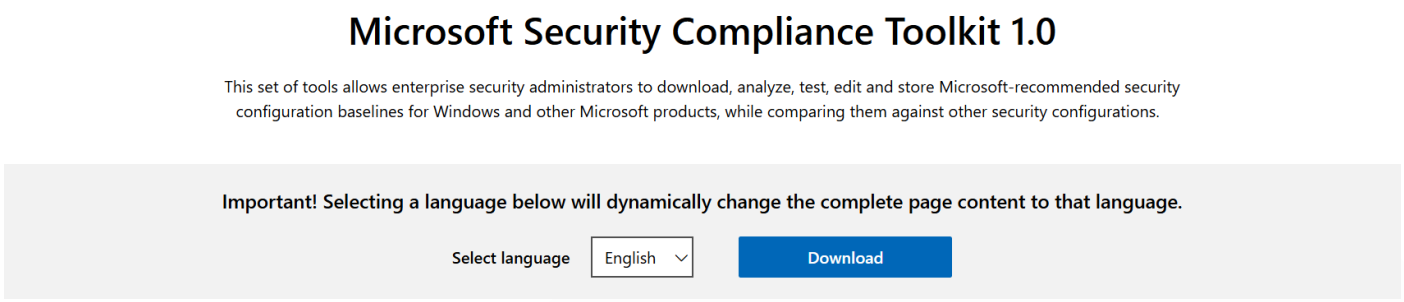
DEPLOIEMENT SCT

La Security Baseline (ou ligne de base de sécurité) est un ensemble de configurations de sécurité recommandées pour les systèmes d'exploitation ou applications, visant à réduire les risques de sécurité tout en maintenant la compatibilité fonctionnelle. Ces paramètres couvrent des domaines comme les politiques de mot de passe, les services réseau, ou les options de sécurité du système.

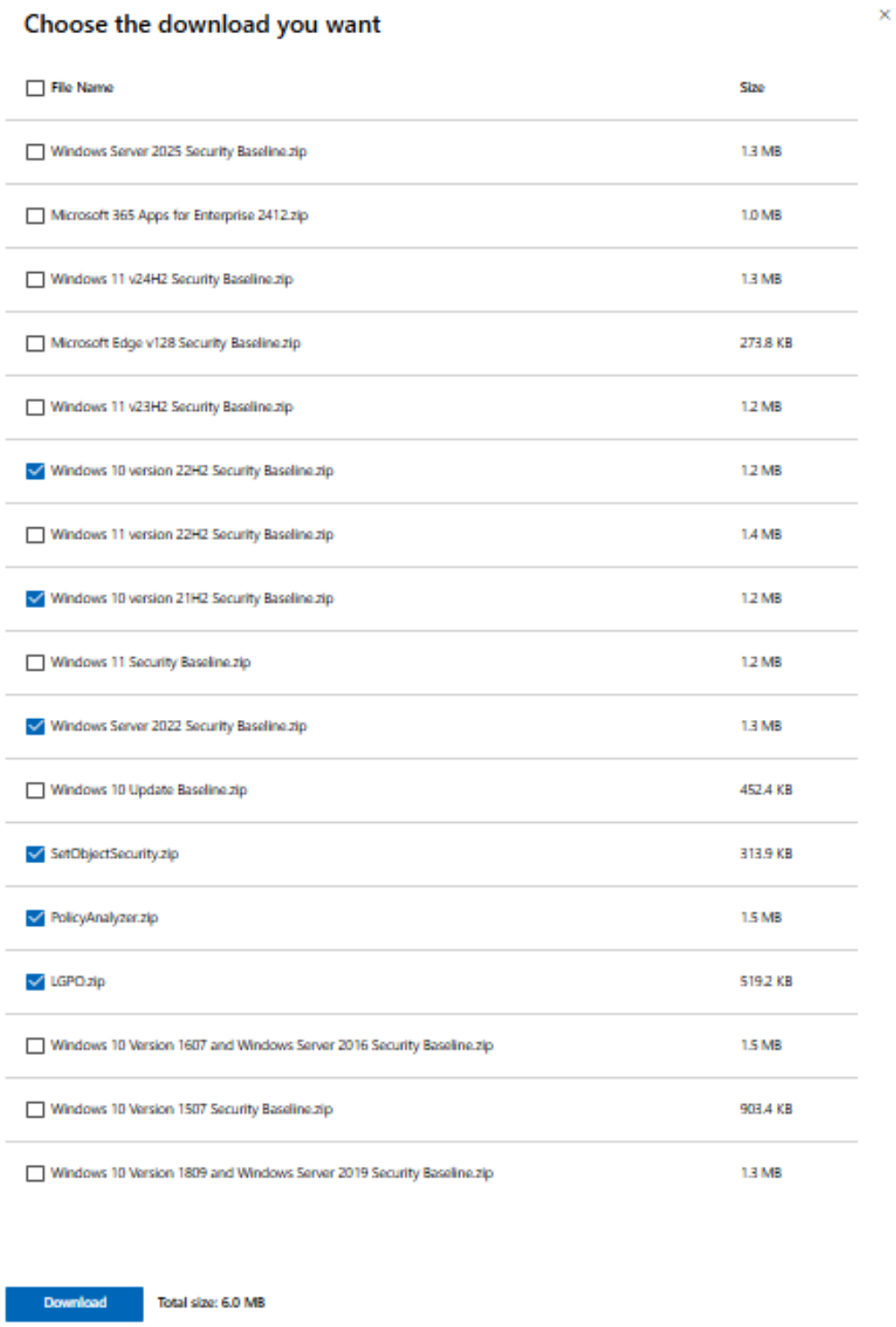
SCT (Security Compliance Toolkit) est un outil fourni par Microsoft qui permet d'appliquer, d'auditer et de comparer ces security baselines sur les systèmes Windows. Il aide les administrateurs à vérifier que leurs machines respectent les recommandations de sécurité de Microsoft

Je me rends sur ce lien pour télécharger windows security baseline toolkit :

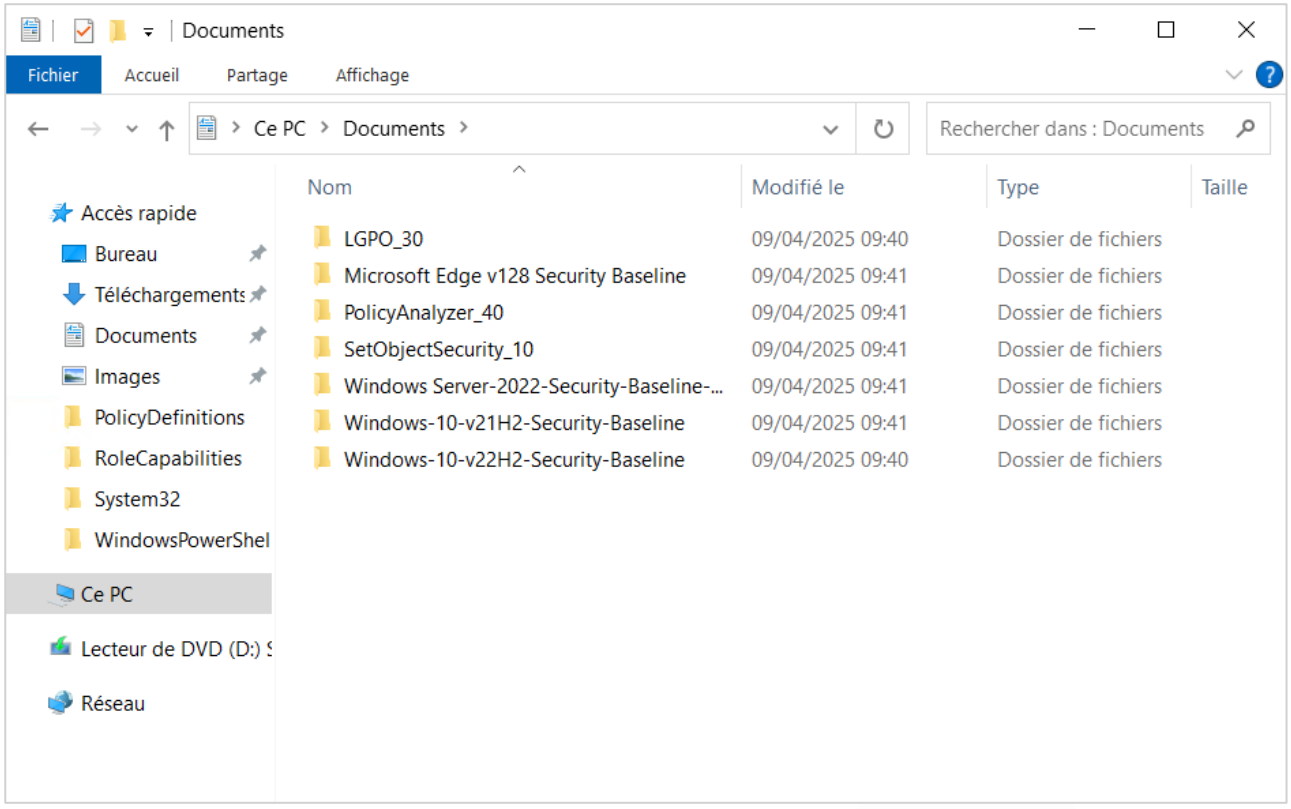
https://www.microsoft.com/en-us/download/details.aspx?id=55319

