Chapitre 4

Pré-requis

☒Connaître les différents types d'objets utilisateur.

☒Avoir des notions sur les stratégies de groupe.

☒Avoir des notions sur les paramètres de stratégies de groupe permettant la mise en place d'une politique de sécurité.

Objectifs

☒Automatisation de la gestion des comptes.

☒Mise en place d'une politique de sécurité.

☒Gestion d'une stratégie de groupe.

☒Maintenance de stratégie de groupe.

A. Introduction

La gestion des utilisateurs est une tâche quotidienne pour un administrateur système et réseau. Les comptes utilisateurs permettent l'authentification de personnes physiques souhaitant accéder à une ressource du domaine.

B. Automatisation de la gestion des comptes utilisateurs

En plus des consoles Active Directory, il est possible de procéder à la gestion des objets à l'aide d'outils en ligne de commande.

CSVDE (*Comma-Separated Values Data Exchange*) est un outil permettant l'export et l'import d'objets dans un annuaire Active Directory. Des fichiers au format CSV (*Comma-Separated Value*) sont utilisés pour les différentes opérations. Ce type de fichier peut être modifié à l'aide du bloc-notes (notepad) présent dans les systèmes d'exploitation Windows ou avec Microsoft Excel.

Syntaxe de la commande

`csvde -f NomFichier.csv`

Le commutateur `-f` est utilisé afin d'indiquer le fichier à utiliser. La commande permet par défaut d'effectuer une exportation.

Différents commutateurs peuvent être utilisés :

`-d RootDN` : permet de définir le conteneur où débute l'exportation. Par défaut, le conteneur sélectionné est la racine du domaine.

`-p ÉtendueRecherche` : détermine l'étendue de la recherche (Base, OneLevel, Subtree).

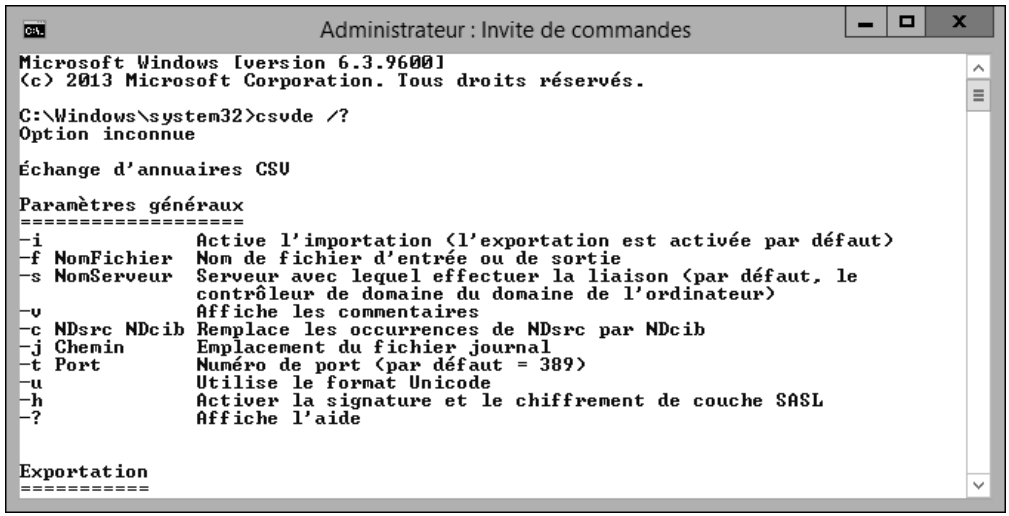
`-r Filtre` : permet la mise en place d'un filtre LDAP.

`-l ListeAttributs` : fournit la liste des attributs sur lesquels il est nécessaire d'effectuer une recherche. Chacun de ces attributs est séparé des autres par une virgule.

☞*Exemples d'attributs : givenName, userPrincipalName,…*

`-i` : informe la commande qu'il est nécessaire d'effectuer une importation. Pour rappel, une exportation est effectuée par défaut.

