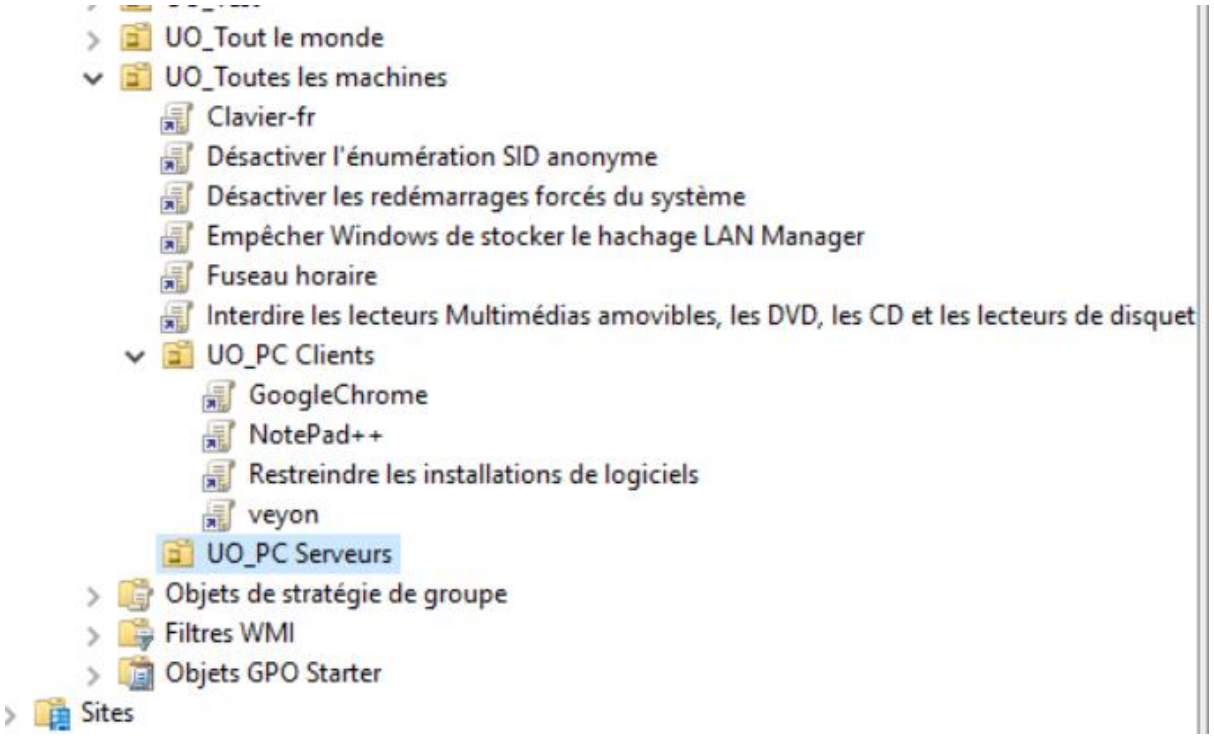
RÉALISATION D'ACTIVITÉS

5 GPO effectuées durant l'atelier :

- Désactiver l'énumération SIP anonyme
- Désactiver les redémarrages forcés du système
- Empêcher Windows de stocker le hachage LAN Manager
- Interdire les lecteurs Multimédias amovibles, les DVD, les CD et les lecteurs de disquettes
- Restreindre les installations de logiciels



1. **Désactiver l'énumération SID anonyme :**

Active Directory attribue un numéro unique à tous les objets de sécurité dans Active Directory ; y compris les utilisateurs, les groupes et autres, appelés numéros d'identificateurs de sécurité (SID). Dans les anciennes versions de Windows, les utilisateurs pouvaient interroger les SID pour identifier les utilisateurs et groupes importants. Cette disposition peut être exploitée par des pirates pour obtenir un accès non autorisé aux données. Par défaut, ce paramètre est désactivé, assurez-vous qu'il le reste. Effectuez les étapes suivantes :