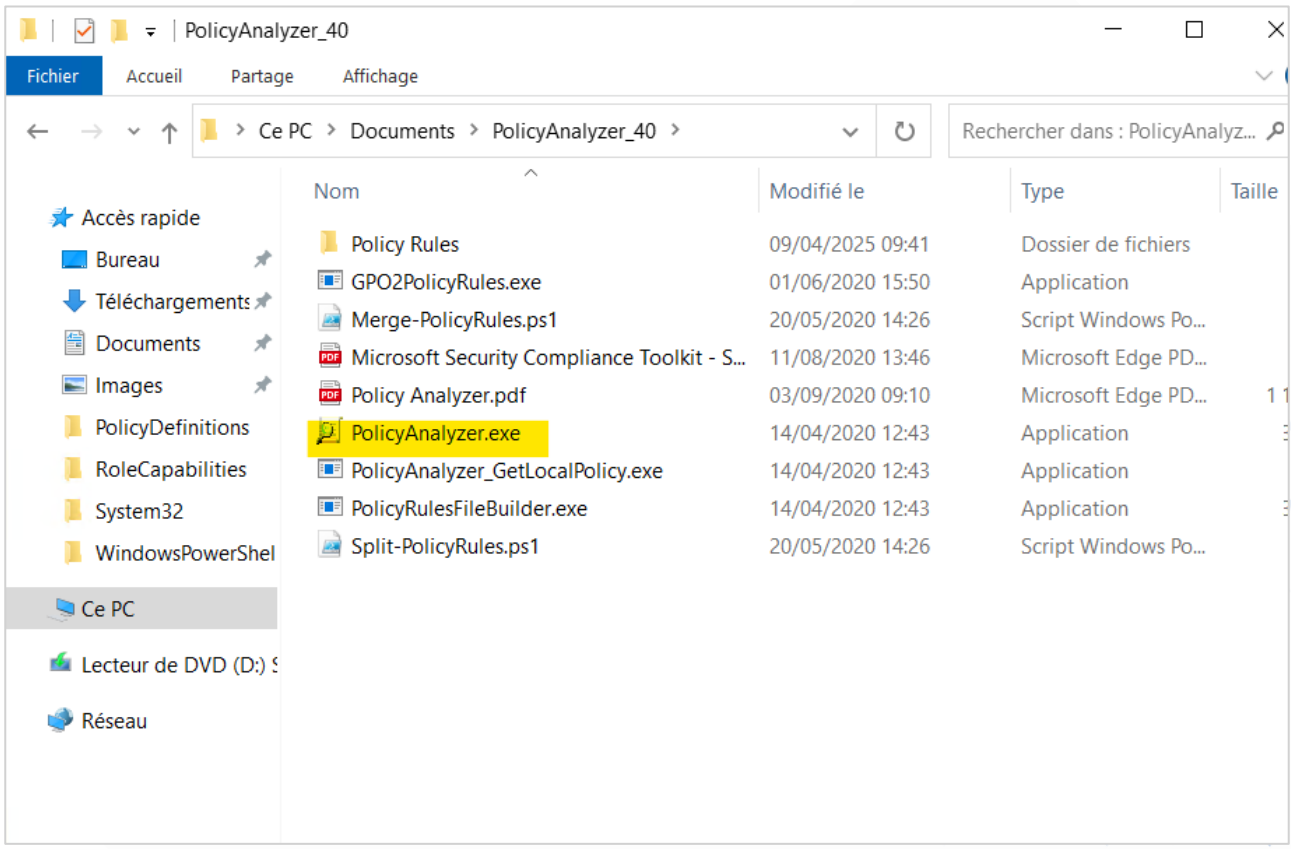


Je sélectionne les paramètres qui correspondent à mon infrastructure réseau, mais je ne configurerai SCT que dans le cadre de mon Windows server 2022, c'est donc ce fichier, ainsi que les trois derniers cochés qui m'intéressent en majorité :

