



Didacticiel : Stratégies de mot de passe affinées

Département Mathématiques & Informatique

Table des matières

Introduction.....	2
Pré requis à la création de Stratégie de mot de passe affinée.....	2
Fonctionnement technique.....	2
Classe Password Settings Container (PSC) : msDS-PasswordSettingsContainer	5
Classe Password Settings Object : msDS-PasswordSettings.....	7
Le tableau ci-dessous énumère les différentes valeurs d’attribut à renseigner tout au long de la création de l’objet PSO :	8
Procédure d’installation d’une stratégie de mot de passe affinée.....	9
1. Création d’un objet PSO.....	10
2. Application des objets PSO aux utilisateurs et aux groupes de sécurité globaux	24
Création de la stratégie de mot de passe affinée en utilisant l’outil : Centre d’administration Active Directory.....	33
Vérifier l’application de la stratégie de mot de passe affinée	39
Références :	43

Introduction

Dans les versions antérieures à Windows 2008, la stratégie de mot de passe et de verrouillage de compte était unique au sein d'un même domaine (stratégie de domaine par défaut) et mise à part en utilisant des produits tiers payants (Specops Password Policy) ou un filtre de mot de passe, il était impossible de définir des stratégies différentes en fonction des besoins de l'entreprise. Cela pouvait se révéler problématique si vous vouliez par exemple complexifier le mot de passe pour certaines catégories d'utilisateur de votre domaine.

Par exemple, en admettant que la politique de mot de passe soit peu sécurisée sur votre domaine (pas de complexité et une longueur de 6 caractères), cela donnait la possibilité à des personnes avec des privilèges élevés de définir un mot de passe simple et donc facile à cracker, laissant ainsi une faille de sécurité importante sur votre Active Directory.

Avec Windows 2008, il est maintenant possible de définir plusieurs stratégies de mot de passe et de verrouillage de compte sous le nom de « stratégie de mot de passe affinée ». La stratégie de base s'applique comme auparavant au niveau du domaine, cependant quelques manipulations permettent d'affecter différentes stratégies appliquées à des objets utilisateurs ou groupes globaux Active Directory.

Vous pouvez donc appliquer par exemple des stratégies de mot de passe et de verrouillage de compte différentes suivant le type de compte. Par exemple, une stratégie classique pour les utilisateurs « normaux », une stratégie plus sécurisée pour les administrateurs et enfin une autre pour les comptes de service.

Un scénario typique inclurait 3 à 4 stratégies de ce type (attention, ça n'est pas Le scénario best practices, juste un exemple) :

- Une stratégie de mots de passe pour les administrateurs (ex : 16 caractères, expiration tous les 20 jours)
- Une stratégie pour les utilisateurs simples (ex : 8 caractères, expiration tous les 120 jours)
- Une stratégie pour les utilisateurs sensibles (ex : 16 caractères, expiration tous les 30 jours)
- -éventuellement- Une stratégie pour les comptes de service (ex : 32 caractères, pas d'expiration)

Pré requis à la création de Stratégie de mot de passe affinée

- ✓ Mode fonctionnel du domaine en Windows 2008 ou plus (2012, 2016 ou 2019)
- ✓ Etre administrateur du domaine si aucune délégation spécifique n'a été mise en place

Fonctionnement technique

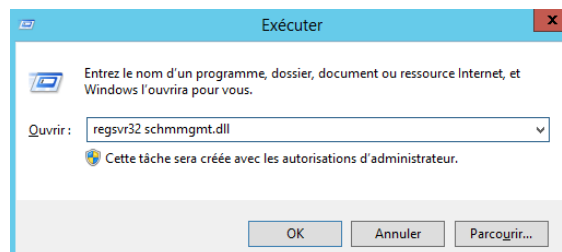
Cette nouvelle fonctionnalité s'appuie sur 2 nouvelles classes d'objet et quelques attributs liés à

une de ces 2 classes du schéma Active Directory : Password Settings Container (PSC) et Password settings Object (PSO).

La console de gestion du schéma n'est plus disponible par défaut. A fin de l'activer, cette manipulation à faire en tant qu'administrateur du schéma AD.

Voici la démarche à suivre pour activer le composant logiciel enfichable "console de schéma Active Directory" afin de l'insérer dans votre MMC.

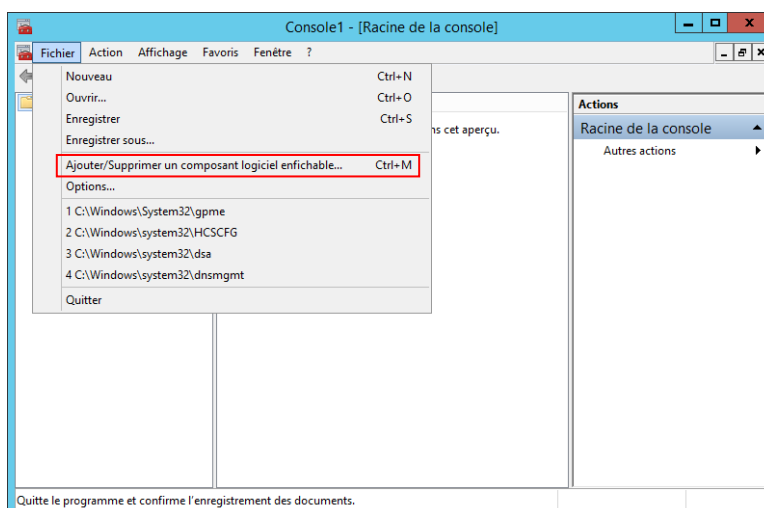
Dirigez-vous sur "**Démarrer**" puis "**Exécuter**" et tapez "**regsvr32 schmmgmt.dll**".



