



Configuration d'une stratégie de mot de passe affinée

Configuration d'une stratégie de mot de passe affinée

Procédure configuration d'une stratégie de mot de passe affinée	1
Présentation	1
La notion de stratégie de mot de passe affinée	1
Création de la Stratégie de mot de passe affinée	2
Descriptions des différents champs	3
Assignation a des Utilisateurs / Groupes	4
Conclusion	5

Présentation

Avec cette procédure, nous allons mettre en place une stratégie de mot de passe via l'Active Directory. Celle-ci permet une gestion plus sécurisée et plus stricte des mots de passe pour les utilisateurs.

Historiquement, la gestion des politiques de mots de passe était gérée via les **GPO** (Group Policy Object), avec des paramètres présents par défaut :

Computer Configuration	Enforce password history	Not Defined
Policies	Maximum password age	Not Defined
Software Settings	Minimum password age	Not Defined
Windows Settings	Minimum password length	Not Defined
Name Resolution Policy	Minimum password length audit	Not Defined
Scripts (Startup/Shutdown)	Password must meet complexity requirements	Not Defined
Deployed Printers	Relax minimum password length limits	Not Defined
Security Settings	Store passwords using reversible encryption	Not Defined
Account Policies		
Password Policy		
Account Lockout Policy		
Kerberos Policy		

La notion de stratégie de mot de passe affinée

Depuis la version de Windows server 2008, il est possible de créer des « **Stratégie de mot de passe affinée** » depuis l'Active Directory.

Les stratégies de mot de passe affinées correspondent à des objets « Paramètres de mot de passe » et sont également appelées « **PSO** » pour « **Password Settings Object** »

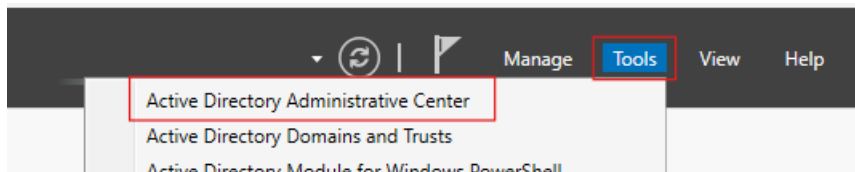
L'avantage de cette solution, est que l'on peut créer plusieurs politiques au sein d'un même domaine, avec des priorités différentes, et les attribuer seulement à certains utilisateurs ou groupes.



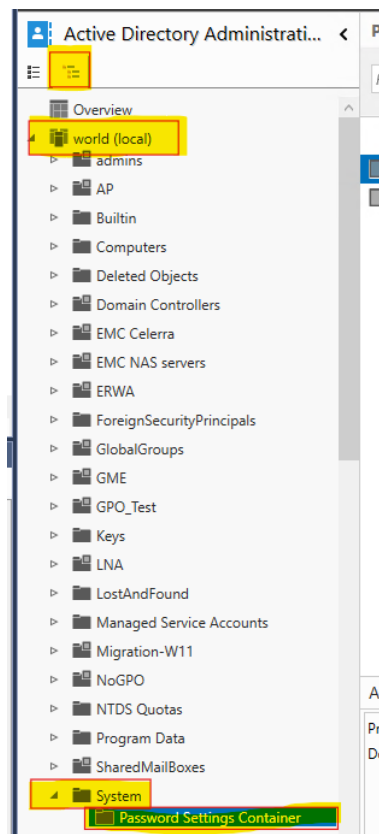
Un utilisateur / groupe peut donc être assigné à plusieurs PSO, mais en cas de conflits, l'attribut de priorité nommé « **Valeur de précedence** »

Création de la Stratégie de mot de passe affinée

Sur le contrôleur de domaine, ouvrir la console « **Centre d'administration Active Directory** » (accessible directement via les outils du **Server Manager**)

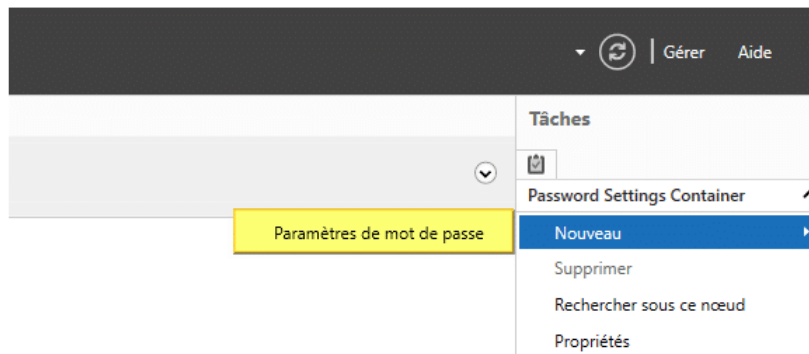


Accéder ensuite, via l'arborescence à gauche, au **Password Settings Container**



Nous nous situons donc maintenant à l'endroit où seront stockées nos stratégies.

Nous allons maintenant créer notre nouvelle stratégie en appuyant sur nouveau dans le bandeau à droite, puis lui donner un nom parlant (ex : PSO – Users).



Nous voici maintenant devant tous les différents paramètres de notre future stratégie. Quelques champs sont déjà pré remplis avec des valeurs par défaut.

Nous n'allons pas conserver ses valeurs, car nous voulons une stratégie personnalisée pour notre utilisation.