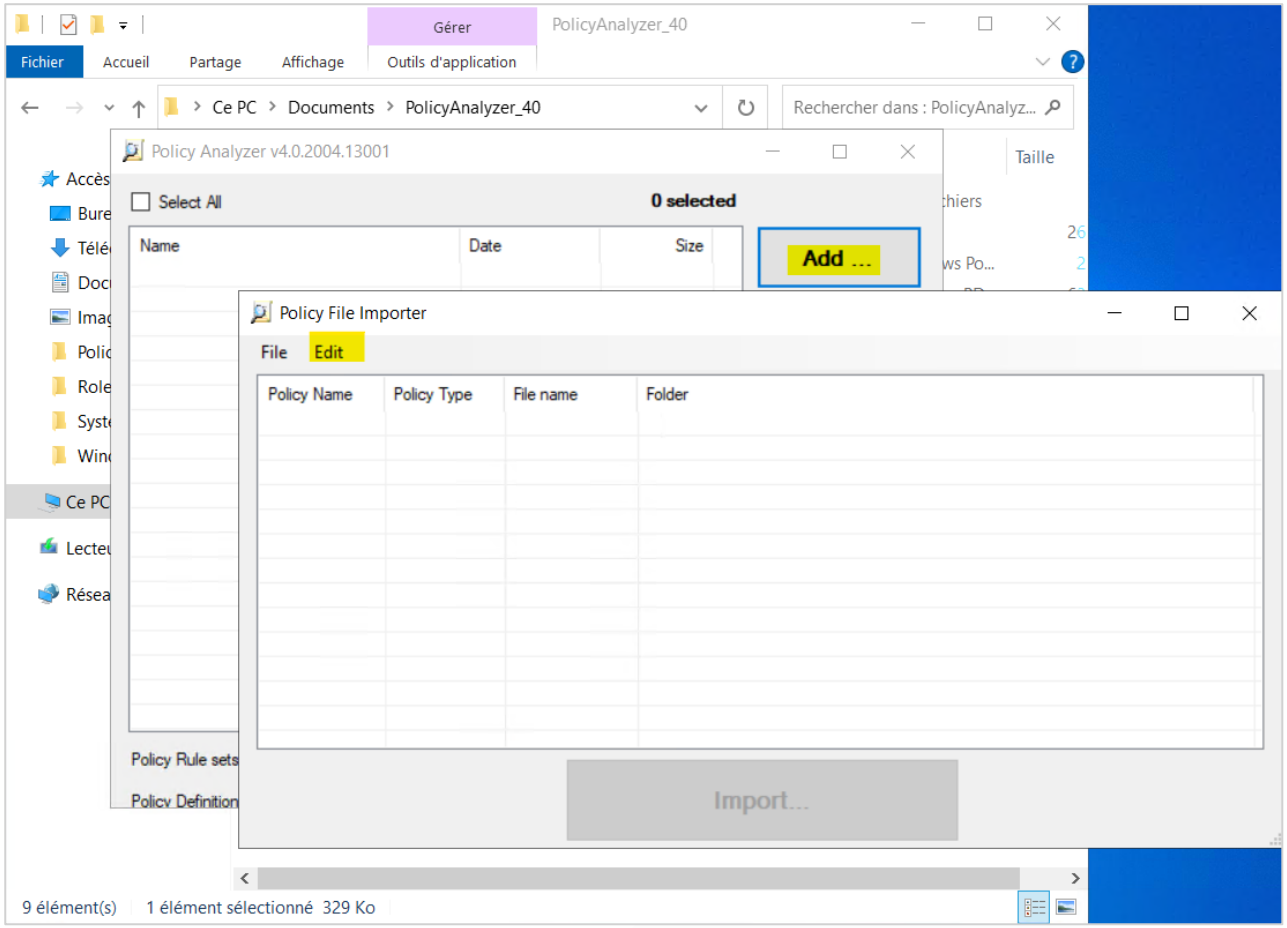


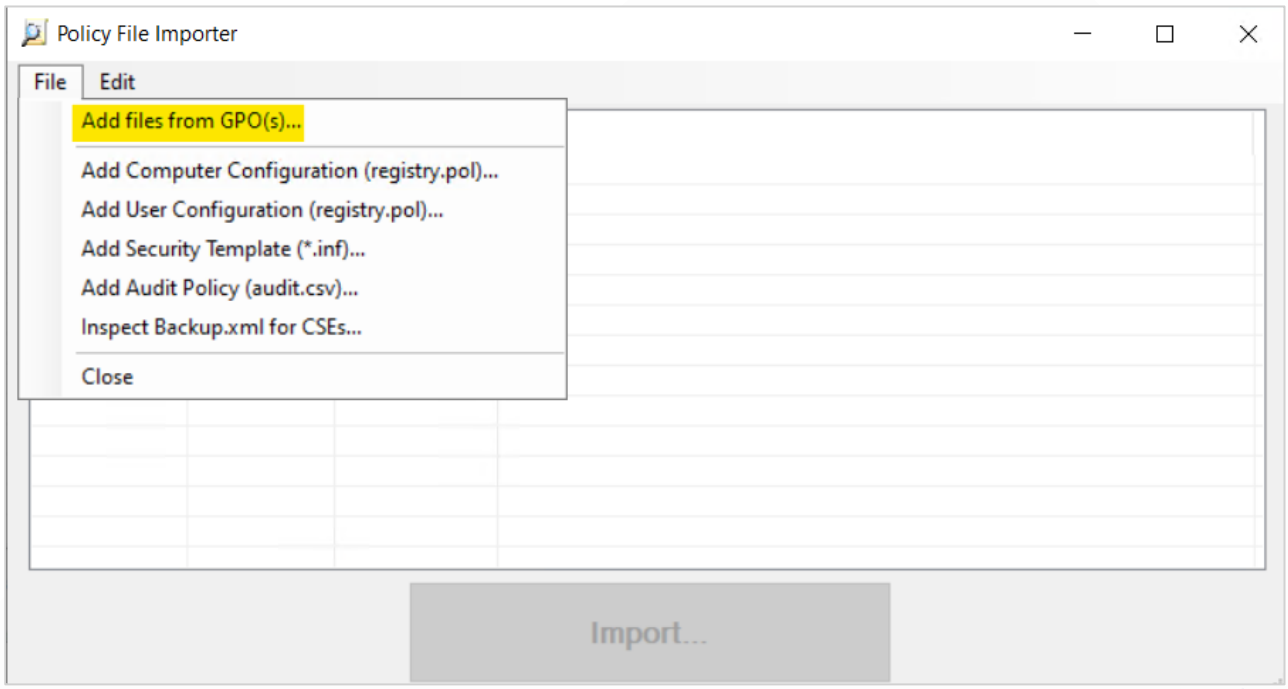
J'obtiens des fichiers zip que j'extrais, puis, je me rends dans le dossier PolicyAnalyzer et j'ouvre PolicyAnalyzer.exe.

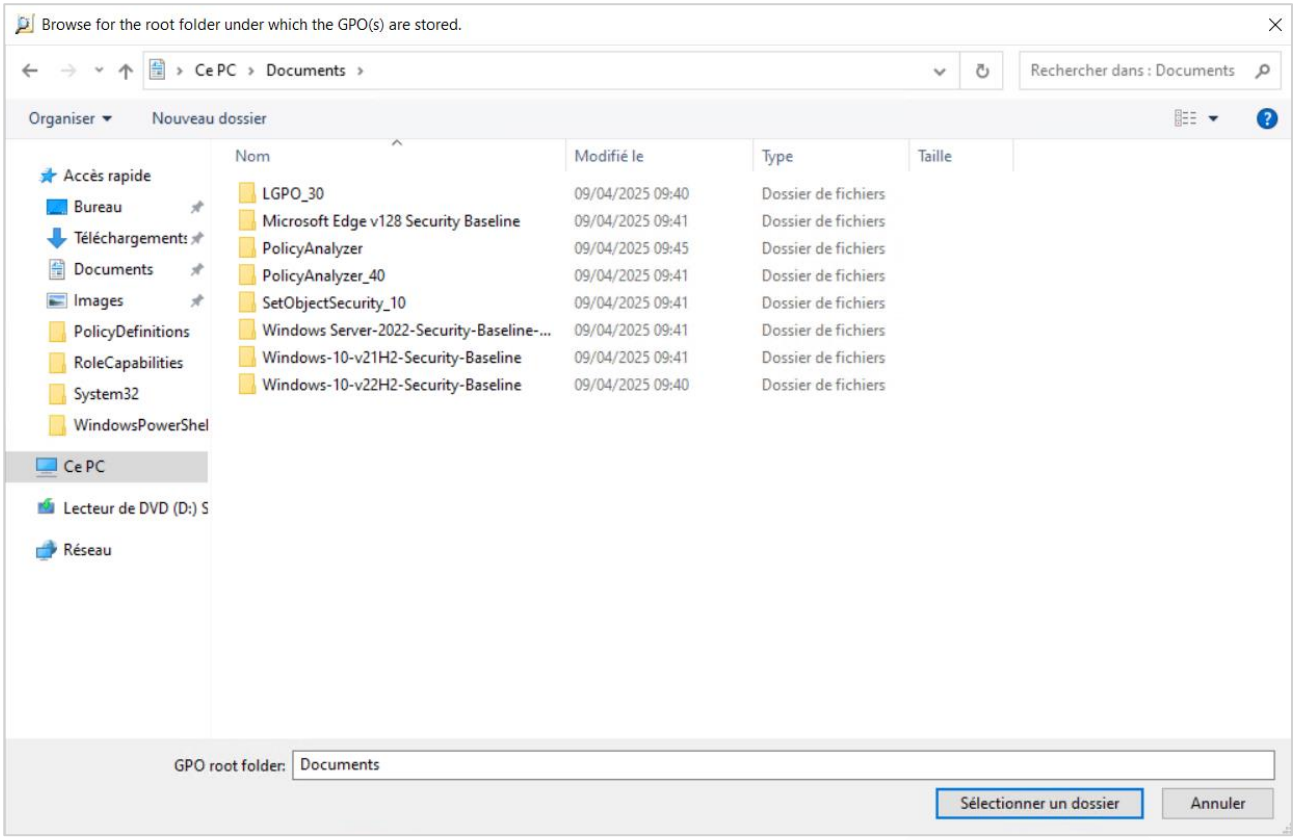


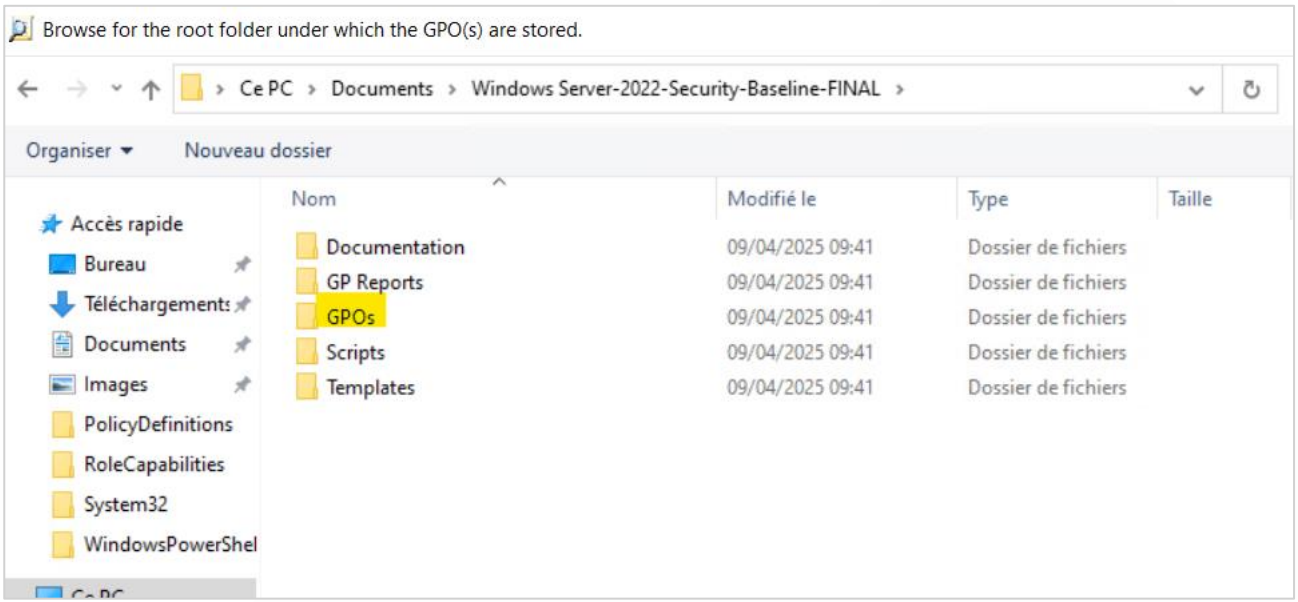


Une interface s'ouvre. J'appuie sur « **ADD** », puis « **File** », « **add files from GPO(s)...** », je cible le dossier qui m'intéresse, je me rends dans le dossier **GPOs** et sélectionne tout ce qu'il y a dedans.