`-k` : le commutateur `-k` permet d'ignorer les erreurs lors de l'importation. Ainsi, l'exécution de la commande se poursuit même si une erreur de type non-respect de contrainte ou objet existant est rencontrée.



Une deuxième commande peut être utilisée, `ldifde`. Cette instruction DOS permet comme pour `csvde` d'effectuer des opérations d'importation ou d'exportation, de plus il est possible d'effectuer des modifications sur un objet (contrairement à `csvde`).

Pour effectuer ces opérations des fichiers portant l'extension LDIF (*LDAP Data Interchange Format*) sont nécessaires. Ces fichiers contiennent des blocs de lignes qui constituent chacun une opération. Il est évident qu'un fichier peut contenir plusieurs actions, dans ce cas chaque bloc est séparé des autres par une ligne blanche.

Chaque opération nécessite de posséder l'attribut DN (*Distinguished Name*) ainsi que l'opération à effectuer (Add, Modify, Delete).

Syntaxe de la commande

`ldifde -f` *`NomFichier`*`.ldif`

Le commutateur `-f` est utilisé afin d'indiquer le fichier à utiliser. La commande permet par défaut d'effectuer une exportation.

Comme pour la commande `csvde`, plusieurs commutateurs peuvent être utilisés :

`-i` : permet d'effectuer une importation. Par défaut, une exportation est effectuée.

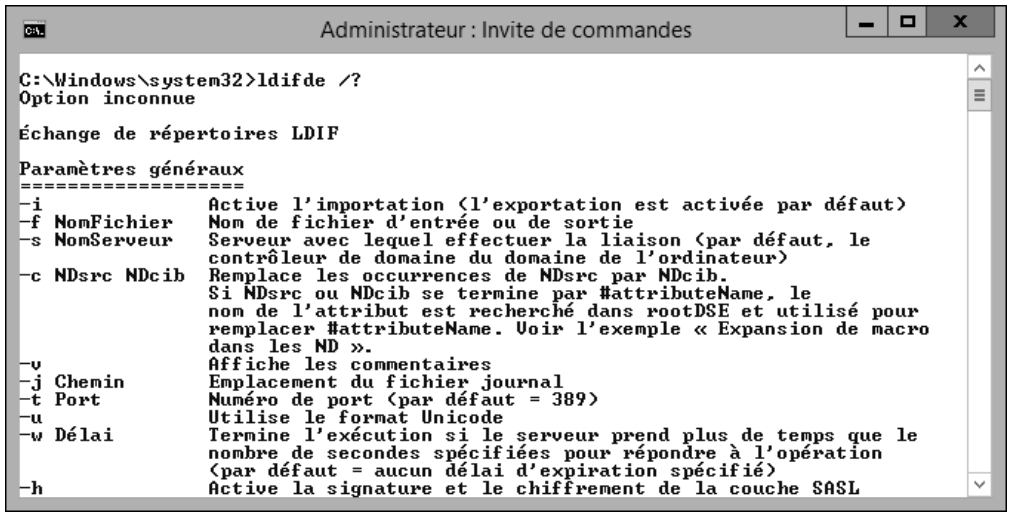
`-k` : le commutateur `-k` permet d'ignorer les erreurs lors de l'importation. Ainsi l'exécution de la commande se poursuit même si une erreur de type non-respect de contrainte ou objet existant est rencontrée.

`-s` *`NomServeur`* : indique le serveur sur lequel il est nécessaire de se connecter.

`-t` *`Port`* : indique le port à utiliser (port par défaut : 389).

`-d` *`NDRacine`* : permet de situer la racine de la recherche.

`-r` *`Filtre`* : permet la mise en place d'un filtre LDAP.



1. Configuration de la politique de sécurité

La politique de sécurité permet de définir un ensemble de paramètres qui s'appliquent à plusieurs objets. On retrouve dans cette politique deux types de paramètres différents :

- Paramètre de sécurité
- Paramètre de verrouillage

Les deux peuvent évidemment être configurés pour une machine spécifique (stratégie de groupe locale) ou l'ensemble des objets d'un domaine AD (généralement configuré dans la Default Domain Policy).