Un message indiquera que l'enregistrement de la DLL est un succès. Validez.



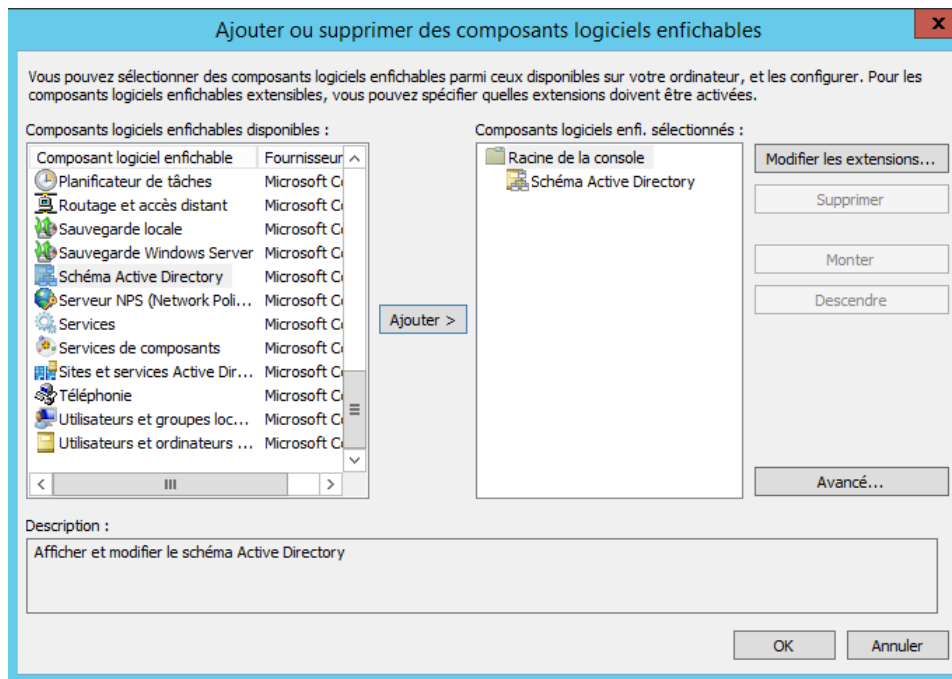
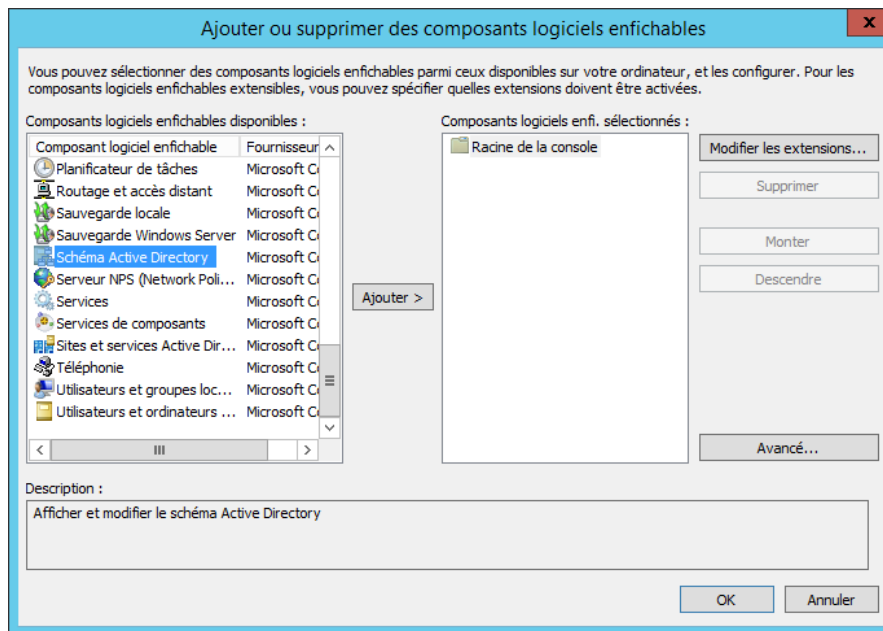
Lancez la Console MMC (Microsoft Management Console) en tapant "**mmc**" dans "**Exécuter**". Une fois la console lancée, allez dans "**Fichier**" puis "**Ajouter/supprimer un composant logiciel enfichable**" (Ctrl+M).