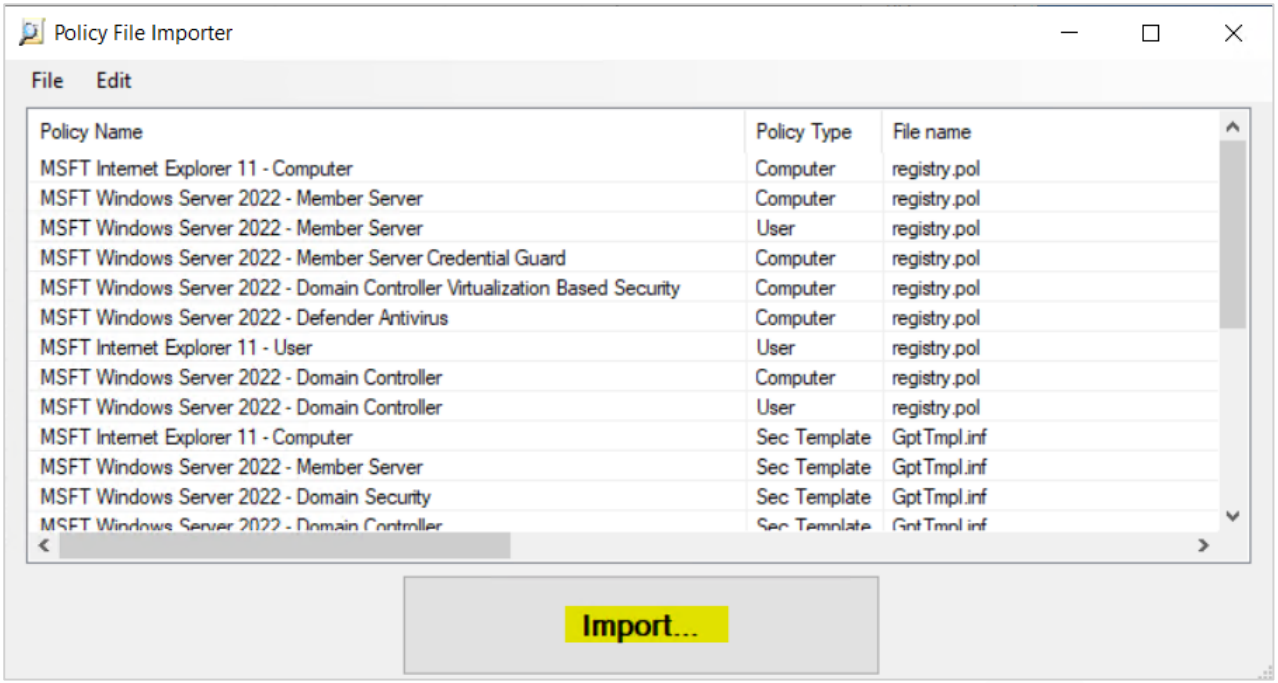

Gérer
PolicyAnalyzer_40
Fichier
Accueil
Partage
Affichage
Outils d'application
Ce PC › Documents › PolicyAnalyzer_40
Rechercher dans : PolicyAnalyz...
Policy Analyzer v4.0.2004.13001
Select All
0 selected
Name
Date
Size
Add ...
Taille
Policy Rule sets
Policy Definition
Policy File Importer
File
Edit
Policy Name
Policy Type
File name
Folder
Import...
9 élément(s)
1 élément sélectionné 329 Ko

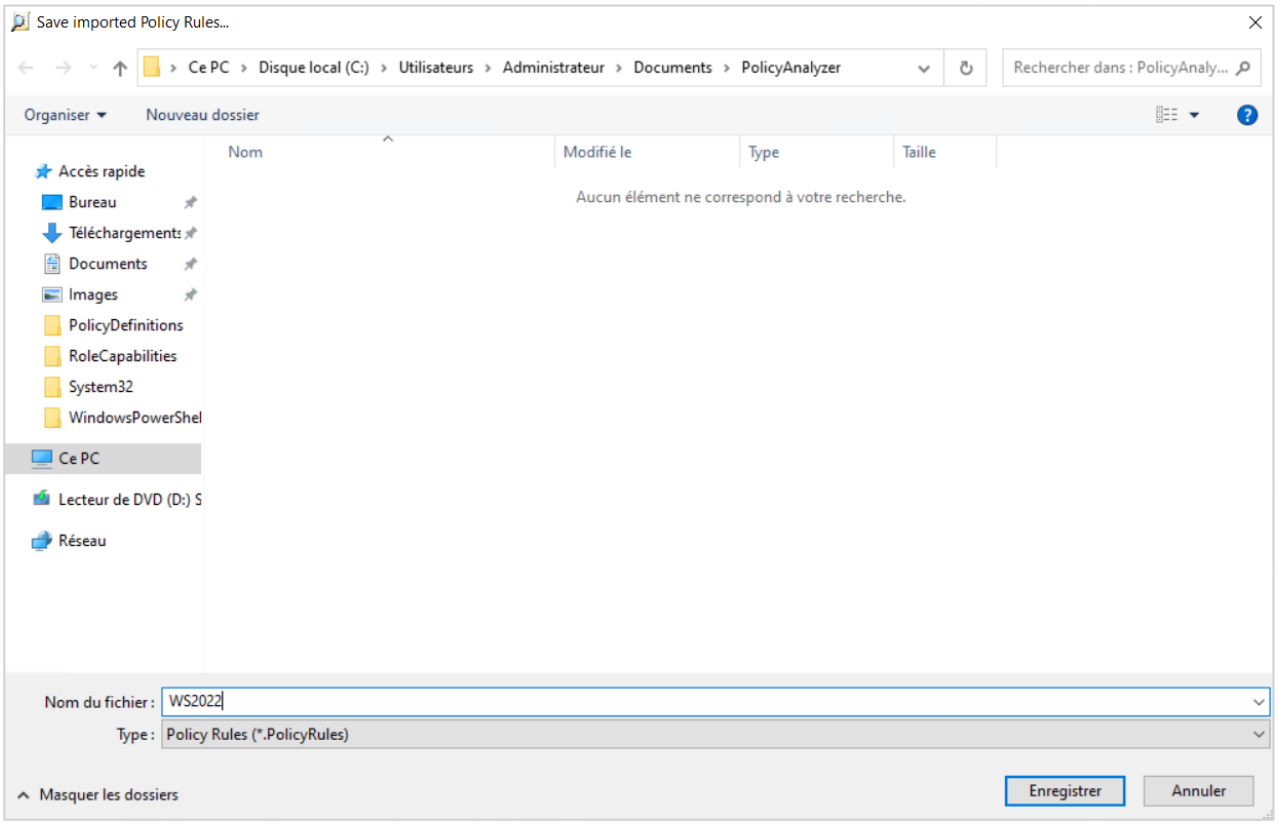

Policy File Importer
File
Edit
Add files from GPO(s)...
Add Computer Configuration (registry.pol)...
Add User Configuration (registry.pol)...
Add Security Template (*.inf)...
Add Audit Policy (audit.csv)...
Inspect Backup.xml for CSEs...
Close
Import...


Browse for the root folder under which the GPO(s) are stored.
Ce PC › Documents ›
Rechercher dans : Documents
Organiser
Nouveau dossier
Accès rapide
Bureau
Téléchargements
Documents
Images
PolicyDefinitions
RoleCapabilities
System32
WindowsPowerShel
Ce PC
Lecteur de DVD (D:) S
Réseau
Nom
Modifié le
Type
Taille
LGPO_30 09/04/2025 09:40 Dossier de fichiers
Microsoft Edge v128 Security Baseline 09/04/2025 09:41 Dossier de fichiers
PolicyAnalyzer 09/04/2025 09:45 Dossier de fichiers
PolicyAnalyzer_40 09/04/2025 09:41 Dossier de fichiers
SetObjectSecurity_10 09/04/2025 09:41 Dossier de fichiers
Windows Server-2022-Security-Baseline-... 09/04/2025 09:41 Dossier de fichiers
Windows-10-v21H2-Security-Baseline 09/04/2025 09:41 Dossier de fichiers
Windows-10-v22H2-Security-Baseline 09/04/2025 09:40 Dossier de fichiers
GPO root folder:
Documents
Sélectionner un dossier
Annuler

