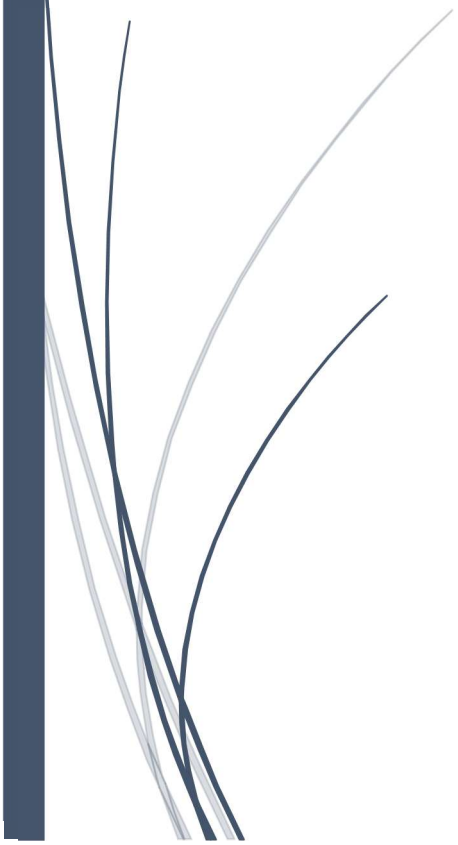
Mr JACQUEMIN

02/12/2024

Compte rendu TP

Sécurisation Windows Server – Active Directory - LAPS



TEWES Arnaud
BTS SIO SISR 2ÈME ANNÉE

Introduction

Dans ce TP, nous avons vu comment mieux sécuriser un serveur sous Windows Server avec certaines configurations de bases, comment sécuriser un contrôleur de domaine Active Directory en 7 étapes et comment paramétrer et installer Windows LAPS. C'est toutes ces étapes que je vais vous présenter dans ce compte-rendu.

Sécurisation de Windows Server

Pour sécuriser un serveur sous Windows Server, il est essentiel de suivre certaines configurations de base :

- **Activer le pare-feu Windows** : Cela aide à protéger le serveur contre les accès non autorisés.
- **Faire les mises à jour** : Assurer que le système d'exploitation et les logiciels sont à jour pour corriger les vulnérabilités.
- **Activer BitLocker** : Chiffrer les disques pour protéger les données sensibles.
- **Activer Windows Defender** : Utiliser Windows Defender si aucun autre antivirus ou solution IPS/IDS n'est disponible.
- **Désactiver le service spouleur d'impression** : Désactiver et supprimer ce service du démarrage automatique pour réduire les risques d'attaques.
- **Désactiver SMB V1** : Désactiver cette version obsolète du protocole SMB pour éviter les vulnérabilités connues.
- **Activer les clichés instantanés** : Utiliser les clichés instantanés pour sauvegarder et restaurer les données en cas de besoin.

Sécurisation d'un contrôleur de domaine Active Directory

Pour sécuriser un contrôleur de domaine Active Directory, voici les étapes à suivre :

- **Activer la corbeille AD** : Permet de restaurer facilement les objets supprimés.
- **Modifier le quota d'utilisateur dans ADSI** : Réduire le quota d'utilisateurs autorisés à joindre des machines au domaine à 0 au lieu de 10 par défaut.
- **Supprimer "Utilisateur authentifié" du groupe "Accès compatible pré-Windows 2000"** : Réduire les permissions par défaut pour améliorer la sécurité.
- **Supprimer "Administrateur" du groupe "Administrateur du schéma"** : Limiter les privilèges pour réduire les risques de modifications non autorisées.
- **Ajouter "Administrateur" au groupe "Protected Users"** : Renforcer la sécurité des comptes administratifs.
- **Créer une stratégie de groupe pour désactiver NTLM** : Désactiver NTLM pour utiliser des protocoles d'authentification par mot de passe plus sécurisés.

Paramétrage et installation de Windows LAPS

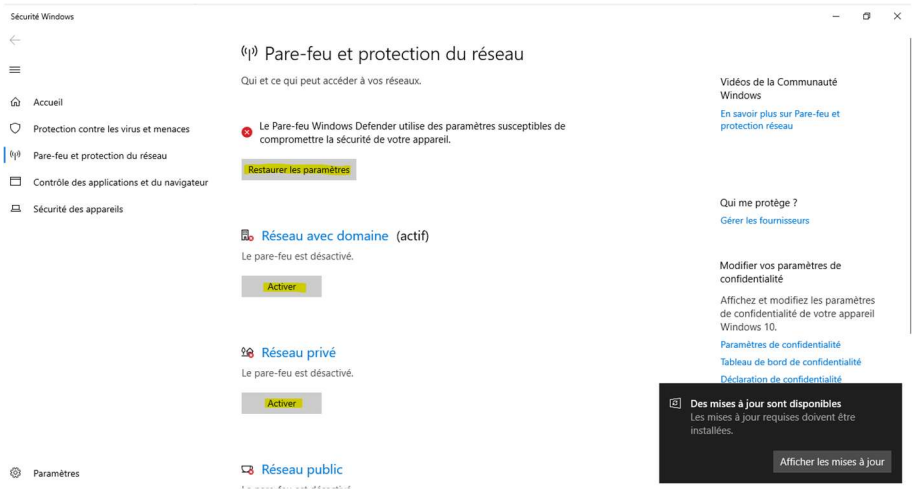
Windows Local Administrator Password Solution (LAPS) permet de gérer les mots de passe des comptes administrateurs locaux de manière sécurisée :

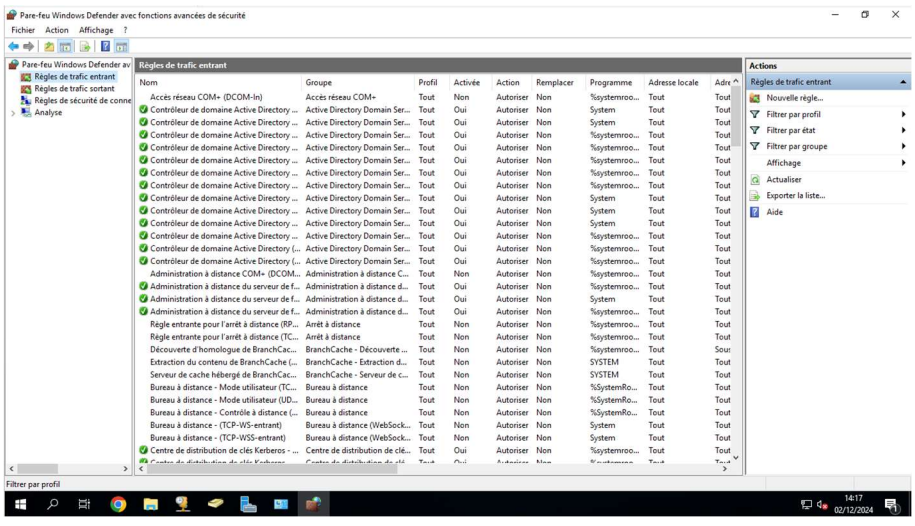
1. **Installer LAPS** : Déployer le logiciel sur les machines cibles.
2. **Configurer les paramètres de LAPS** : Définir les politiques de gestion des mots de passe, comme la longueur et la complexité.
3. **Déployer les stratégies de groupe** : Appliquer les stratégies de groupe pour automatiser la gestion des mots de passe sur les machines.

