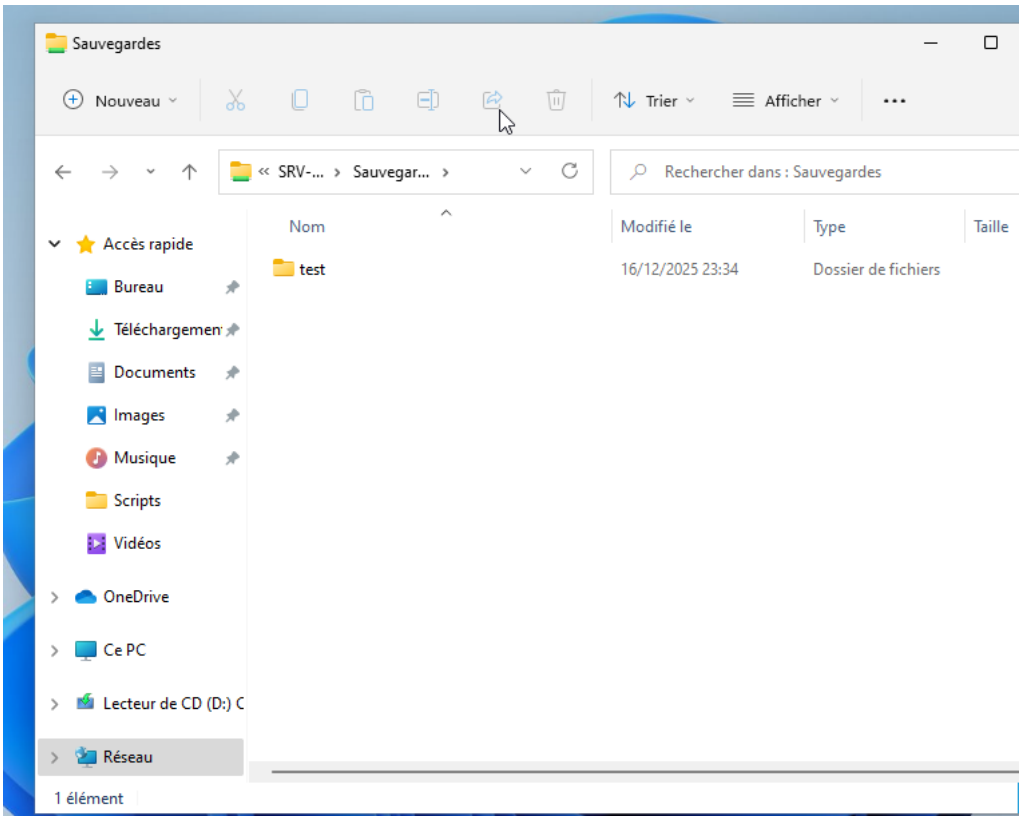
Ce script répond aux objectifs suivants :

- Copier automatiquement les fichiers à sauvegarder
- Générer des logs afin d'assurer la traçabilité des opérations
- Gérer les erreurs éventuelles lors de l'exécution

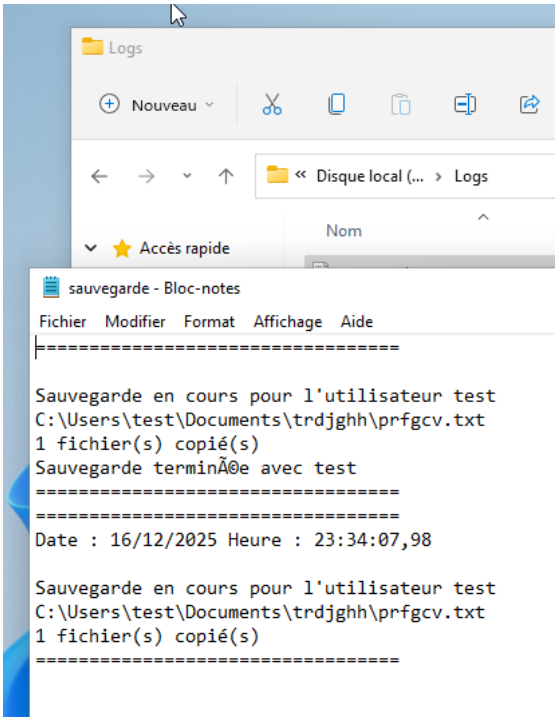


L'utilisation de variables systèmes telles que « date », « time » ou encore « ERRORLEVEL » ont servi pour répondre à la demande.