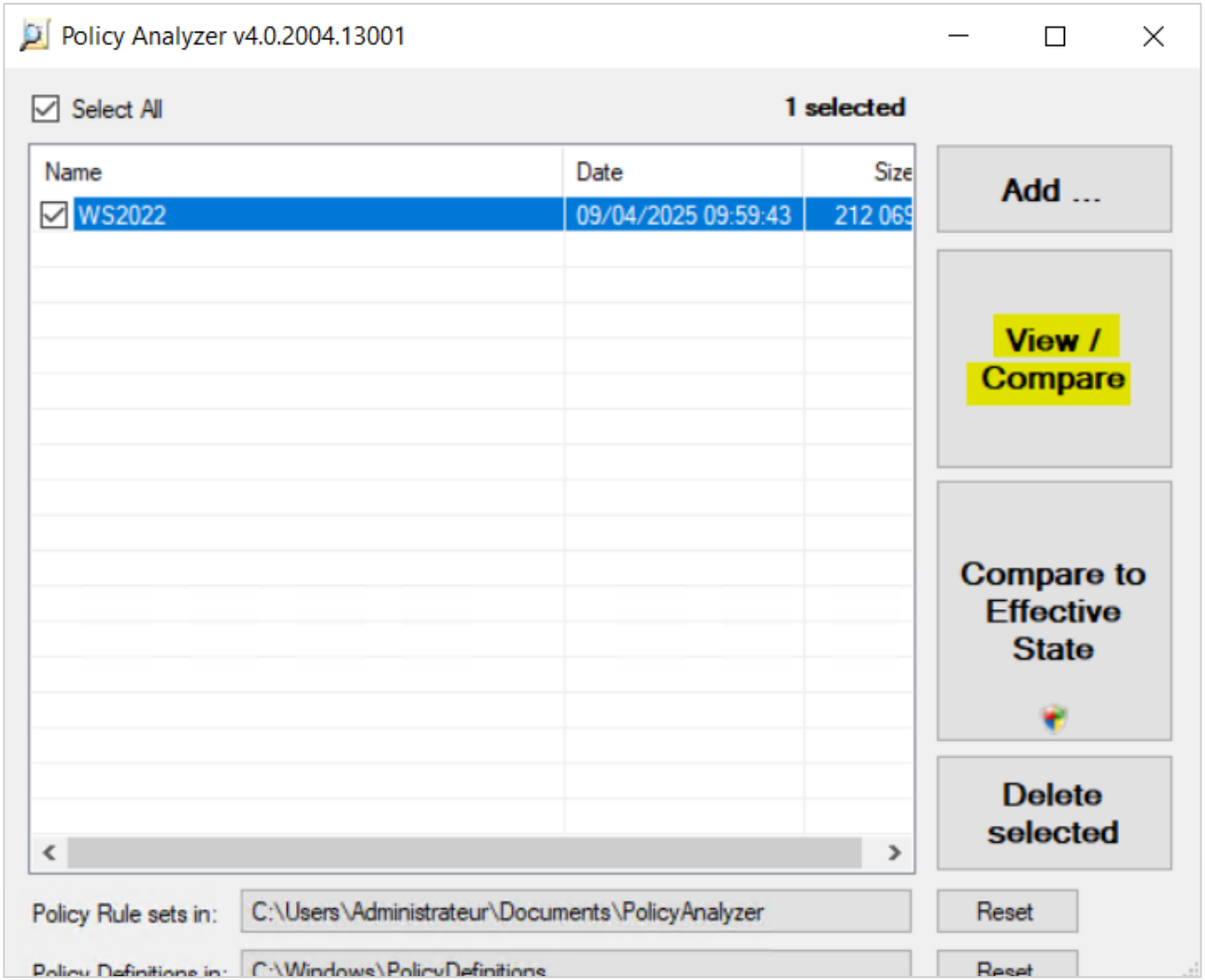

Browse for the root folder under which the GPO(s) are stored.
Ce PC › Documents › Windows Server-2022-Security-Baseline-FINAL ›
Organiser
Nouveau dossier
Accès rapide
Bureau
Téléchargements
Documents
Images
PolicyDefinitions
RoleCapabilities
System32
WindowsPowerShel
Nom
Modifié le
Type
Taille
Documentation 09/04/2025 09:41 Dossier de fichiers
GP Reports 09/04/2025 09:41 Dossier de fichiers
GPOs 09/04/2025 09:41 Dossier de fichiers
Scripts 09/04/2025 09:41 Dossier de fichiers
Templates 09/04/2025 09:41 Dossier de fichiers

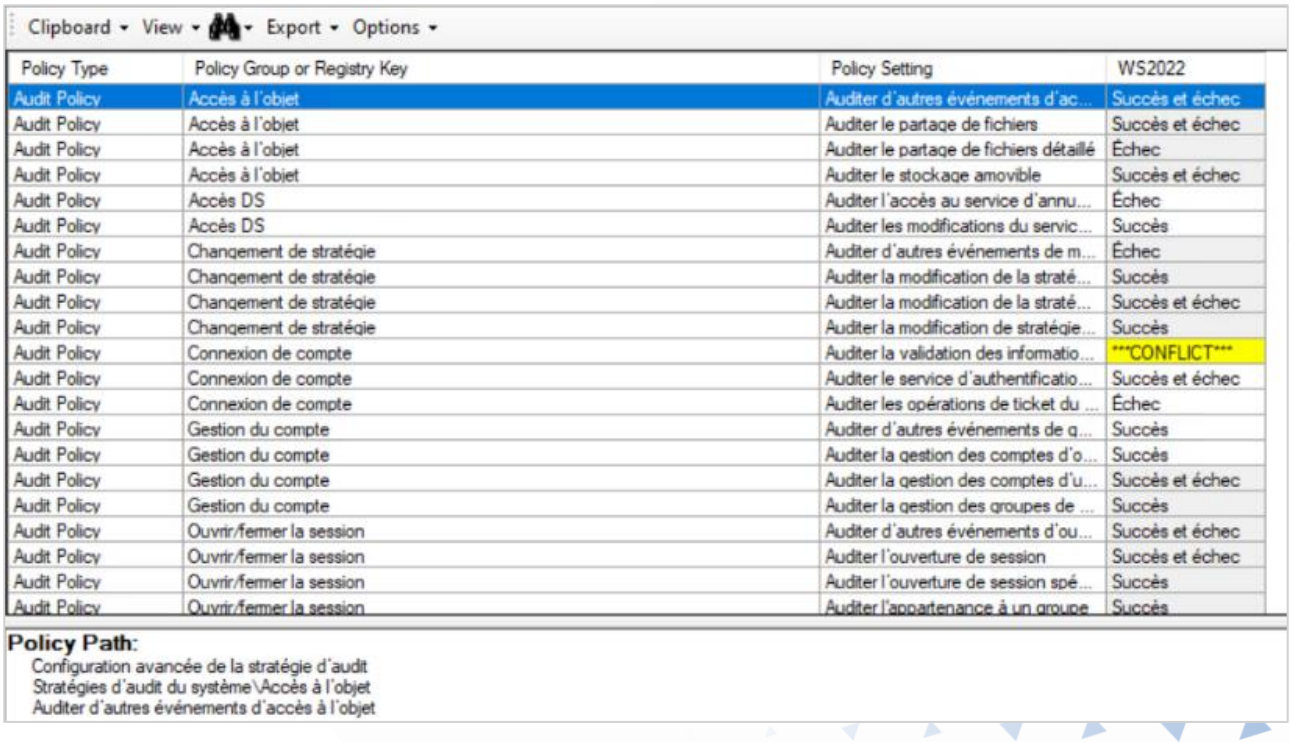
Cette fenêtre apparaît. Je sélectionne ce que je souhaite analyser (en maintenant shift ou ctrl pour en sélectionner plusieurs) et je clic donc sur « import ». Cela va me demander de créer un fichier que je nomme de façon à me souvenir quels paramètres celui-ci concerne.



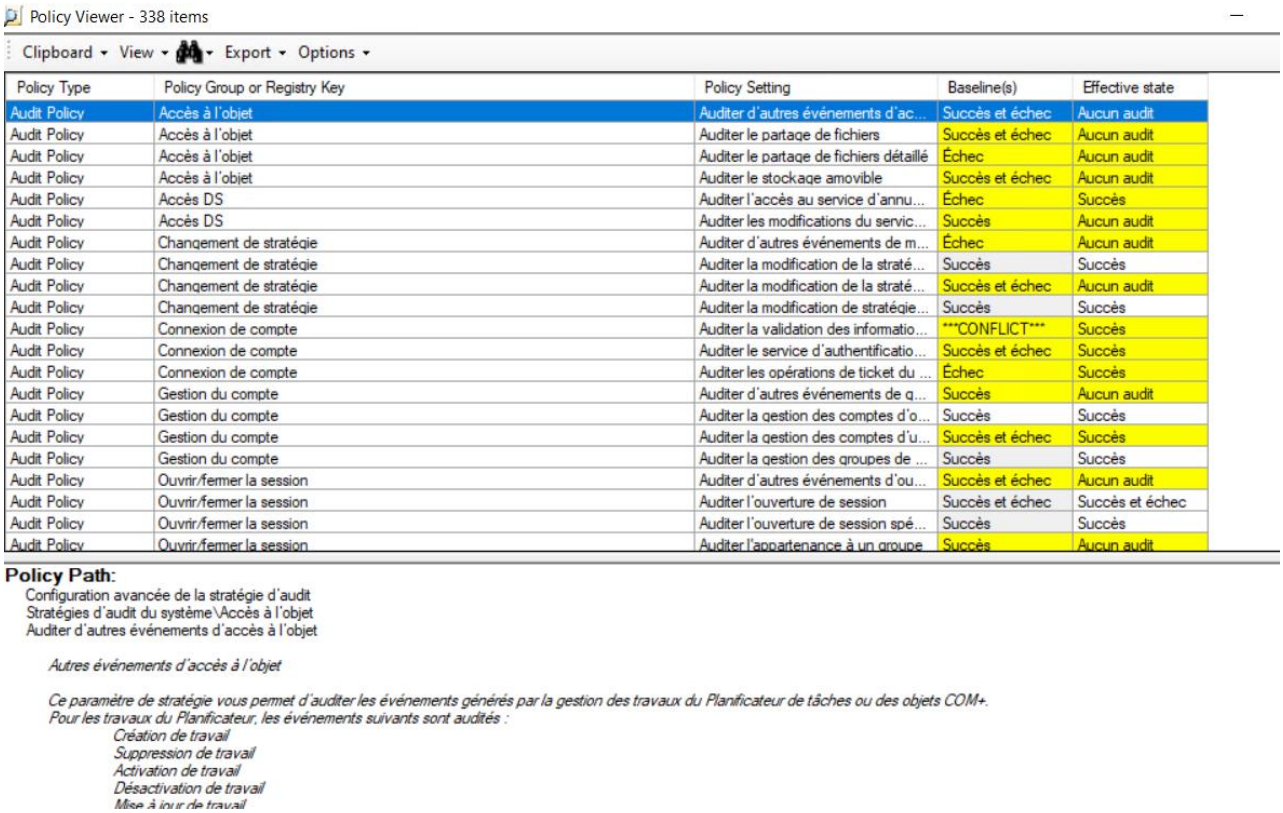


Je sélectionne le fichier et clic sur « view/compare » pour avoir une analyse des paramètres sélectionnés.