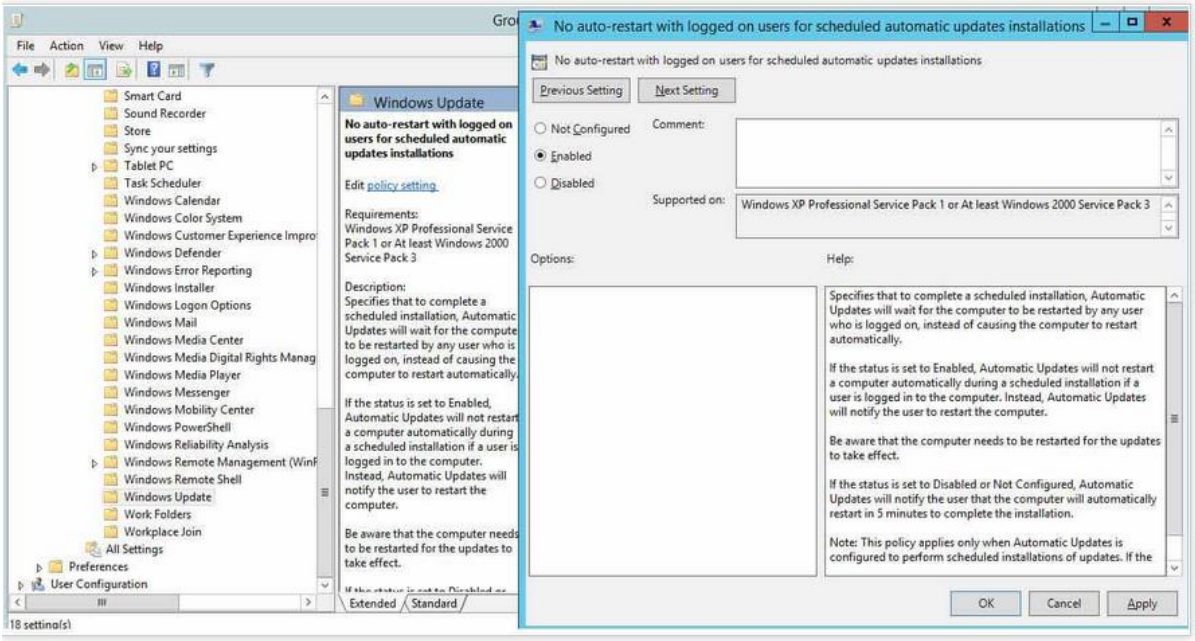
1. Dans la fenêtre de l'éditeur de gestion des stratégies de groupe, accédez à "Configuration de l'ordinateur" "Politiques" "Paramètres Windows" "Paramètres de sécurité" "Politiques locales" "Options de sécurité".
2. Dans le volet de droite, double-cliquez sur le paramètre de stratégie "Accès réseau : ne pas autoriser l'énumération anonyme des comptes et partages SAM".
3. Choisissez « Activé », puis cliquez sur « Appliquer » et « OK » pour enregistrer vos paramètres.

2. Désactiver les redémarrages forcé du système :

Les redémarrages forcés du système sont courants. Par exemple, vous pouvez être confronté à une situation où vous travaillez sur votre ordinateur et Windows affiche un message indiquant que votre système doit redémarrer en raison d'une mise à jour de sécurité.

Dans de nombreux cas, si vous ne remarquez pas le message ou si vous prenez un certain temps pour répondre, l'ordinateur redémarre automatiquement et vous perdez un travail important non enregistré.

1. Dans la fenêtre "Group Policy Management Editor" (ouverte pour un GPO personnalisé), accédez à "Configuration de l'ordinateur" "Modèles d'administration" "Composant Windows" "Windows Update".
2. Dans le volet de droite, double-cliquez sur la stratégie "Pas de redémarrage automatique avec les utilisateurs connectés pour les installations de mises à jour automatiques planifiées".
3. Cliquez sur "Activé" pour activer la politique.
4. Cliquez sur "Appliquer" et "OK".