1. Sécurisation Windows Server

Activer le pare-feu Windows

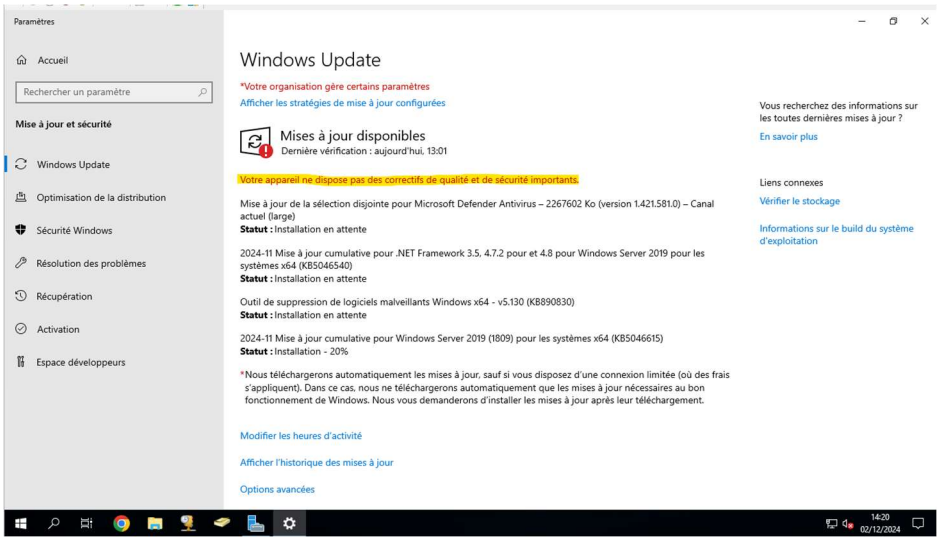
Dans notre première configuration de Windows Server, il est préférable de désactiver le pare-feu pour éviter les soucis. La première étape de notre sécurisation va donc être de réactiver tous les pare-feux.
Si un souci venait à surgir après l'activation, on pourrait donc savoir que ce n'est pas un souci « logiciel » mais plus un souci réseau que le pare-feu bloquerait.





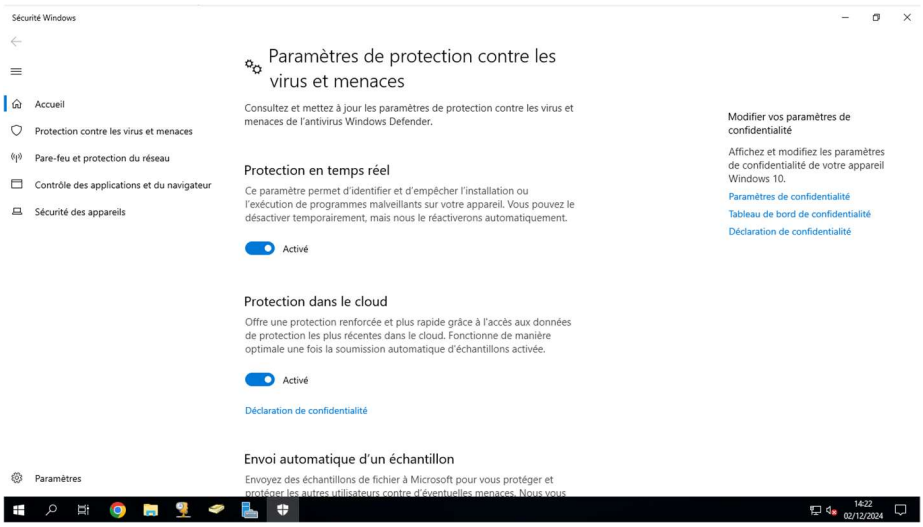
Faire les mises à jour

La deuxième étape va être d'effectuer toutes les mises à jour disponible sous Windows Update. En effet, Microsoft déploie tous les mois des mises à jour et correctifs de sécurité qu'il est essentiel d'installer sur nos serveurs pour éviter les risques d'actions malveillantes. Nous avons la possibilité de créer des planificateurs d'événements pour que les mises à jour se télécharge et/ou s'installent en dehors des heures d'activités. Mais il est impératif de toujours les effectuer.