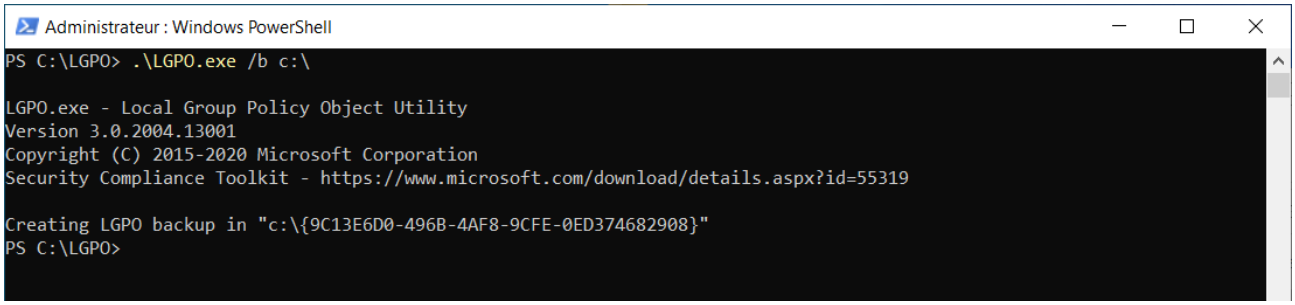
Je peux faire compare to effective state pour comparer avec ma configuration actuelle. En jaune apparaissent les paramètres que Microsoft me conseille d'appliquer.



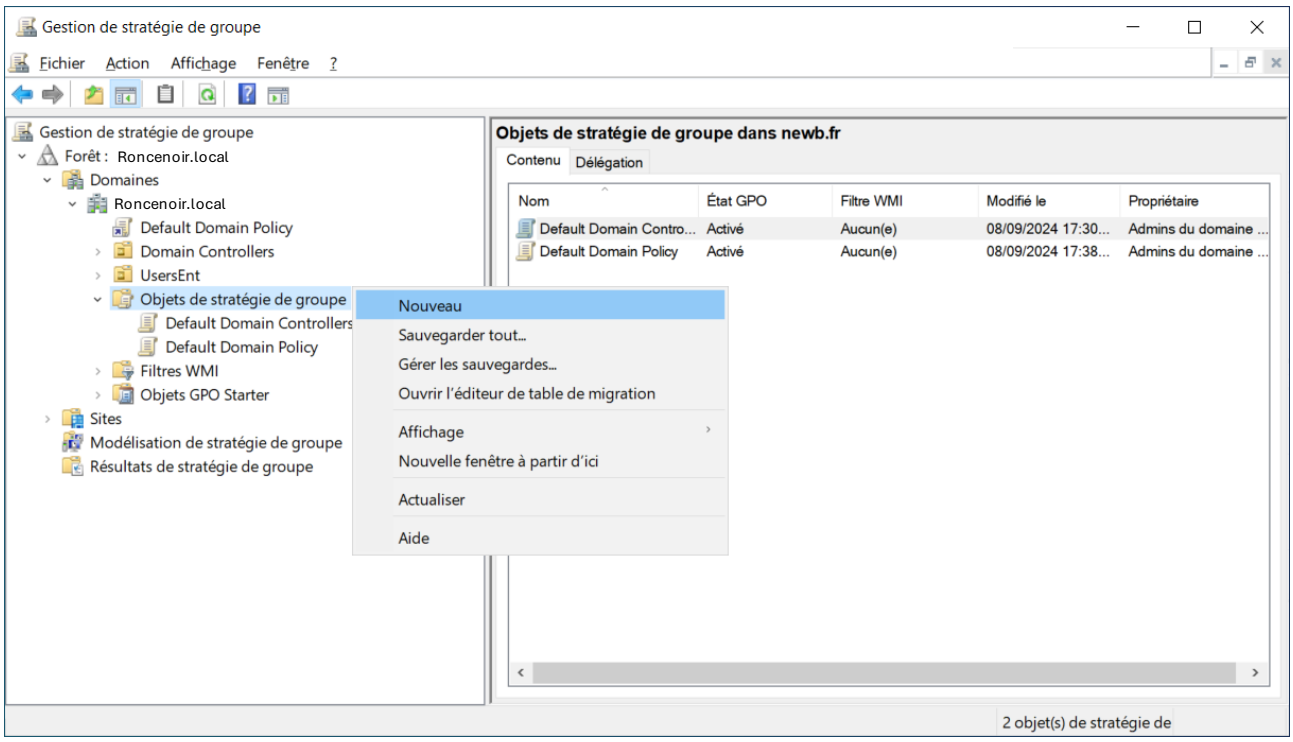
Maintenant, nous allons pouvoir appliquer les paramètres qui nous intéressent.

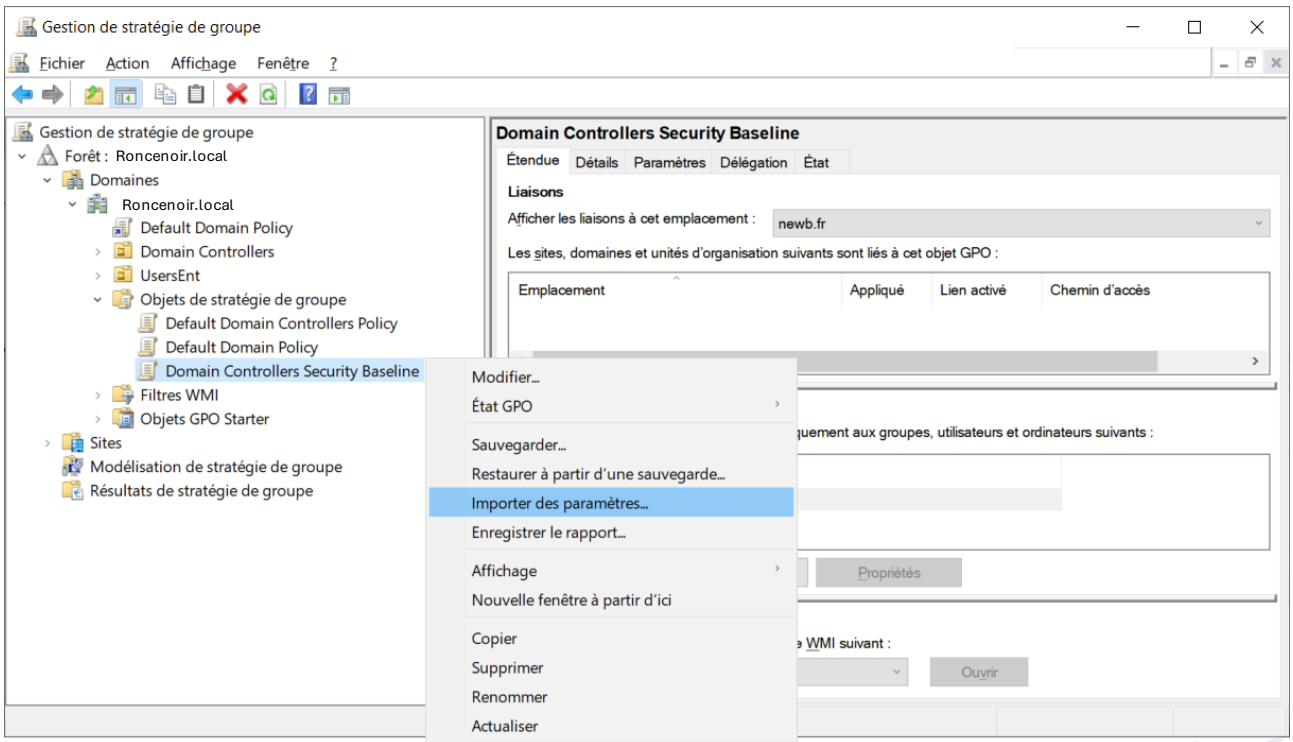
Tout d'abord, faisons une sauvegarde de nos paramètres actuels avant d'en appliquer de nouveaux : LGPO.exe /b peut effectuer cette action.