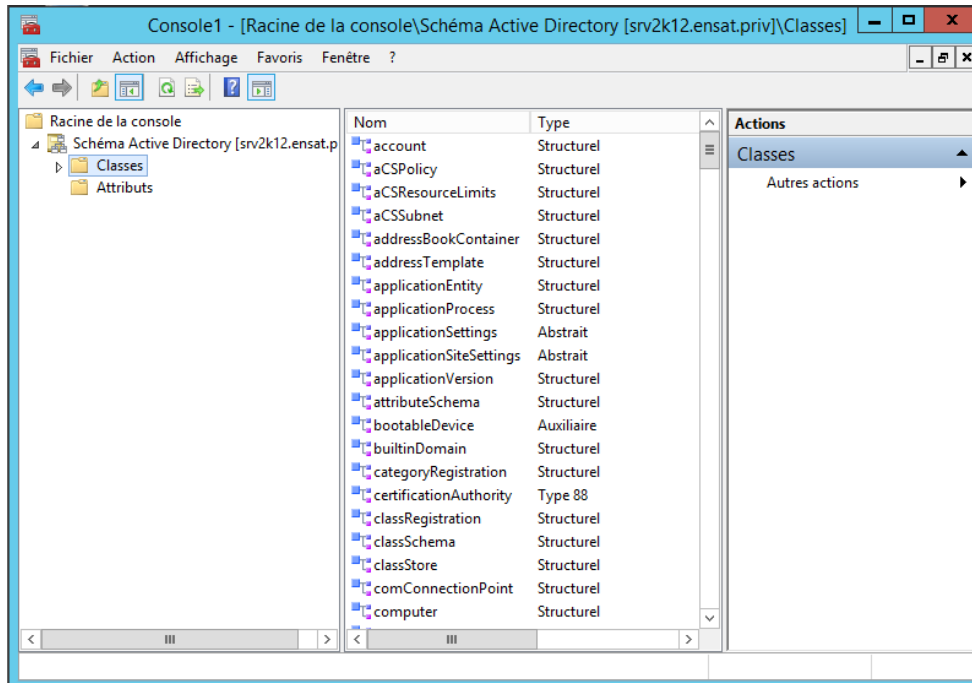
Dans la fenêtre qui s'ouvre, cliquez sur le bouton "**Ajouter**" en bas à gauche afin d'ouvrir une fenêtre de sélection avec la liste des composants. Cherchez puis sélectionnez "Schéma Active Directory" pour finir en cliquant sur les boutons "**Ajouter**" puis "**Fermer**". Cliquez sur "**OK**"

dans la fenêtre restante pour voir votre composant apparaître.

N'oubliez pas d'enregistrer votre console en quittant pour ne pas recommencer!

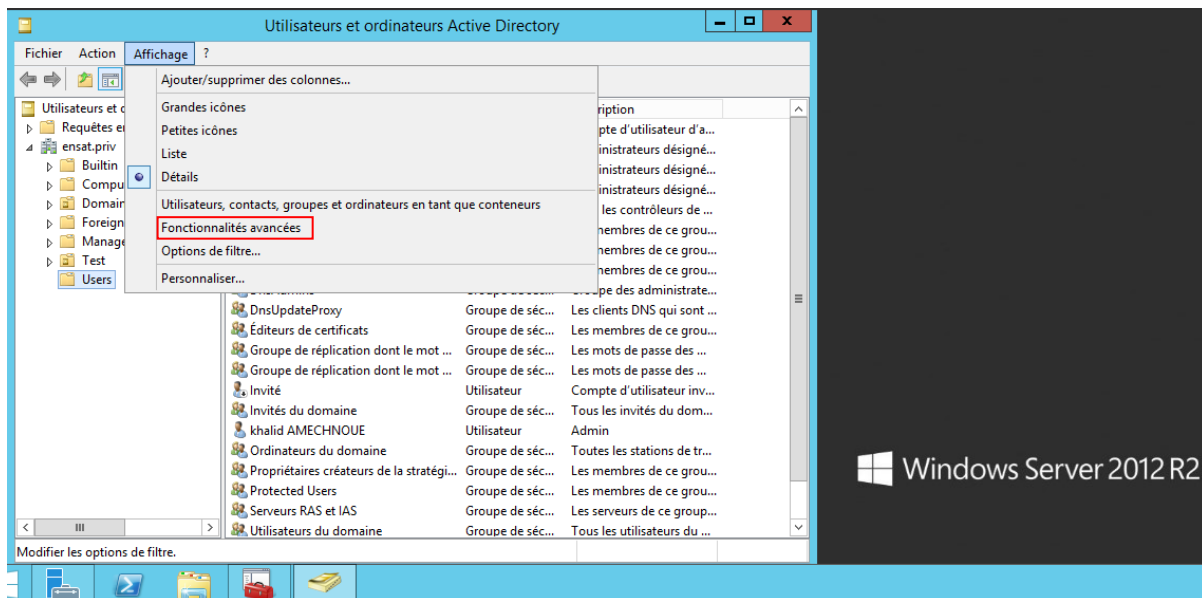


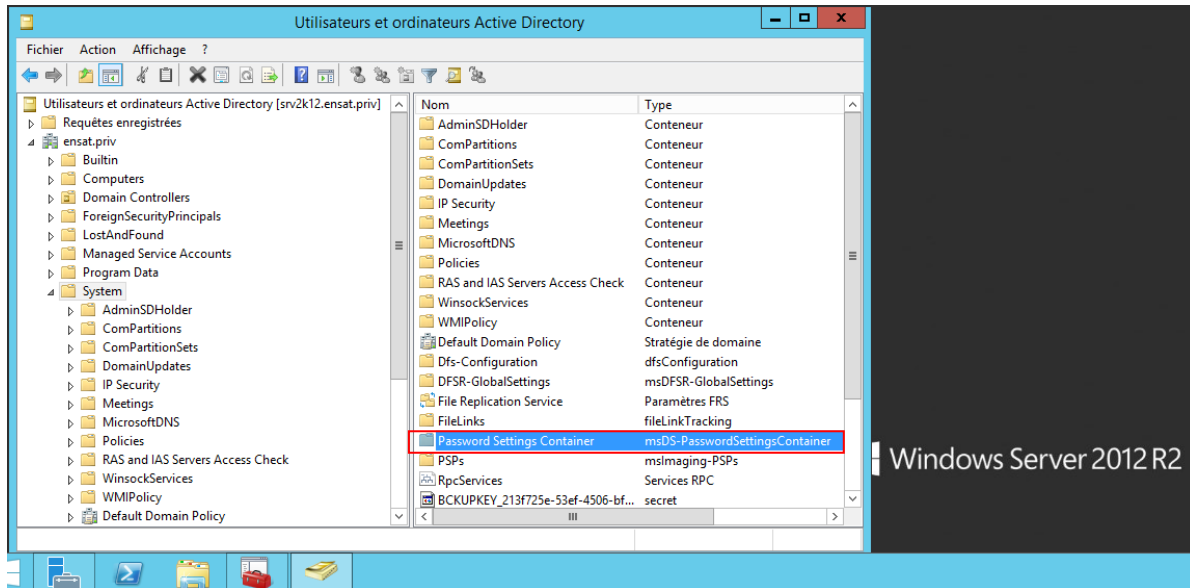
L'apparence de la console est comme suit :