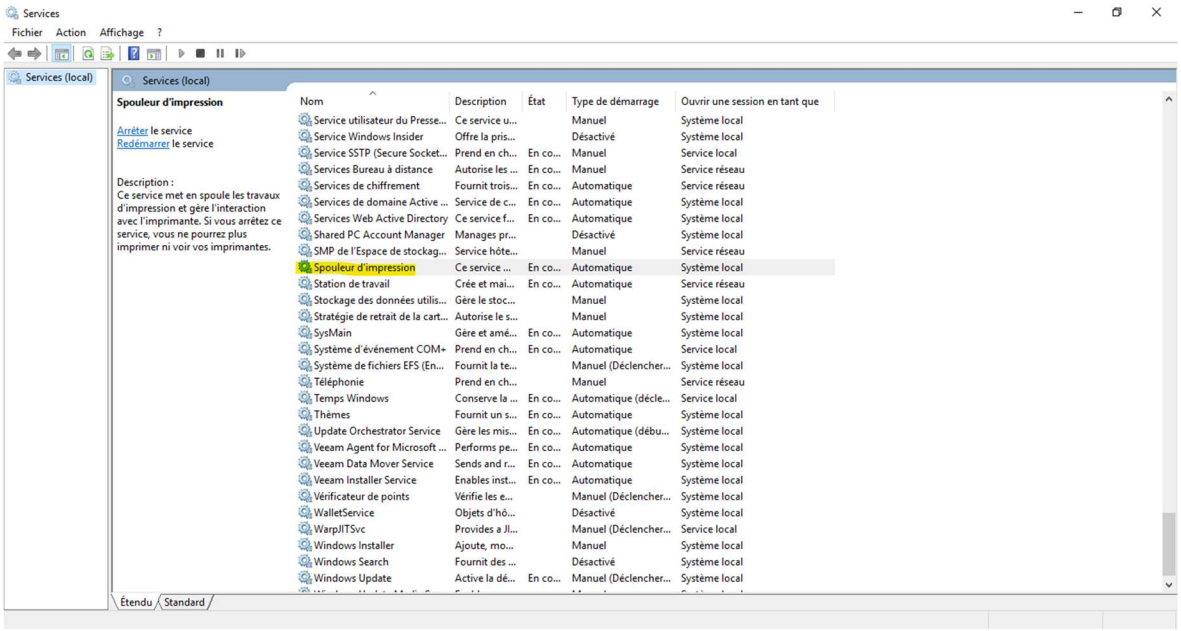
Activer Windows Defender

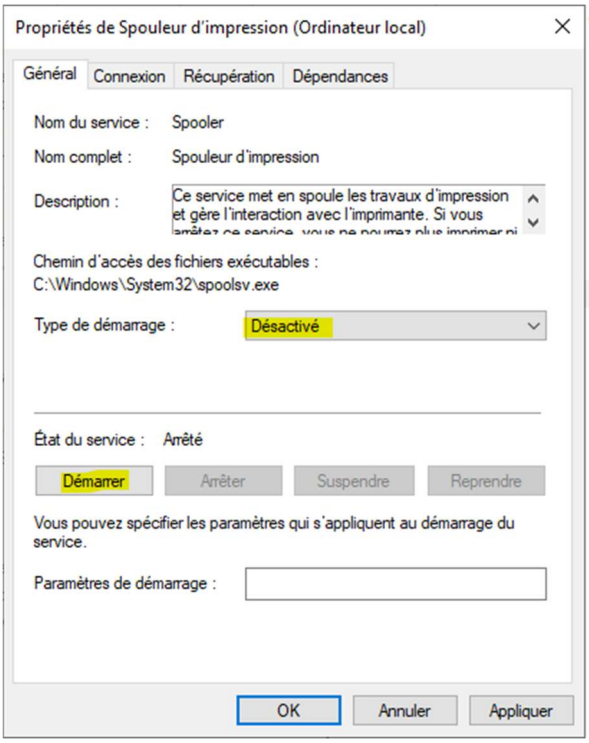
La troisième étape est bien sûr d'utiliser et d'activer la protection via Windows Defender si aucun autre logiciel antivirus est installé sur le poste et/ou si nous n'avons pas de solutions IPS/IDS.



Désactiver le service spouleur d'impression

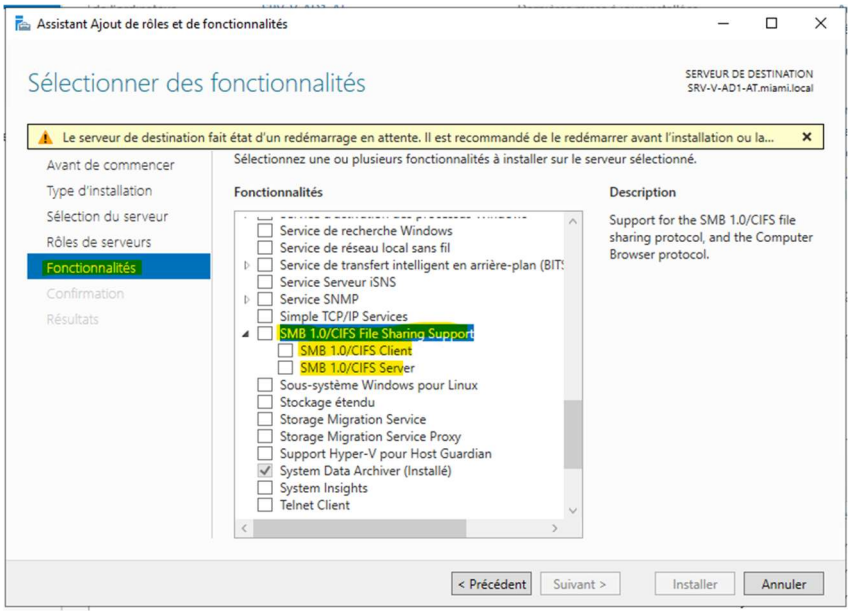
La 4eme étape va être de désactiver le spouleur d'impression pour renforcer la sécurité de nos serveurs. En effet, ce service a été la cible de nombreuses vulnérabilités. En désactivant ce service, nous réduisons la surface d'attaque potentielle et protégeons nos systèmes contre des exploits connus. De plus, si le serveur n'a pas besoin de gérer des tâches d'impression, il est logique de désactiver ce service pour éviter des risques inutiles.





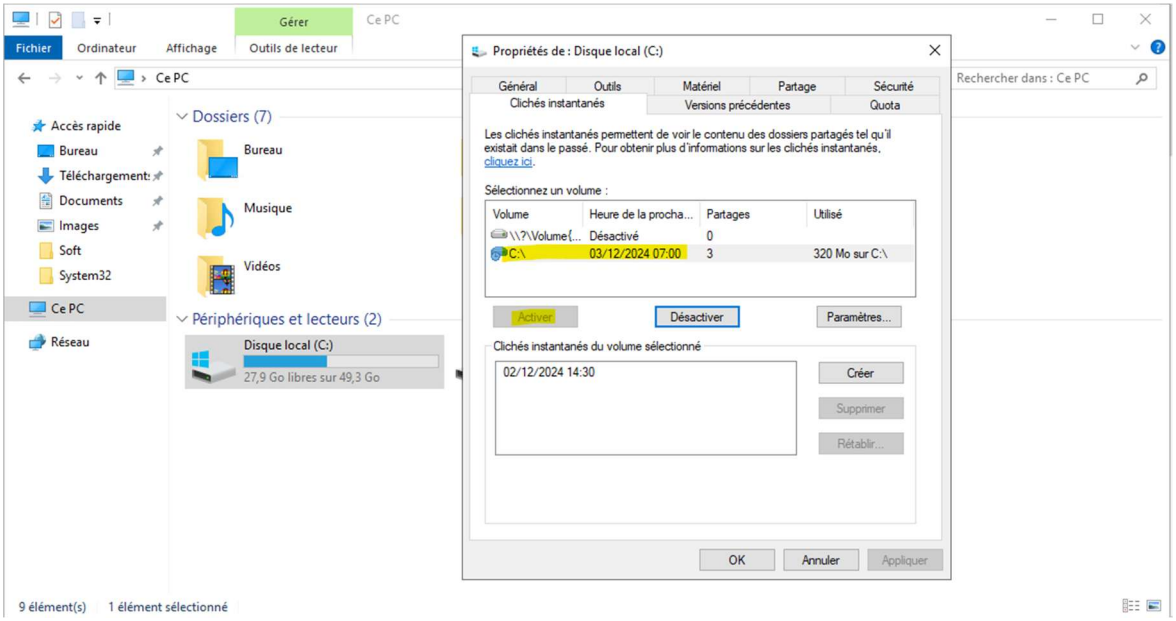
Désactiver SMB V1

La 5eme étape va être de désactiver SMB V1. Cette version obsolète du protocole SMB est connue pour ses nombreuses vulnérabilités, qui peuvent être exploitées par des attaquants pour accéder à nos systèmes.