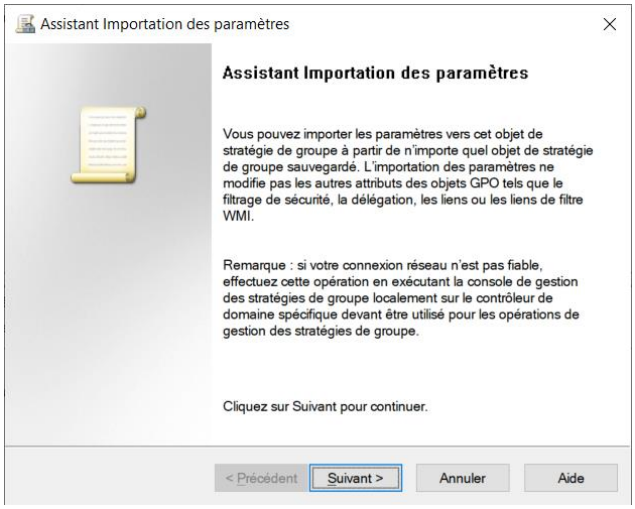
PS C :\ <chemin d'accès au répertoire LGPO.exe> > .\LGPO.exe /b <chemin d'accès à l'enregistrement de la sauvegarde GPO>

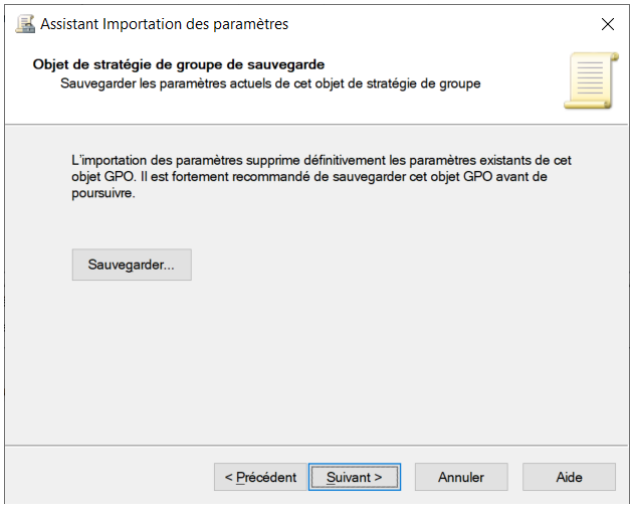


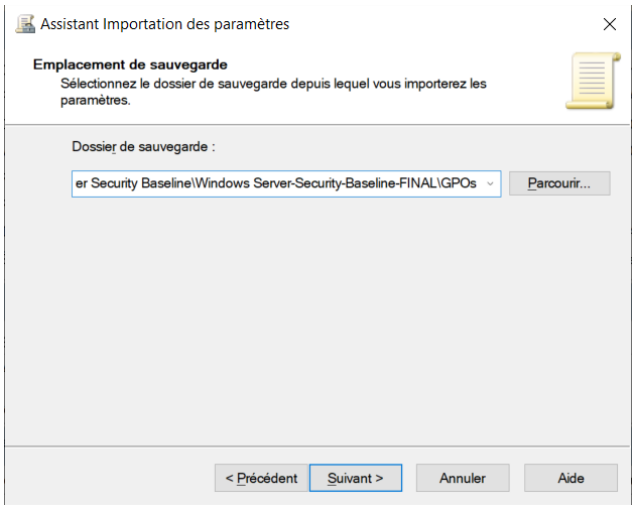
Je me rends sur mon contrôleur de domaine adsecure1 et ouvre l'application « gestion de stratégie de groupe » afin de créer une nouvelle GPO.

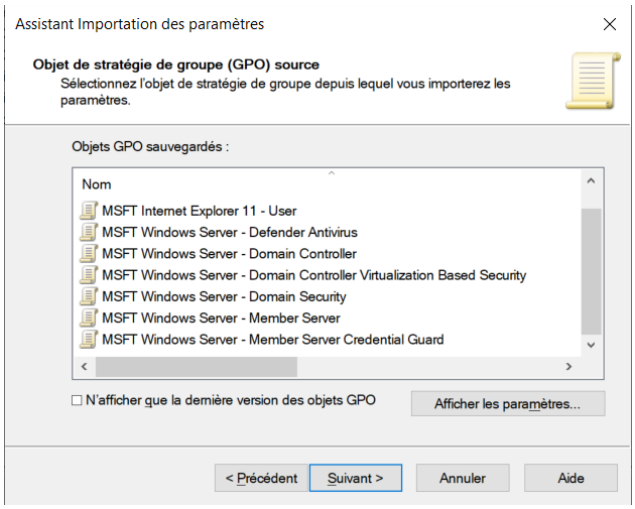

Gestion de stratégie de groupe
Fichier Action Affichage Fenêtre ?
Gestion de stratégie de groupe
Forêt : Roncenoir.local
Domaines
Roncenoir.local
Default Domain Policy
Domain Controllers
UsersEnt
Objets de stratégie de groupe
Default Domain Controllers
Default Domain Policy
Filtres WMI
Objets GPO Starter
Sites
Modélisation de stratégie de groupe
Résultats de stratégie de groupe
Objets de stratégie de groupe dans newb.fr
Contenu Délégation
Nom État GPO Filtre WMI Modifié le Propriétaire
Default Domain Contro... Activé Aucun(e) 08/09/2024 17:30... Admins du domaine ...
Default Domain Policy Activé Aucun(e) 08/09/2024 17:38... Admins du domaine ...
Nouveau
Sauvegarder tout...
Gérer les sauvegardes...
Ouvrir l'éditeur de table de migration
Affichage
Nouvelle fenêtre à partir d'ici
Actualiser
Aide
2 objet(s) de stratégie de

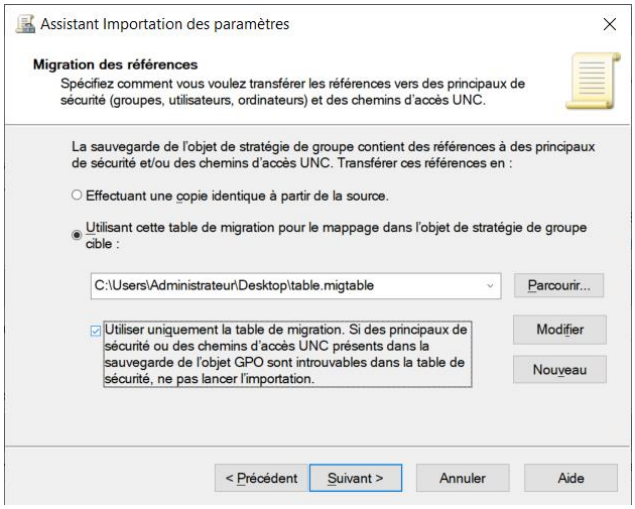

Gestion de stratégie de groupe
Fichier Action Affichage Fenêtre ?
Gestion de stratégie de groupe
Forêt : Roncenoir.local
Domaines
Roncenoir.local
Default Domain Policy
Domain Controllers
UsersEnt
Objets de stratégie de groupe
Default Domain Controllers Policy
Default Domain Policy
Domain Controllers Security Baseline
Filtres WMI
Objets GPO Starter
Sites
Modélisation de stratégie de groupe
Résultats de stratégie de groupe
Domain Controllers Security Baseline
Étendue Détails Paramètres Délégation État
Liaisons
Afficher les liaisons à cet emplacement : newb.fr
Les sites, domaines et unités d'organisation suivants sont liés à cet objet GPO :
Emplacement Appliqué Lien activé Chemin d'accès
Modifier...
État GPO
Sauvegarder...
Restaurer à partir d'une sauvegarde...
Importer des paramètres...
Enregistrer le rapport...
Affichage
Nouvelle fenêtre à partir d'ici
Copier
Supprimer
Renommer
Actualiser
Aide
Propriétés
Ouvrir

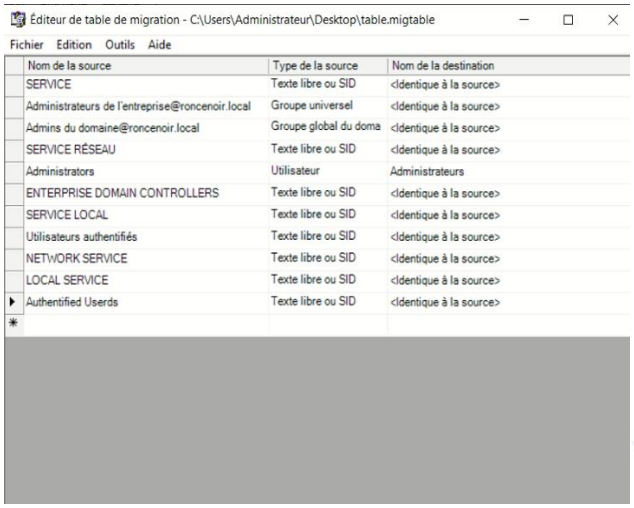

Assistant Importation des paramètres
Assistant Importation des paramètres
Vous pouvez importer les paramètres vers cet objet de stratégie de groupe à partir de n'importe quel objet de stratégie de groupe sauvegardé. L'importation des paramètres ne modifie pas les autres attributs des objets GPO tels que le filtrage de sécurité, la délégation, les liens ou les liens de filtre WMI.
Remarque : si votre connexion réseau n'est pas fiable, effectuez cette opération en exécutant la console de gestion des stratégies de groupe localement sur le contrôleur de domaine spécifique devant être utilisé pour les opérations de gestion des stratégies de groupe.
Cliquez sur Suivant pour continuer.
< Précédent
Suivant >
Annuler
Aide