Classe Password Settings Container (PSC) : msDS-PasswordSettingsContainer

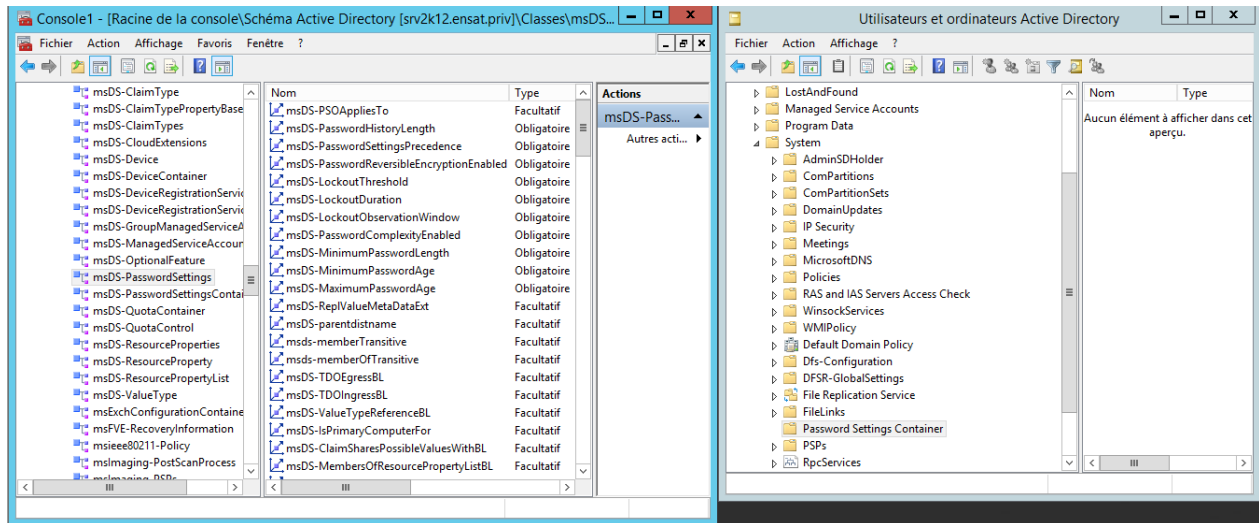
La classe Password Settings Container (PSC) est visible directement dans la console « Utilisateurs et ordinateurs Active Directory » en activant les fonctionnalités avancées :





Windows Server 2012 R2

Ce conteneur par défaut vide contiendra tous les paramètres de mot de passe (Password Settings Object – PSO) créés suivant les besoins :



Classe Password Settings Object : msDS-PasswordSettings

Nom	Type	Système	Description
msDS-PSOAppliesTo	Facultatif	Oui	Links to objects that this password settings object applies to
msDS-PasswordHistoryLength	Obligatoire	Oui	Password History Length for user accounts
msDS-PasswordSettingsPrecedence	Obligatoire	Oui	Password Settings Precedence
msDS-PasswordReversibleEncryptionEnabled	Obligatoire	Oui	Password reversible encryption status for user accounts
msDS-LockoutThreshold	Obligatoire	Oui	Lockout threshold for lockout of user accounts
msDS-LockoutDuration	Obligatoire	Oui	Lockout duration for locked out user accounts
msDS-LockoutObservationWindow	Obligatoire	Oui	Observation Window for lockout of user accounts
msDS-PasswordComplexityEnabled	Obligatoire	Oui	Password complexity status for user accounts
msDS-MinimumPasswordLength	Obligatoire	Oui	Minimum Password Length for user accounts
msDS-MinimumPasswordAge	Obligatoire	Oui	Minimum Password Age for user accounts
msDS-MaximumPasswordAge	Obligatoire	Oui	Maximum Password Age for user accounts
msDS-EnabledFeatureBL	Facultatif	Oui	Scopes where this optional feature is enabled.
msDS-LastKnownRDN	Facultatif	Oui	Holds original RDN of a deleted object.
msDS-HostServiceAccountBL	Facultatif	Oui	Service Accounts Back Link for linking machines associated with the service account.
msDS-OIDToGroupLinkBL	Facultatif	Oui	Backlink for ms-DS-OIDToGroup-Link; identifies the issuance policy, represented by an OID object, which is max
msDS-LocalEffectiveRecycleTime	Facultatif	Oui	Recycle time of the object in the local DIT.
msDS-LocalEffectiveDeletionTime	Facultatif	Oui	Deletion time of the object in the local DIT.
msDS-PSOApplied	Facultatif	Oui	Password settings object applied to this object
msDS-NCType	Facultatif	Oui	A bit field that maintains information about aspects of a NC replica that are relevant to replication.
msDS-PrincipalName	Facultatif	Oui	Account name for the security principal (constructed)
msDS-RevealedListBL	Facultatif	Oui	backlink attribute for ms-DS-Revealed-List.
msDS-NC-RO-Replica-Locations-BL	Facultatif	Oui	backlink attribute for ms-DS-NC-RO-Replica-Locations.
msDS-Key-Recovery-Agent	Facultatif	Oui	Backlink for ms-DS-AuthenticatedAt-DC; for a Computer, identifies which users have authenticated to this Com
msDS-AuthenticatedToAccountList	Facultatif	Oui	Backlink for has-Partial-Replica-NCs; for a partition root object, identifies which Directory instances (DSA) hold
msDS-IsPartialReplicaFor	Facultatif	Oui	Backlink for ms-DS-Has-Domain-NCs; for a partition root object, identifies which Directory instances (DSA) hold
msDS-IsDomainFor	Facultatif	Oui	Backlink for ms-DS-Has-Full-Replica-NCs; for a partition root object, identifies which Directory instances (DSA) hold
msDS-IsFullReplicaFor	Facultatif	Oui	Backlink for ms-DS-Has-Full-Replica-NCs; for a partition root object, identifies which Directory instances (DSA) hold
msDS-RevealedDSAs	Facultatif	Oui	Backlink for ms-DS-Revealed-Users; for a user, identifies which Directory instances (DSA) hold that user's secre