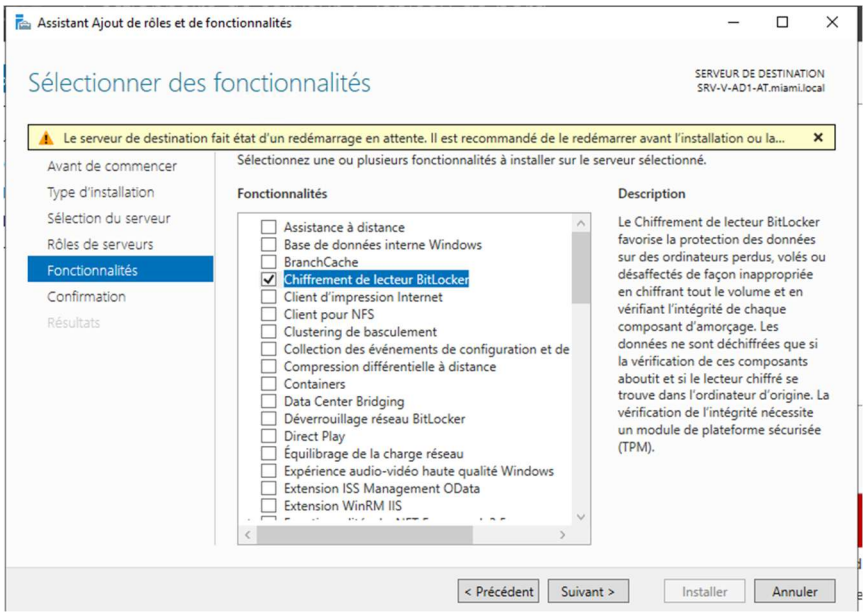
Activer les clichés instantanés

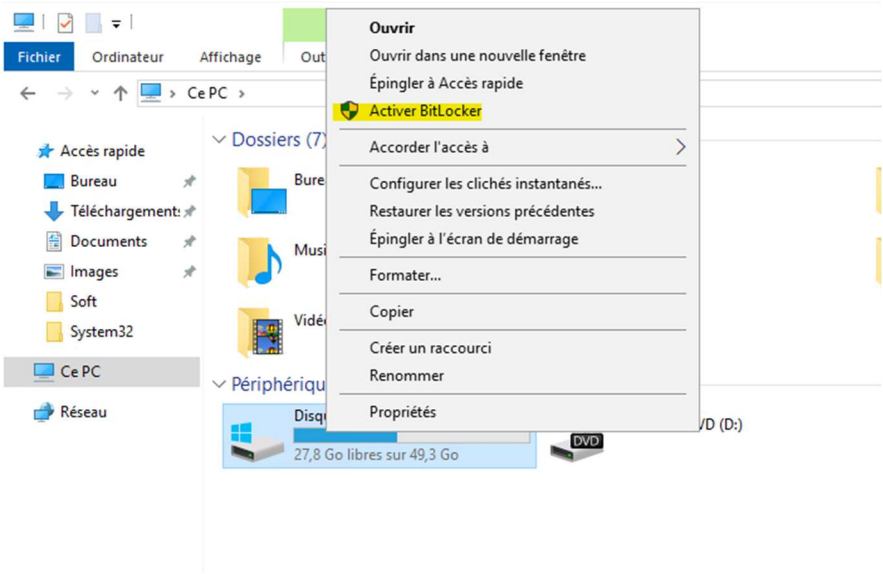
La 6eme étape va être d'activer les clichés instantanés, ce qui permet de sauvegarder et de faire un instant afin de restaurer les données en cas de besoin. Cette fonctionnalité crée des copies de sauvegarde des fichiers à des moments précis, ce qui facilite la récupération des données en cas de perte ou de corruption.



Activer BitLocker

La 7eme étape est, bien entendu, d'activer BitLocker pour protéger les données sensibles sur nos serveurs. BitLocker chiffre les disques durs, rendant les données illisibles pour toute personne non autorisée. En cas de vol ou de perte de l'appareil, les informations restent sécurisées car elles sont chiffrées