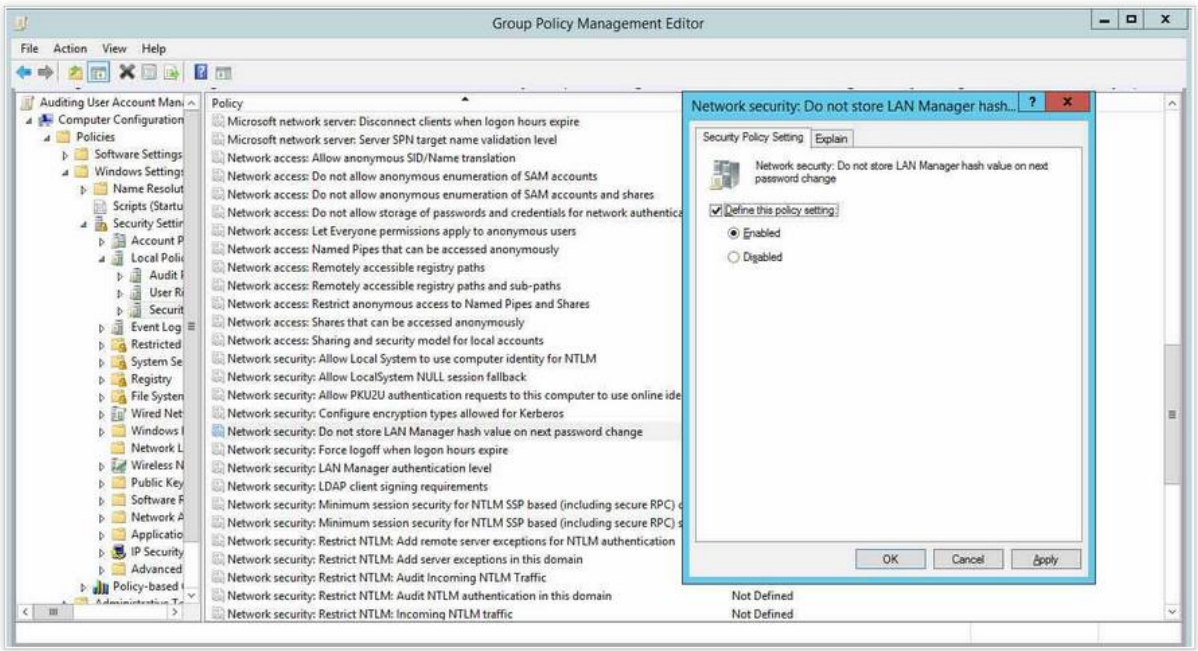


3. Empêcher Windows de stocker le hachage LAN Manager :

Windows génère et stocke les mots de passe des comptes d'utilisateurs dans des "hachages". Windows génère à la fois un hachage LAN Manager (hachage LM) et un hachage Windows NT (hachage NT) des mots de passe. Il les stocke dans la base de données locale du gestionnaire de comptes de sécurité (SAM) ou dans Active Directory.

Le hachage LM est faible et sujet au piratage. Par conséquent, vous devez empêcher Windows de stocker un hachage LM de vos mots de passe.