Cette classe s'appuie sur des attributs existants déjà utilisés dans la stratégie de domaine par défaut.

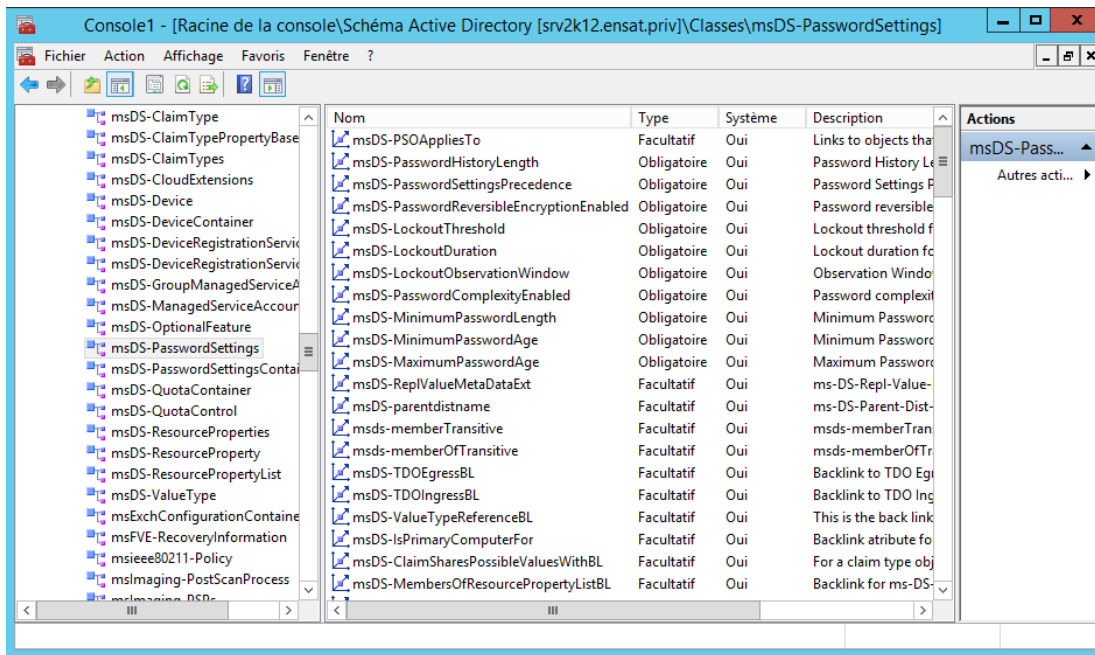
- msDS-PasswordHistoryLength : Appliquer l'historique des mots de passe
- msDS-MaximumPasswordAge : Durée de vie maximale du mot de passe
- msDS-MinimumPasswordAge : Durée de vie minimale du mot de passe
- msDS-MinimumPasswordLength : Longueur minimale du mot de passe
- msDS-PasswordComplexityEnabled : Le mot de passe doit respecter des exigences de complexité
- msDS-PasswordReversibleEncryptionEnabled : Enregistrer les mots de passe en utilisant un chiffrement réversible
- msDS-LockoutDuration : Durée de verrouillage de compte
- msDS-LockoutThreshold : Seuil de verrouillage de compte
- msDS-LockoutObservationWindow : Réinitialiser le compteur de verrouillage de compte après

2 nouveaux attributs viennent compléter cette liste :

msDS-PSOAppliesTo : attribut multi valeur lié aux objets Utilisateur et/ou Groupe. C'est un lien de redirection vers des objets Utilisateur ou groupe uniquement.

msDS-PasswordSettingsPrecedence : attribut permettant de gérer la priorité en cas de conflit si plusieurs Password Settings Object sont appliquées sur un même objet. Il s'agit d'un entier utilisé pour résoudre les conflits si plusieurs objets PSO sont appliqués à un objet utilisateur ou groupe.

Hormis l'attribut **msDS-PSOAppliesTo**, les 10 autres attributs sont **des attributs obligatoires** de type « MustHave » c'est-à-dire qu'une valeur doit être absolument définie pour chacun d'entre eux.