Descriptions des différents champs

-Priorité : Nombre qui définit la priorité de la PSO (la valeur la plus faible sera toujours prioritaire, penser à espacer ce nombre sur chacune de vos PSO pour pouvoir jouer par la suite sur les priorités)

-Longueur minimale du mot de passe : Cette case peut être cochée et définit le nombre de caractères minimum des mots de passe lors de leur création

-Historique des mots de passe : Si cette case est cochée, le nombre renseigné correspond au nombre de mot de passe de chaque utilisateur conservé en mémoire. Lors du changement de mot de passe de l'utilisateur, le nouveau devra donc être différents de ses x derniers mots de passe.

-Respect des exigences de complexité : Définit si les mots de passe devront respecter les paramètres de complexité (recommandé pour une meilleure sécurité)

-Stockage du mot de passe avec chiffrement réversible : Définit si les mots de passe seront stockés ou non, de manière chiffrée

-Age minimal de mot de passe : Définit en nombre de jours, la durée de vie minimale d'un mot de passe, ce qui permet d'empêcher un utilisateur de changer successivement plusieurs fois son mot de passe. Cela pourrait lui permettre de dépasser la limite d'historique de mot de passe pour redéfinir son mot de passe initial

-Age maximal de mot de passe : Définit en nombre de jours, la durée de vie maximale d'un mot de passe. Durée après laquelle il est expiré et doit être modifié.

-Stratégie de verrouillage des comptes : Définit le nombre de tentative échouée avant le verrouillage du compte. Le second nombre correspond en minutes, au temps après lequel, le nombre de tentative échouée est réinitialisé. Le dernier paramètre est un choix à faire si la case est cochée.



-Protection contre la suppression accidentelle : Permet de protéger votre PSO contre la suppression accidentelle (il est recommandé de cocher cette case).

Après avoir remplis les champs nécessaires, notre politique devrait ressembler à quelque chose comme ça :

Créer Paramètres de mot de passe : PSO_Comptabilite

Paramètres de mot de passe

S'applique directement à

Options d'âge du mot de passe :

Nom : * PSO_Comptabilite

Priorité : * 10

☒ Appliquer la longueur minimale du mot de passe

Longueur minimale du mot de passe (caractères) : * 7

☒ Appliquer l'historique des mots de passe

Nombre de mots de passe mémorisés : * 24

☒ Le mot de passe doit respecter des exigences de complexité

☐ Stocker le mot de passe en utilisant un chiffrement réversible

☒ Protéger contre la suppression accidentelle

Description :

☒ Appliquer l'âge minimal de mot de passe

L'utilisateur ne peut pas changer le mot de passe d'i... * 2

☐ Appliquer l'âge maximal de mot de passe

L'utilisateur doit changer le mot de passe après (jour...) * 42

☒ Appliquer la stratégie de verrouillage des comptes :

Nombre de tentatives de connexion échouées autorisé : * 3

Réinitialiser le nombre de tentatives de connexion écho... * 60

Le compte va être verrouillé

☐ Pendant une durée de (mins) : * 30

☒ Jusqu'à ce qu'un administrateur déverrouille manuellement le compte

Assignation a des Utilisateurs / Groupes

Maintenant, il faut assigner cette stratégie à nos utilisateurs ou groupes.

Premièrement, nous allons vérifier si une stratégie est déjà assignée à un utilisateur, en passant par l'éditeurs d'attributs depuis la console « **Utilisateurs et ordinateurs Active Directory** »

Tout d'abord aller dans « **Affichage** » puis « **Fonctionnalités avancées** », sans quoi vous n'aurez pas la possibilité de voir l'éditeur d'attributs.

Ensuite, clique droit sur un utilisateur, « **propriétés** » puis « **Editeurs d'attributs** ».

Il faut maintenant filtrer : « **Filtre** » puis cliquer sur « **Construit** ».

Enfin, l'attribut que nous recherchons se nomme : **msDS-ResultantPSO**

Si cet attribut possède une valeur, alors une PSO est déjà affectée à cet utilisateur.

Sinon, nous allons pouvoir procéder à l'affectation de la PSO que nous venons de créer.

Depuis notre PSO, dans l'espace « **S'applique directement à** », cliquer sur « **Ajouter** »

Puis renseigner le(s) groupe(s) ou les utilisateurs souhaités.

S'applique directement à

Nom

Courrier

Comptabilité

Ajouter...

Supprimer

Informations supplémentaires...

OK

Annuler



Nous avons maintenant les assignations de renseignées dans ce champ :

Vérifier maintenant que notre stratégie est bien assignée à l'utilisateur souhaité, avec la méthode vue juste ci-dessus.

The screenshot shows the 'Attribute Editor' tab in the Active Directory user properties dialog. The list of attributes includes 'msDS-ResultantPSO', which is highlighted. The value for this attribute is 'CN=PSO_Comptabilite,CN=Password Settings Container,CN=System,DC=...'. A modal dialog box titled 'Éditeur d'attributs de type Chaîne' is open, showing the same attribute and value, with buttons for 'Effacer', 'OK', and 'Annuler'.

Ici, nous voyons bien que notre stratégie est assignée à notre utilisateur.

Conclusion

L'objectif des PSO est d'éviter la règle unique pour toute l'entreprise. Cette méthode permet d'adapter la sécurité en fonction de l'importance du compte.

Par exemple, un compte utilisateur et un compte admin n'auront pas les même PSO, car les comptes administrateur sont des comptes plus critiques, et donc ont besoin d'une encore plus grande sécurité, là où pour un compte utilisateurs, nous voulons aussi faciliter le quotidien de nos collaborateurs (tout en restant sécurisé bien sûr)

En résumé, les PSO permettent de **renforcer la sécurité là où c'est nécessaire**, sans bloquer le travail des équipes.