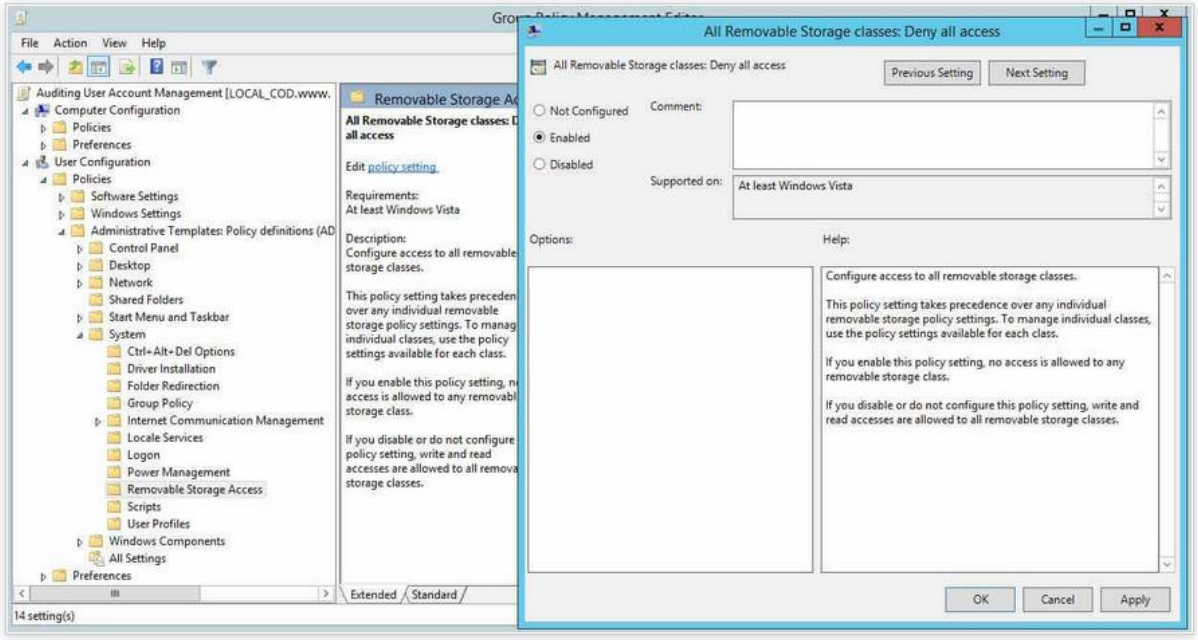
1. Dans la fenêtre de l'éditeur de gestion des stratégies de groupe (ouverte pour un GPO personnalisé), accédez à "Configuration de l'ordinateur" "Paramètres Windows" "Paramètres de sécurité" "Politiques locales" "Options de sécurité".
2. Dans le volet de droite, double-cliquez sur la stratégie "Sécurité réseau : ne pas stocker la valeur de hachage LAN Manager lors du prochain changement de mot de passe".
3. Cochez la case "Définir ce paramètre de stratégie" et cliquez sur "Activé".
4. Cliquez sur "Appliquer" et "OK".



4. **Interdire les lecteurs de supports amovibles, les DVD, les CD et les lecteurs de disquette :**

Les lecteurs de supports amovibles sont très sujets aux infections et peuvent également contenir un virus ou un logiciel malveillant. Si un utilisateur branche un lecteur infecté sur un ordinateur du réseau, cela peut affecter l'ensemble du réseau. De même, les DVD, les CD et les lecteurs de disquettes sont sujets aux infections.

1. Dans la fenêtre de l'éditeur de gestion des stratégies de groupe (ouverte pour un GPO personnalisé), accédez à "Configuration utilisateur" "Politiques" "Modèles d'administration" "Système" "Accès au stockage amovible".
2. Dans le volet de droite, double-cliquez sur la stratégie "Toutes les classes de stockage amovibles : Refuser tous les accès"
3. Cliquez sur "Activé" pour activer la politique.
4. Cliquez sur "Appliquer" et "OK".



5. **Restreindre les installations de logiciels :**

Lorsque vous donnez aux utilisateurs la liberté d'installer des logiciels, ils peuvent installer des applications indésirables qui compromettent votre système. Les administrateurs système devront généralement effectuer régulièrement la maintenance et le nettoyage de ces systèmes. Pour plus de sécurité, il est conseillé d'empêcher les installations de logiciels via la stratégie de groupe.

1. Dans l'éditeur de gestion des stratégies de groupe (ouvert pour un GPO personnalisé), accédez à "Configuration de l'ordinateur" "Modèles d'administration" "Composant Windows" "Windows Installer".
2. Dans le volet de droite, double-cliquez sur la stratégie "Interdire l'installation de l'utilisateur".
3. Cliquez sur "Activé" pour activer la politique
4. Cliquez sur "Appliquer" et "OK".