Le tableau ci-dessous énumère les différentes valeurs d'attribut à renseigner tout au long de la création de l'objet PSO :

Nom d'attribut	Description	Plage des valeurs acceptables	Exemple de valeur
msDS-PasswordSettingsPrecedence	Précédence des paramètres de mot de passe	Supérieur à 0	10
msDS-PasswordReversibleEncryptionEnabled	État de chiffrement réversible de mot de passe pour les comptes d'utilisateurs	FALSE / TRUE (Valeur recommandée : FALSE)	FALSE
msDS-PasswordHistoryLength	Longueur de l'historique du mot de passe pour les comptes d'utilisateurs	de 0 à 1 024	24
msDS-PasswordComplexityEnabled	État de complexité du mot de passe pour les comptes d'utilisateurs	FALSE / TRUE (Valeur recommandée : TRUE)	TRUE
msDS-MinimumPasswordLength	Longueur minimale du mot de passe pour les comptes d'utilisateurs	De 0 à 255	8
msDS-MinimumPasswordAge	Durée de vie minimale du mot de passe pour les comptes d'utilisateurs	<ul style="list-style-type: none"> (Aucune) De 00:00:00:00 à la valeur msDS-MaximumPasswordAge 	1:00:00:00 (1 jour)

msDS-MaximumPasswordAge	Durée de vie maximale du mot de passe pour les comptes d'utilisateurs	<ul style="list-style-type: none"> • (Jamais) • De la valeur msDS-MinimumPasswordAge à (Jamais) • La valeur de msDS-MaximumPasswordAge ne peut pas être définie à zéro 	42:00:00:00 (42 jours)
msDS-LockoutThreshold	Seuil de verrouillage pour le verrouillage des comptes d'utilisateurs	De 0 à 65 535	10
msDS-LockoutObservationWindow	Fenêtre d'observation pour le verrouillage des comptes d'utilisateurs	<ul style="list-style-type: none"> • (Aucune) • De 00:00:00:01 à la valeur msDS-LockoutDuration 	0:00:30:00 (30 minutes)
msDS-LockoutDuration	Durée de verrouillage pour les comptes d'utilisateurs verrouillés	<ul style="list-style-type: none"> • (Aucune) • (Jamais) • De la valeur msDS-LockoutObservationWindow à (Jamais) 	0:00:30:00 (30 minutes)
msDS-PSOAppliesTo	Liens jusqu'aux objets auxquels cet objet PSO s'applique (lien avant)	0 ou plusieurs noms uniques d'utilisateurs ou de groupes de sécurité globaux	"CN=u1,CN=Users,DC=DC1,DC=contoso,DC=com"

Procédure d'installation d'une stratégie de mot de passe affinée

Deux méthodes sont disponibles pour implémenter une stratégie de mot de passe affinée :

- L'utilitaire en ligne de commande LDIFDE
- L'éditeur ADSI

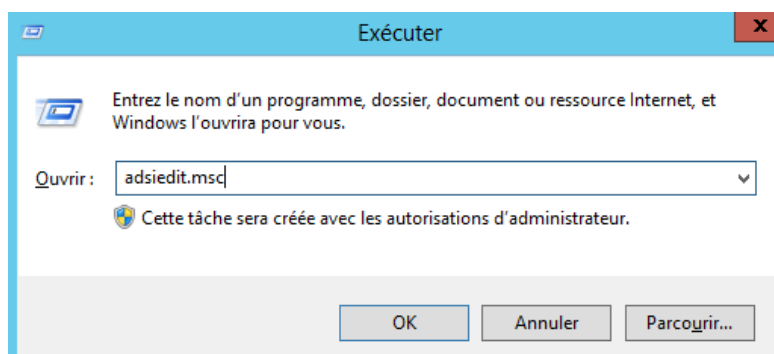
Dans la procédure ci-dessous, nous utiliserons AdsiEdit (Active Directory Service Interfaces, abrégé en ADSI, est une bibliothèque logicielle fournissant une interface de programmation de Microsoft basée sur le modèle COM et permettant aux programmeurs de lire et manipuler le contenu d'un Active Directory).

L'Éditeur ADSI (Active Directory® Service Interfaces) est un éditeur LDAP (Lightweight Directory Access Protocol) que vous pouvez utiliser pour gérer les objets et les attributs des services de domaine Active Directory (AD DS). L'Éditeur ADSI (adsiedit.msc) offre une vue de tous les objets et attributs figurant dans une forêt Active Directory. Vous pouvez l'utiliser pour interroger, afficher et modifier les attributs qui ne sont pas accessibles par le biais d'autres composants logiciels enfichables MMC (Microsoft Management Console) pour AD DS : Utilisateurs et ordinateurs Active Directory, Sites et services Active Directory, Domaines et approbations Active Directory et Schéma Active Directory. Dans le système d'exploitation Windows Server® 2008, vous pouvez utiliser l'Éditeur ADSI pour administrer des stratégies de verrouillage de compte et de mot de passe affinées.