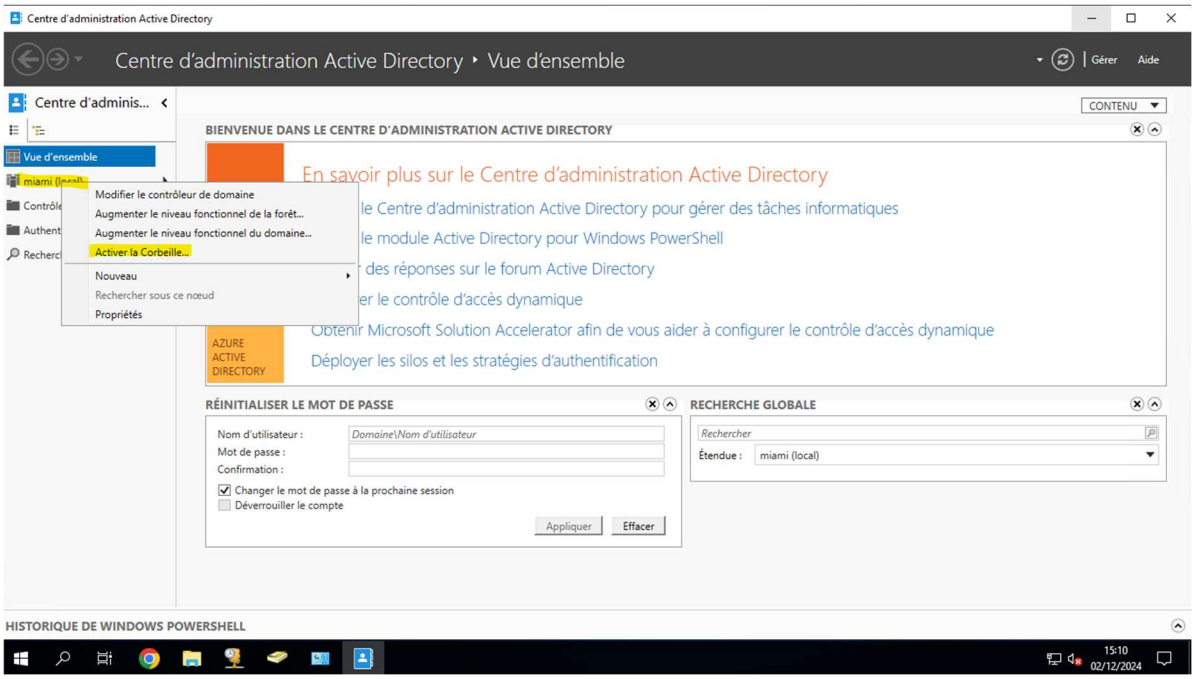


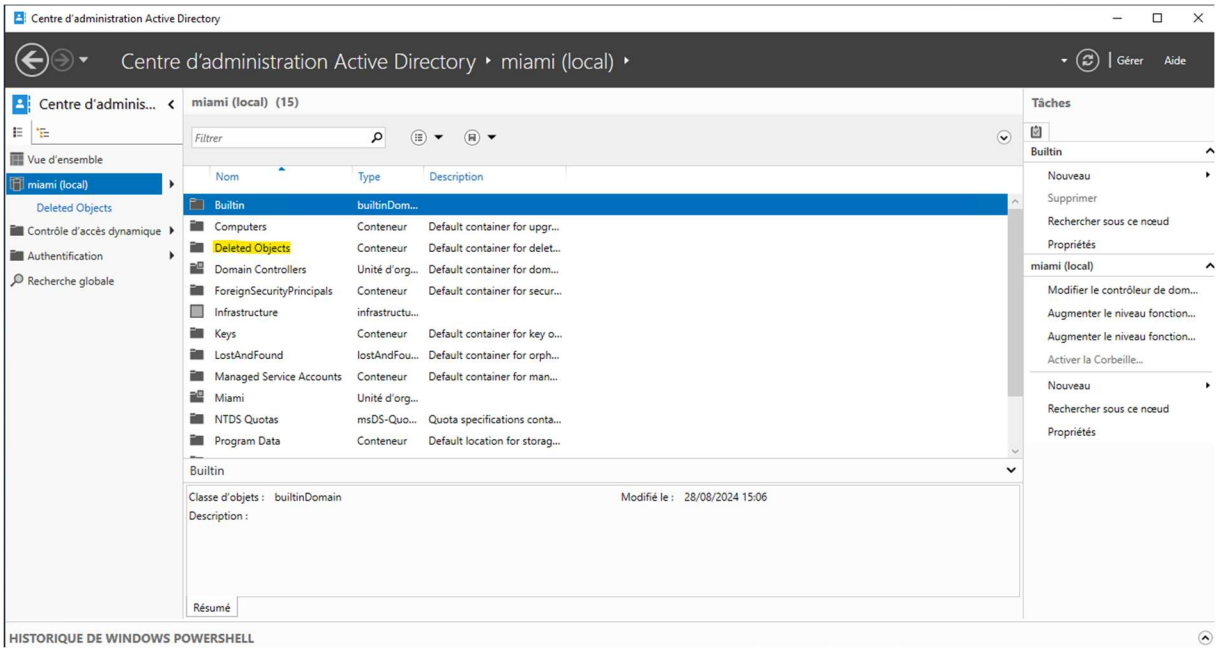
Il suffit ensuite de suivre les étape et surtout de bien conserver la clé de récupération dans un endroit sur.

2. Sécurisation d'un contrôleur de domaine Active Directory

Activer la corbeille AD

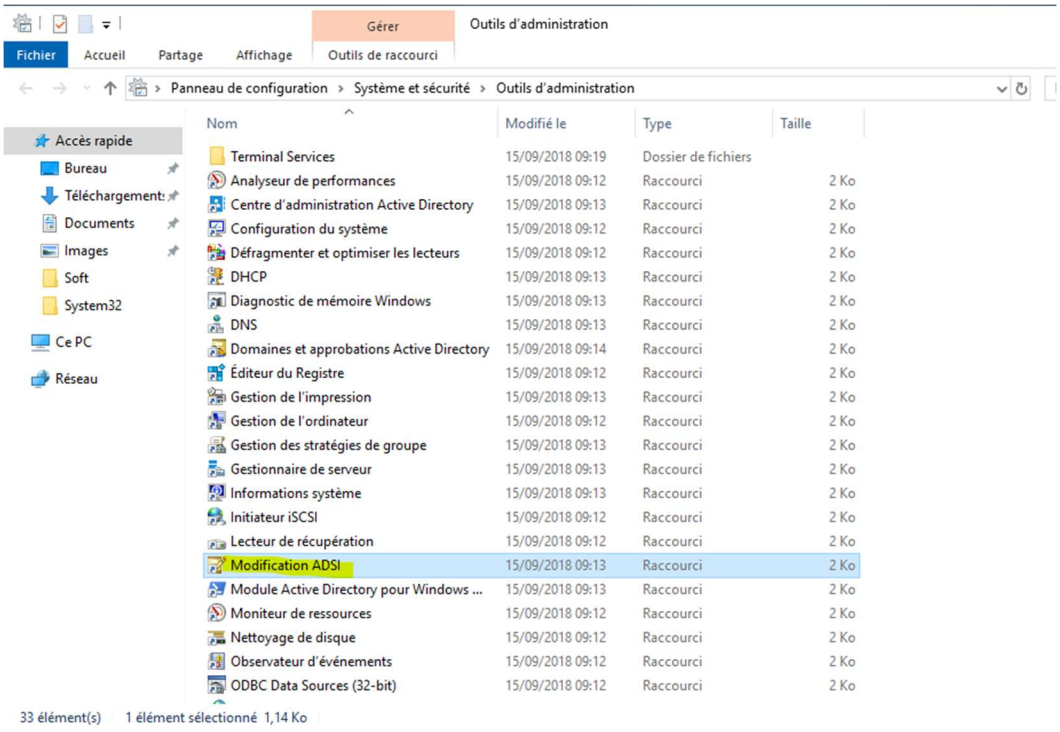
La première étape consiste à activer la corbeille AD. Cette fonctionnalité permet de restaurer facilement les objets supprimés, tels que les utilisateurs, groupes ou ordinateurs, sans avoir besoin de restaurer l'ensemble de la base de données AD.