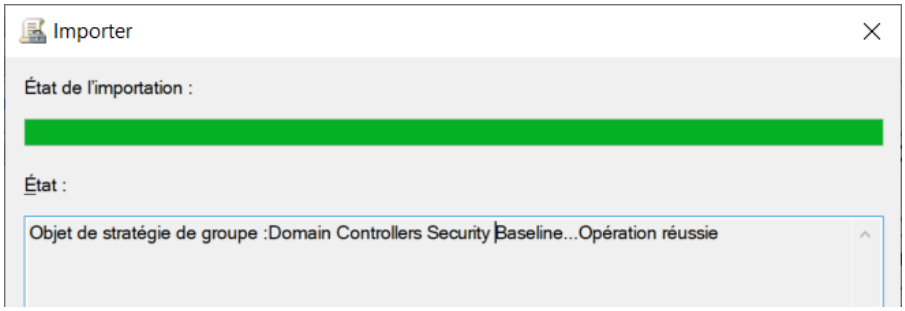

Assistant Importation des paramètres
Objet de stratégie de groupe de sauvegarde
Sauvegarder les paramètres actuels de cet objet de stratégie de groupe
L'importation des paramètres supprime définitivement les paramètres existants de cet objet GPO. Il est fortement recommandé de sauvegarder cet objet GPO avant de poursuivre.
Sauvegarder...
< Précédent
Suivant >
Annuler
Aide


Assistant Importation des paramètres
Emplacement de sauvegarde
Sélectionnez le dossier de sauvegarde depuis lequel vous importerez les paramètres.
Dossier de sauvegarde :
er Security Baseline\Windows Server-Security-Baseline-FINAL\GPOs
Parcourir...
< Précédent
Suivant >
Annuler
Aide


Assistant Importation des paramètres
Objet de stratégie de groupe (GPO) source
Sélectionnez l'objet de stratégie de groupe depuis lequel vous importerez les paramètres.
Objets GPO sauvegardés :
Nom
MSFT Internet Explorer 11 - User
MSFT Windows Server - Defender Antivirus
MSFT Windows Server - Domain Controller
MSFT Windows Server - Domain Controller Virtualization Based Security
MSFT Windows Server - Domain Security
MSFT Windows Server - Member Server
MSFT Windows Server - Member Server Credential Guard
N'afficher que la dernière version des objets GPO
Afficher les paramètres...
< Précédent
Suivant >
Annuler
Aide


Assistant Importation des paramètres
Migration des références
Spécifiez comment vous voulez transférer les références vers des principaux de sécurité (groupes, utilisateurs, ordinateurs) et des chemins d'accès UNC.
La sauvegarde de l'objet de stratégie de groupe contient des références à des principaux de sécurité et/ou des chemins d'accès UNC. Transférer ces références en :
Effectuant une copie identique à partir de la source.
Utilisant cette table de migration pour le mappage dans l'objet de stratégie de groupe cible :
C:\Users\Administrateur\Desktop\table.migtable
Parcourir...
Utiliser uniquement la table de migration. Si des principaux de sécurité ou des chemins d'accès UNC présents dans la sauvegarde de l'objet GPO sont introuvables dans la table de sécurité, ne pas lancer l'importation.
Modifier
Nouveau
< Précédent
Suivant >
Annuler
Aide


Éditeur de table de migration - C:\Users\Administrateur\Desktop\table.migtable
Fichier Edition Outils Aide
Nom de la source
Type de la source
Nom de la destination
SERVICE
Texte libre ou SID
<Identique à la source>
Administrateurs de l'entreprise@roncenoir.local
Groupe universel
<Identique à la source>
Admins du domaine@roncenoir.local
Groupe global du doma
<Identique à la source>
SERVICE RÉSEAU
Texte libre ou SID
<Identique à la source>
Administrators
Utilisateur
Administrateurs
ENTERPRISE DOMAIN CONTROLLERS
Texte libre ou SID
<Identique à la source>
SERVICE LOCAL
Texte libre ou SID
<Identique à la source>
Utilisateurs authentifiés
Texte libre ou SID
<Identique à la source>
NETWORK SERVICE
Texte libre ou SID
<Identique à la source>
LOCAL SERVICE
Texte libre ou SID
<Identique à la source>
Authentified Userds
Texte libre ou SID
<Identique à la source>


Importer
État de l'importation :
État :
Objet de stratégie de groupe :Domain Controllers Security Baseline...Opération réussie

En fonction des stratégies définies, il peut être nécessaire de créer ou de modifier la table de migration. Cette table sert à faire correspondre différents champs entre les environnements, comme par exemple le nom du compte « Administrator » en anglais, qui ne correspond pas à son équivalent français « administrateur ». Sans cette correspondance, des erreurs peuvent survenir lors de l'importation.

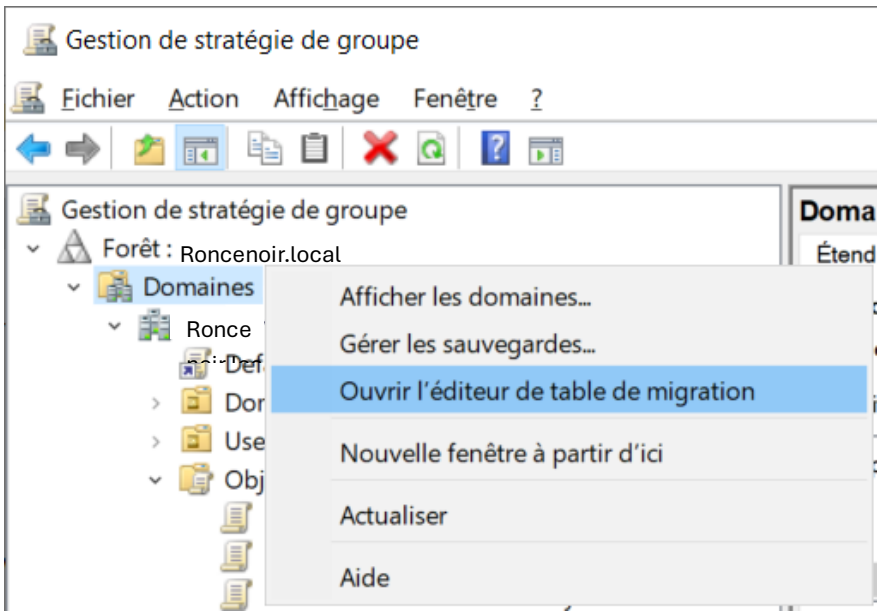
Lorsque les champs ne sont pas connus à l'avance, il est nécessaire d'effectuer une première importation, même si celle-ci génère des erreurs.

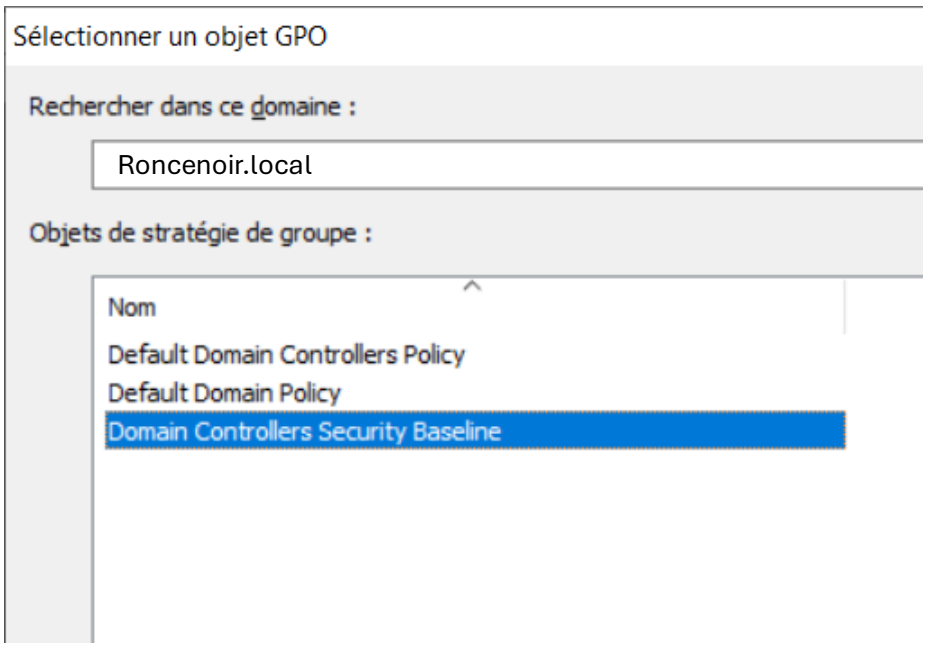
Une fois l'import terminé, faites un clic droit sur le domaine concerné et sélectionnez « Ouvrir l'éditeur de table de migration ».

Dans la fenêtre qui s'ouvre, allez dans le menu « Outils » puis choisissez « Peupler depuis l'objet GPO ».

Sélectionnez la GPO précédemment importée : les champs apparaîtront alors dans leur version localisée (par exemple, en français).

Il faut ensuite relancer la procédure d'importation, cette fois en procédant au mappage correct des champs pour éviter les erreurs.





Éditeur de table de migration - Nouveau

Fichier Edition Outils Aide

Nom de la source	Type de la source	Nom de la destination
SERVICE	Texte libre ou SID	<Identique à la source>
ENTERPRISE DOMAIN CONTROLLERS	Texte libre ou SID	<Identique à la source>
SERVICE RÉSEAU	Texte libre ou SID	<Identique à la source>
Administrateurs	Texte libre ou SID	<Identique à la source>
SERVICE LOCAL	Texte libre ou SID	<Identique à la source>
Utilisateurs authentifiés	Texte libre ou SID	<Identique à la source>