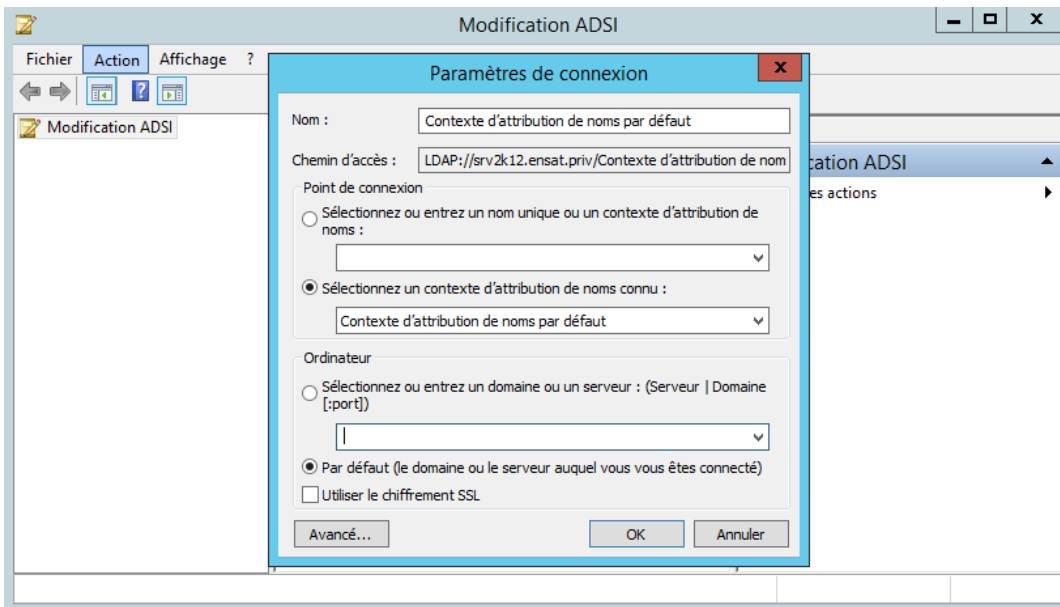
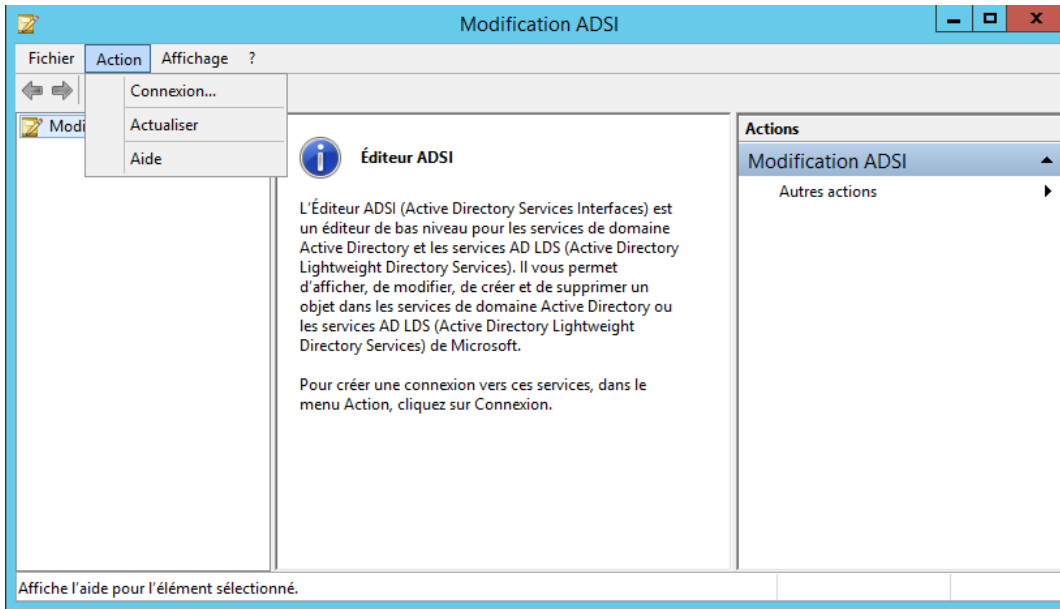
1. Création d'un objet PSO

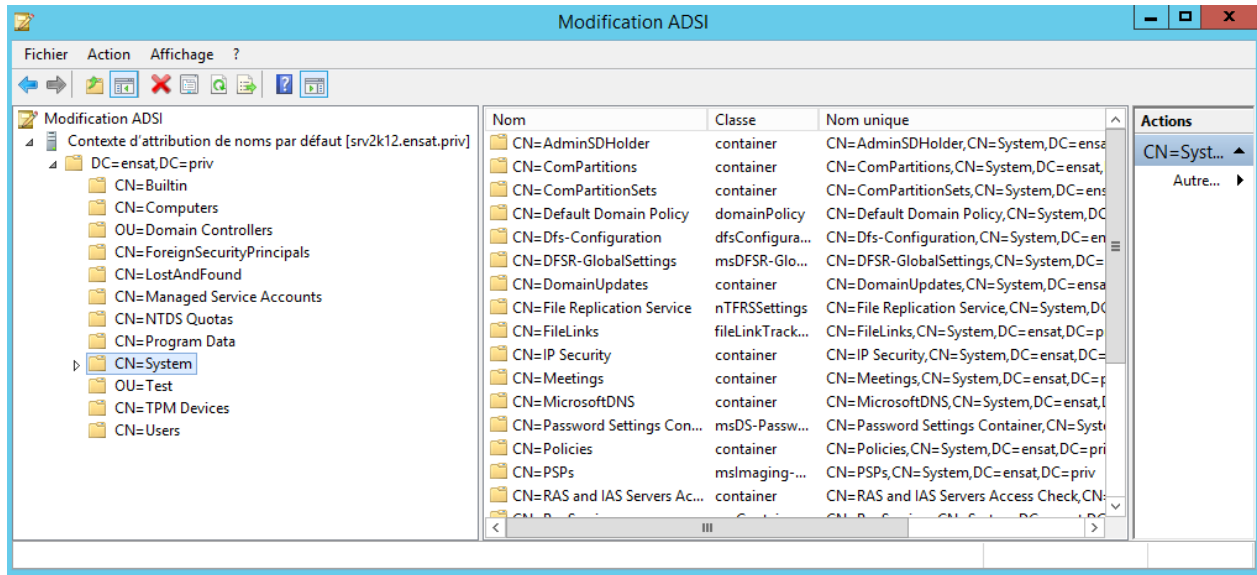
Lancez ADSIEdit.msc, développez le conteneur **CN=System** dans la partition de domaine et cliquez droit sur le « sous conteneur » **CN>Password Settings Container**. Puis choisissez « *nouvel objet* »

Ou Cliquez sur **démarrer** > **exécuter**, tapez **adsiedit.msc** et cliquez sur **OK**