Paramètres de sécurité

Plusieurs types de paramètres peuvent être configurés dans la politique.

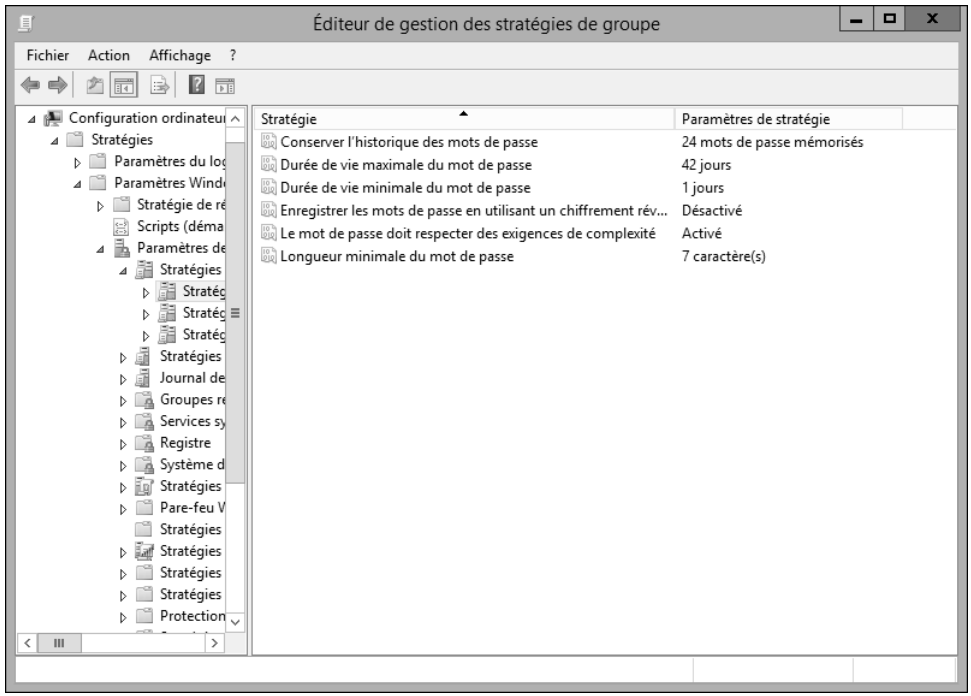
L'âge minimal du mot de passe permet d'indiquer le temps minimum avant qu'un utilisateur puisse de nouveau changer son mot de passe. L'âge maximal indique lui le nombre de jours pendant lequel le mot de passe reste valide. Une fois ce délai passé, l'utilisateur doit changer son mot de passe pour pouvoir ouvrir une session sur le domaine. L'historique de mot de passe est également à prendre en compte, il permet d'interdire les x derniers mots de passe utilisés. Attention à ne pas mettre une trop grosse valeur au niveau de ce paramètre, sans quoi les utilisateurs risquent fortement d'être mécontents.

Lors de la création du domaine Active Directory, la complexité des mots de passe est activée, ce paramètre implique la nécessité de respecter des critères spécifiques dans le mot de passe. En effet, le mot de passe est considéré comme complexe dès lors :

- Qu'il respecte trois des quatre critères suivants :
  - Majuscules
  - Minuscules
  - Caractères alphanumériques
  - Caractères spéciaux
- Qu'il ne contient pas le prénom ou le nom de l'utilisateur.

Cela complique la recherche du mot de passe par un éventuel pirate mais peut (très souvent d'ailleurs) être difficilement accepté par les utilisateurs. Il est préférable de baisser les exigences en termes de sécurité plutôt que de voir les mots de passe marqués en clair sur l'écran ou sous le clavier.