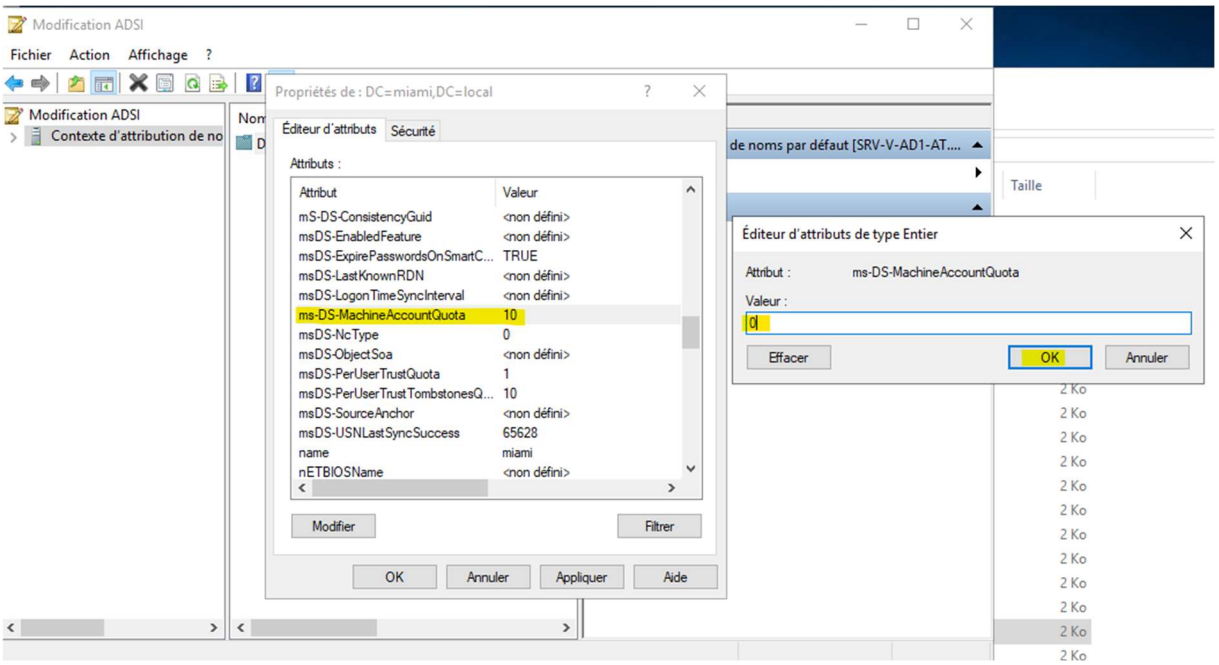




Modifier le quota d'utilisateur dans ADSI

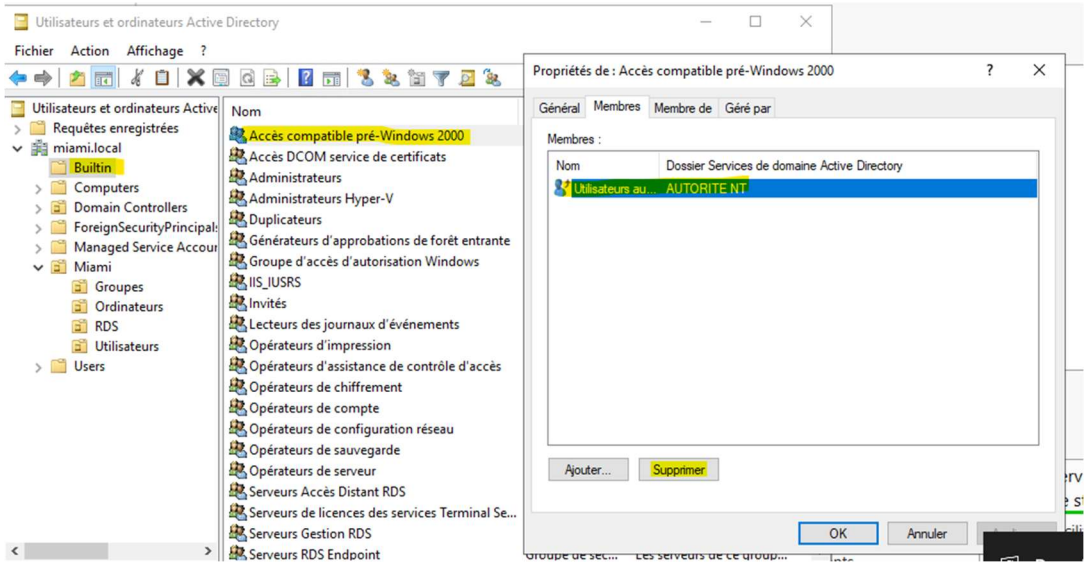
La deuxième étape consiste à modifier le quota d'utilisateur qui ont le droit d'entrer dans ordinateur au domaine dans modificateur ADSI de 10 (par défaut) à 0. Cela permet de limiter les permissions par défaut et empêche les utilisateurs non autorisés d'ajouter des machines au domaine, renforçant ainsi la sécurité globale du réseau.





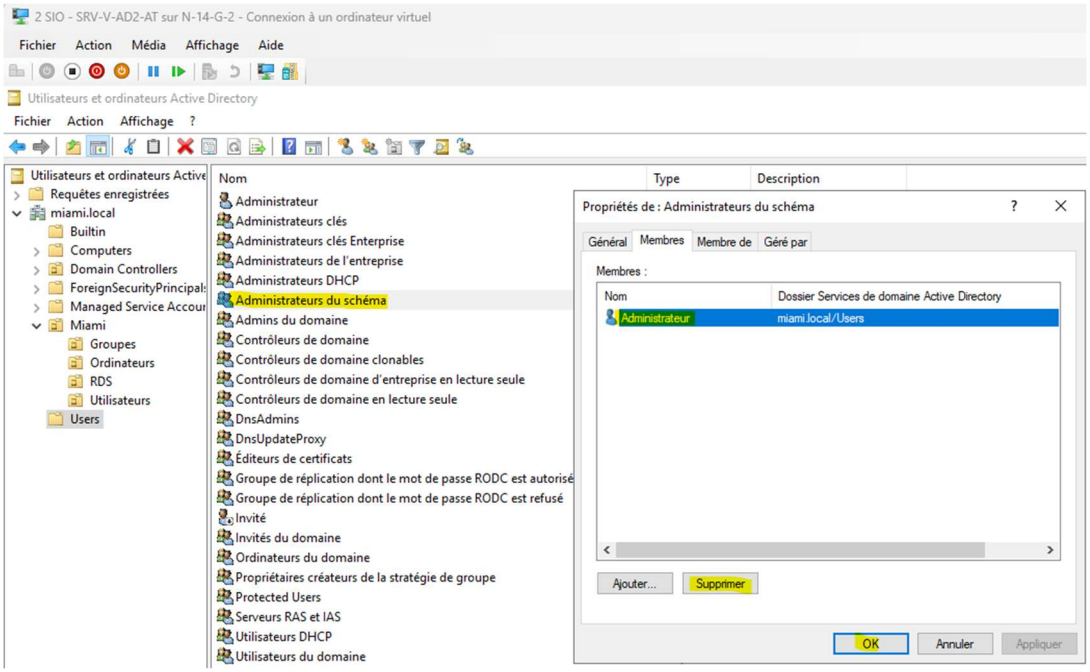
Supprimer "Utilisateur authentifié du groupe Accès compatible pré-Windows 2000

En réduisant les permissions par défaut, nous pouvons limiter l'accès aux ressources du réseau.