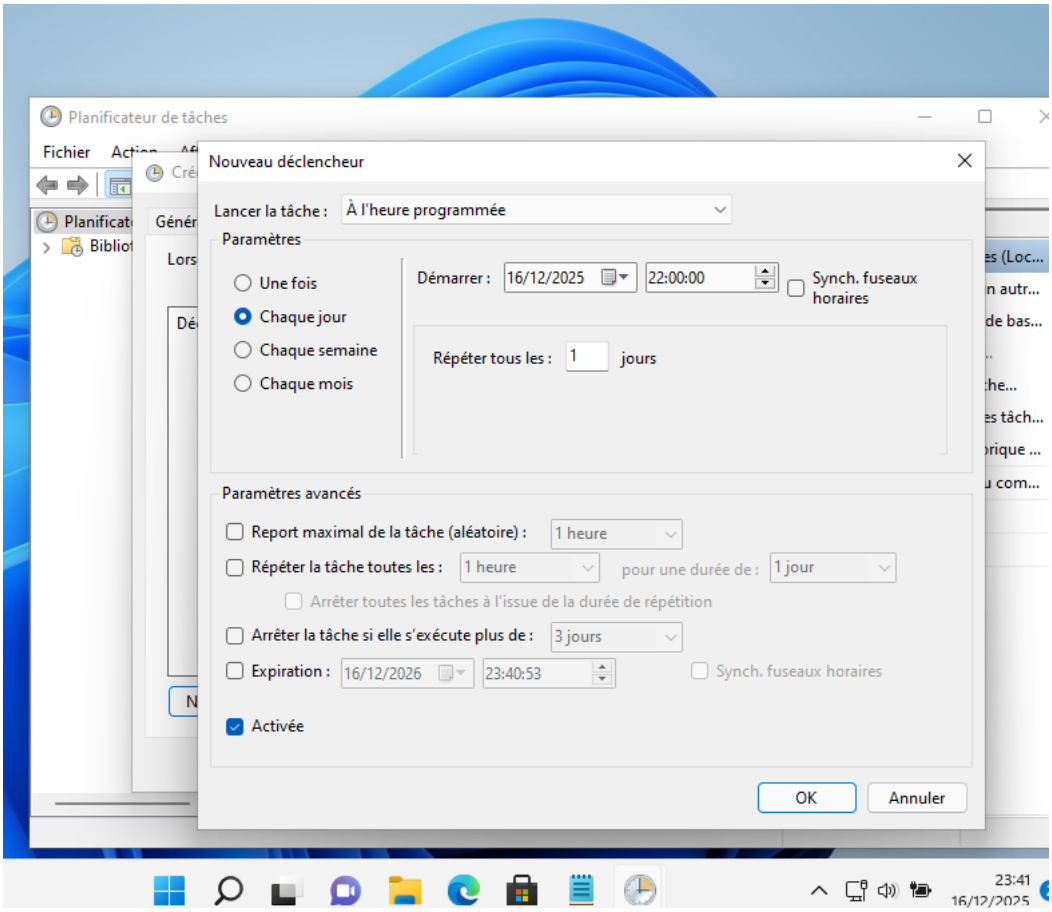
Afin de valider le bon fonctionnement du script, un fichier texte a été placé dans le dossier **« Mes Documents »** du poste client.



Les journaux générés confirment que la sauvegarde s'est déroulée conformément aux attentes.



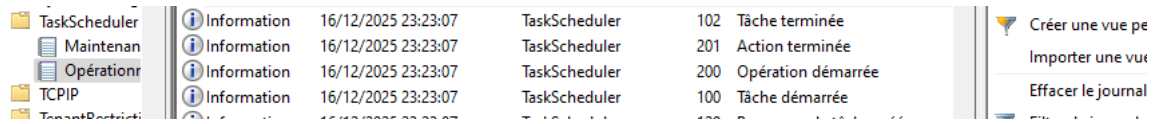
Création d'une nouvelle tâche dans taskschd.msc qui exécute tous les jours le fichier C:\Scripts\Sauvegarde.bat à 22h.



Après exécution automatique de la tâche planifiée, les résultats ont été consultés dans l'Observateur d'événements de Windows.

Les journaux confirment :

- ✓ Le déclenchement de la tâche à l'horaire prévu
- ✓ L'exécution correcte du script
- ✓ L'absence d'erreurs critiques



Snapshot DC & Client

Conclusion :

Ce projet a permis de mettre en œuvre un environnement Windows Server complet, sécurisé et fonctionnel, conforme aux principes fondamentaux de l'administration système en entreprise et aux exigences d'une Politique de Sécurité des Systèmes d'Information (PSSI).

La mise en place du contrôleur de domaine Active Directory a permis de centraliser l'authentification, la gestion des utilisateurs et des postes, tout en structurant l'environnement selon des bonnes pratiques (OU dédiées, nommage cohérent, gestion centralisée).
L'utilisation de stratégies de groupe (GPO) a ensuite renforcé la sécurité des sessions utilisateurs, notamment par la déconnexion automatique des sessions inactives et la restriction d'accès aux paramètres système sensibles.

Roux Axel.