Un autre paramètre important dans une politique de mot de passe est la longueur minimale. En effet, il permet d'indiquer le nombre de caractères que le mot de passe doit contenir.



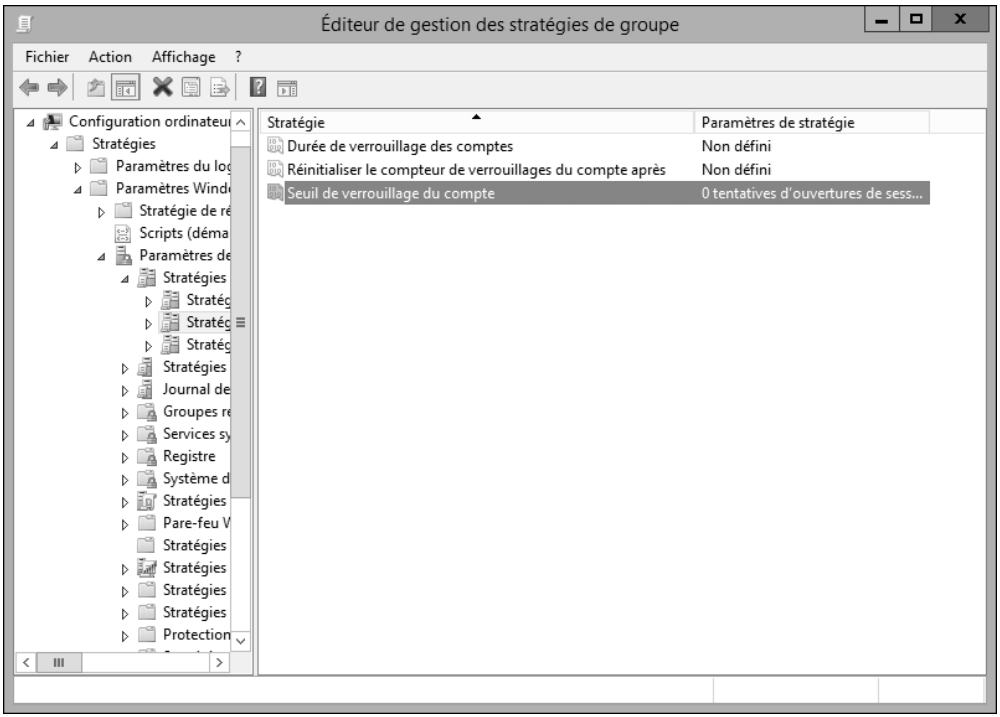
Paramètres de verrouillage

Ces paramètres permettent la configuration du verrouillage.

La durée de verrouillage est celle pendant laquelle le compte utilisateur ne peut ouvrir de session. Pour un déverrouillage manuel effectué par l'administrateur, il est nécessaire de configurer le paramètre à 0.

Le nombre de tentatives infructueuses limite le nombre d'essais en échec. Ainsi le compte concerné est verrouillé une fois ce nombre de tentatives atteint. La valeur 0 implique des tentatives infructueuses illimitées car le compte n'est alors jamais verrouillé.

Il est nécessaire de remettre à zéro le compteur du nombre de tentatives infructueuses sans quoi la politique de verrouillage n'a plus de sens. Ainsi un autre paramètre entre en compte dans la politique de verrouillage, il s'agit cette fois de la mise à jour du compteur (du nombre de tentatives en échec) après un certain nombre de minutes.



Enfin, un troisième type de paramètres (politique Kerberos) peut être également configuré. Il est donc possible d'avoir accès à des paramètres du protocole Kerberos v5.

La configuration peut, comme nous l'avons vu plus haut dans ce chapitre, être paramétrée depuis une stratégie locale ou une stratégie du domaine (console **Éditeur de gestion des stratégies de groupe**). Attention néanmoins, en cas de conflit entre une stratégie de groupe locale et une stratégie du domaine, celle du domaine l'emporte.

Les paramètres de sécurité sont généralement configurés dans la stratégie de groupe Default Domain Policy.