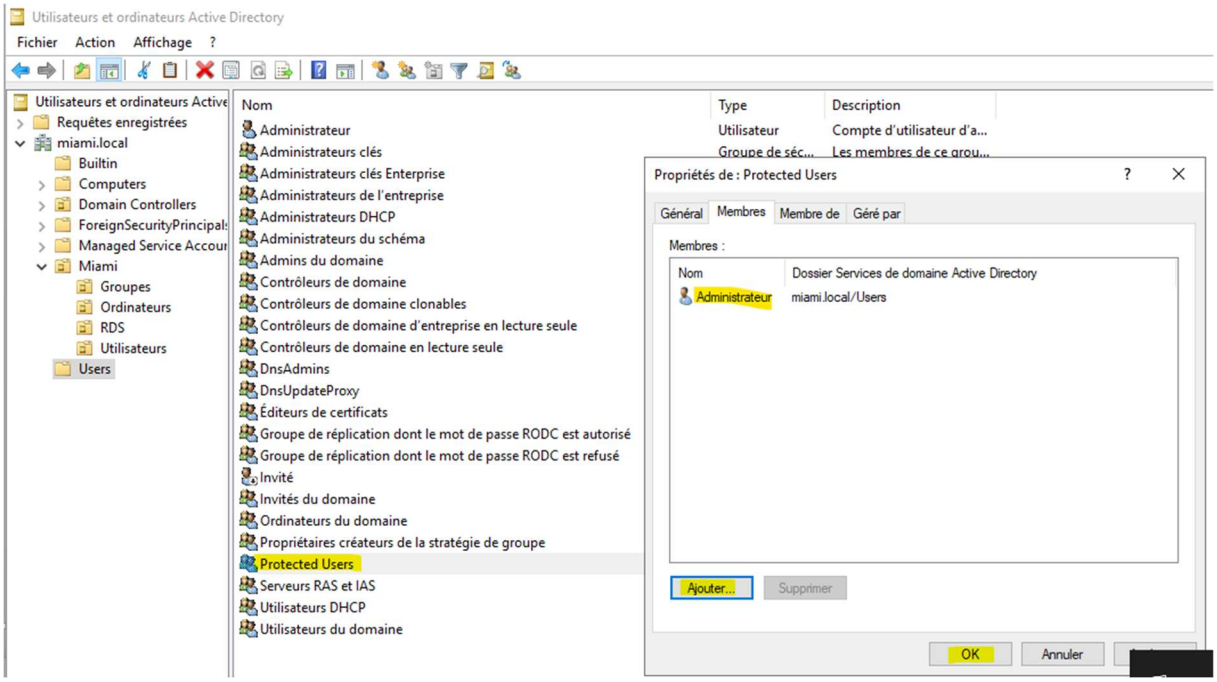
Supprimer "Administrateur" du groupe "Administrateur du schéma"

Cela va permettre de limiter les privilèges des comptes administrateur. En bloquant l'accès aux modifications du schéma, nous réduisons les risques de modifications qui pourraient compromettre la sécurité du Controleur de Domaine.



Ajouter "Administrateur" au groupe "Protected Users"

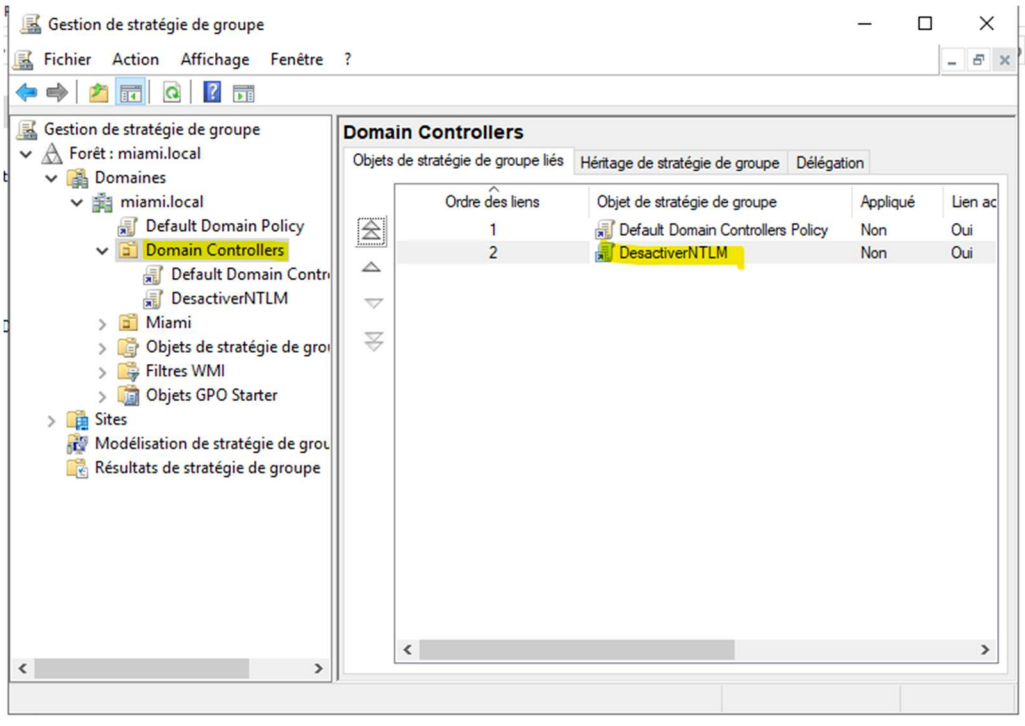
Les membres de ce groupe ont des protections supplémentaires contre les attaques, telles que l'impossibilité d'utiliser des protocoles d'authentification faibles et le fait qu'aucune machine ne garde en cache les hachages des mots de passes des comptes administrateur de notre domaine.

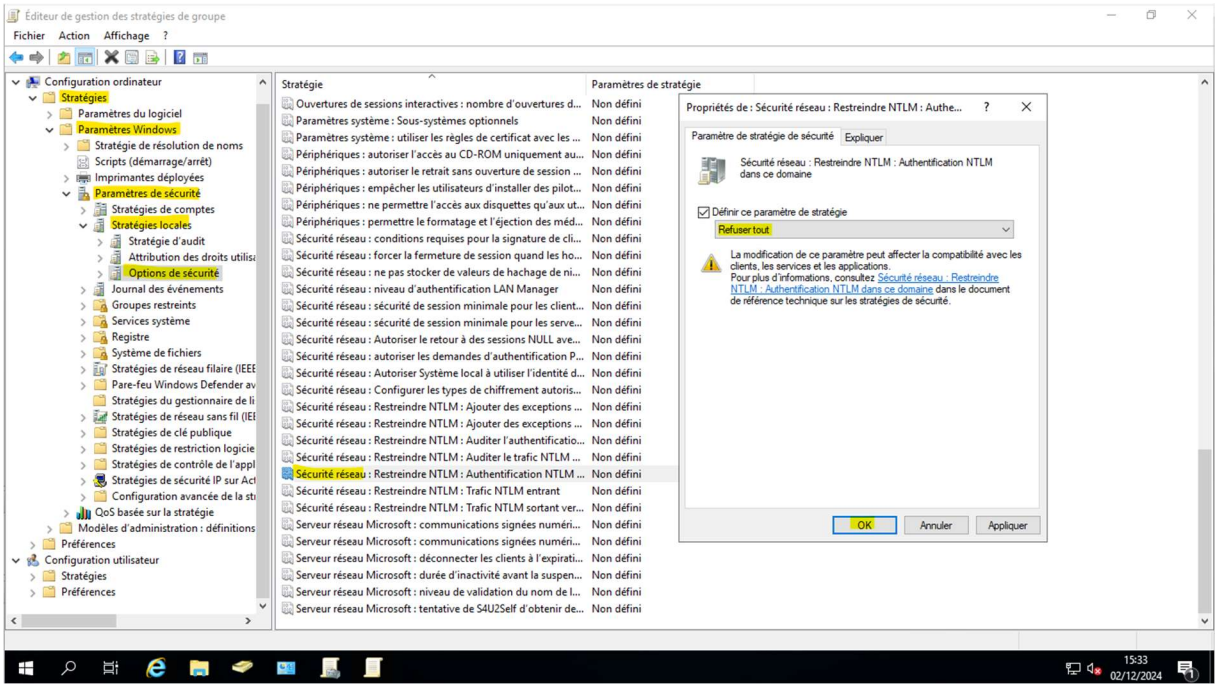


GPO pour désactiver NTLM

La dernière étape va donc être de créer une stratégie de groupe pour désactiver NTLM. NTLM est un protocole obsolète et vulnérable aux attaques. En le désactivant, nous forçons l'utilisation de protocoles plus modernes et sécurisés, tels que Kerberos.

NTLM est considéré comme moins sécurisé que les protocoles modernes comme Kerberos, car il est vulnérable à plusieurs types d'attaques, notamment les attaques par force brute.




Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Configuration ordinateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Stratégie de résolution de noms
Scripts (démarrage/arrêt)
Imprimantes déployées
Paramètres de sécurité
Stratégies de comptes
Stratégies locales
Stratégie d'audit
Attribution des droits utilisa
Options de sécurité
Journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de réseau filaire (IEEE
Pare-feu Windows Defender av
Stratégies du gestionnaire de li
Stratégies de réseau sans fil (IE
Stratégies de clé publique
Stratégies de restriction logicie
Stratégies de contrôle de l'appl
Stratégies de sécurité IP sur Act
Configuration avancée de la st
QoS basée sur la stratégie
Modèles d'administration : définitions
Préférences
Configuration utilisateur
Stratégies
Préférences
Stratégie
Paramètres de stratégie
Ouvertures de sessions interactives : nombre d'ouvertures d... Non défini
Paramètres système : Sous-systèmes optionnels Non défini
Paramètres système : utiliser les règles de certificat avec les ... Non défini
Périphériques : autoriser l'accès au CD-ROM uniquement au... Non défini
Périphériques : autoriser le retrait sans ouverture de session ... Non défini
Périphériques : empêcher les utilisateurs d'installer des pilot... Non défini
Périphériques : ne permettre l'accès aux disquettes qu'aux ut... Non défini
Périphériques : permettre le formatage et l'éjection des méd... Non défini
Sécurité réseau : conditions requises pour la signature de cli... Non défini
Sécurité réseau : forcer la fermeture de session quand les ho... Non défini
Sécurité réseau : ne pas stocker de valeurs de hachage de ni... Non défini
Sécurité réseau : niveau d'authentification LAN Manager Non défini
Sécurité réseau : sécurité de session minimale pour les client... Non défini
Sécurité réseau : sécurité de session minimale pour les serve... Non défini
Sécurité réseau : Autoriser le retour à des sessions NULL ave... Non défini
Sécurité réseau : autoriser les demandes d'authentification P... Non défini
Sécurité réseau : Autoriser Système local à utiliser l'identité d... Non défini
Sécurité réseau : Configurer les types de chiffrement autoris... Non défini
Sécurité réseau : Restreindre NTLM : Ajouter des exceptions ... Non défini
Sécurité réseau : Restreindre NTLM : Ajouter des exceptions ... Non défini
Sécurité réseau : Restreindre NTLM : Auditer l'authentificatio... Non défini
Sécurité réseau : Restreindre NTLM : Auditer le trafic NTLM ... Non défini
Sécurité réseau : Restreindre NTLM : Authentification NTLM ... Non défini
Sécurité réseau : Restreindre NTLM : Trafic NTLM entrant Non défini
Sécurité réseau : Restreindre NTLM : Trafic NTLM sortant ver... Non défini
Serveur réseau Microsoft : communications signées numéri... Non défini
Serveur réseau Microsoft : communications signées numéri... Non défini
Serveur réseau Microsoft : déconnecter les clients à l'expirati... Non défini
Serveur réseau Microsoft : durée d'inactivité avant la suspen... Non défini
Serveur réseau Microsoft : niveau de validation du nom de l... Non défini
Serveur réseau Microsoft : tentative de S4U2Self d'obtenir de... Non défini
Propriétés de : Sécurité réseau : Restreindre NTLM : Authe...
Paramètre de stratégie de sécurité
Expliquer
Sécurité réseau : Restreindre NTLM : Authentification NTLM dans ce domaine
Définir ce paramètre de stratégie
Refuser tout
La modification de ce paramètre peut affecter la compatibilité avec les clients, les services et les applications.
Pour plus d'informations, consultez Sécurité réseau : Restreindre NTLM : Authentification NTLM dans ce domaine dans le document de référence technique sur les stratégies de sécurité.
OK
Annuler
Appliquer
15:33
02/12/2024