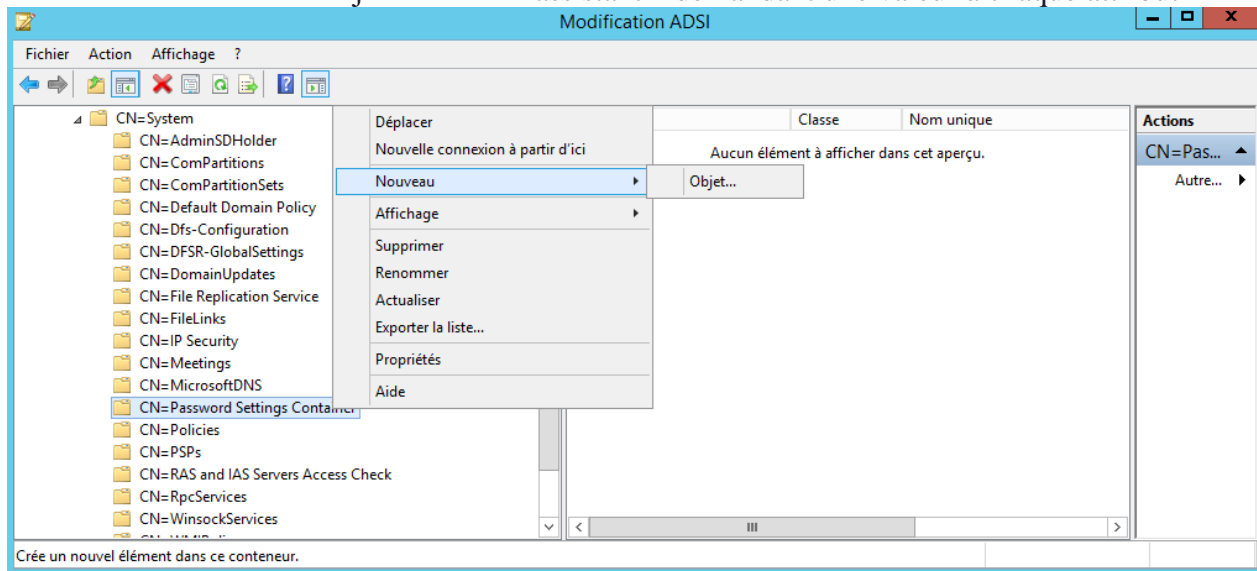
Interface de l'utilitaire Exécuter de Windows





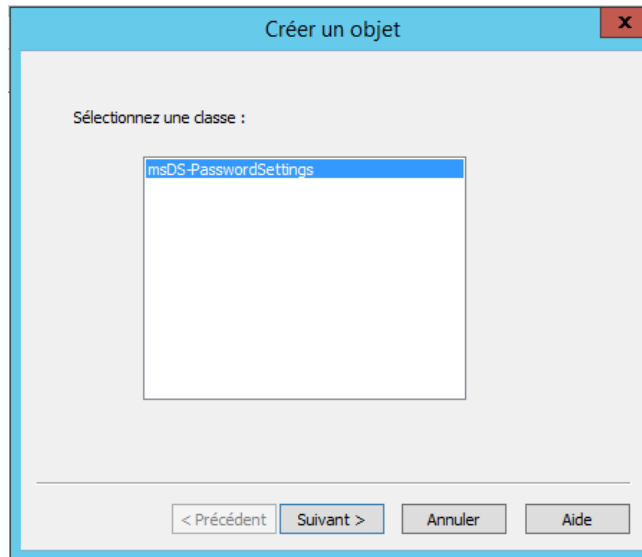
Interface de l'outil de modification ADSI

La création d'un nouvel objet lance un « assistant » demandant une valeur à chaque attribut

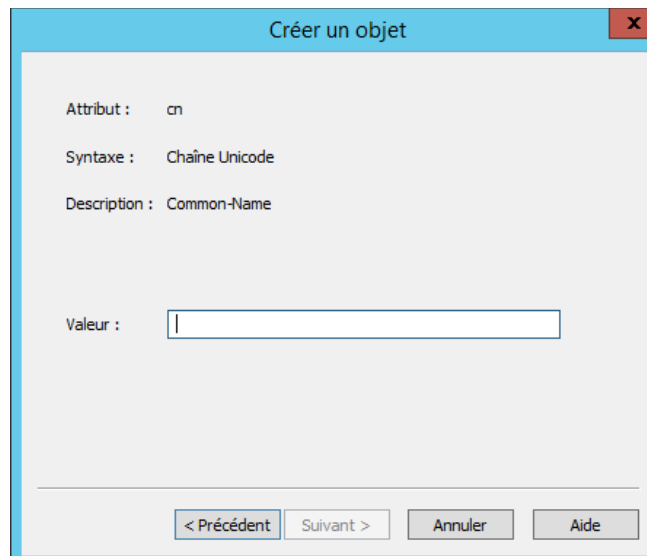


La création d'un nouvel objet via Interface de l'outil de modification ADSI

Sélectionnez **msDS-PasswordSettings** et cliquez sur **Suivant** :



Interface de création d'un objet PSO



Interface de spécification du nom du nouvel objet PSO

Spécifiez le nom de l'objet PSO en remplissant le champ **Valeur**

Créer un objet

Attribut : cn

Syntaxe : Chaîne Unicode

Description : Common-Name

Valeur : UserPwd

< Précédent Suivant > Annuler Aide

Spécifiez la valeur de l'attribut **msDS-PasswordSettingsPrecedence** en remplissant le champ **Valeur**

Créer un objet

Attribut : msDS-PasswordSettingsPrecedence

Syntaxe : Entier

Description : Password Settings Precedence

Valeur : 1

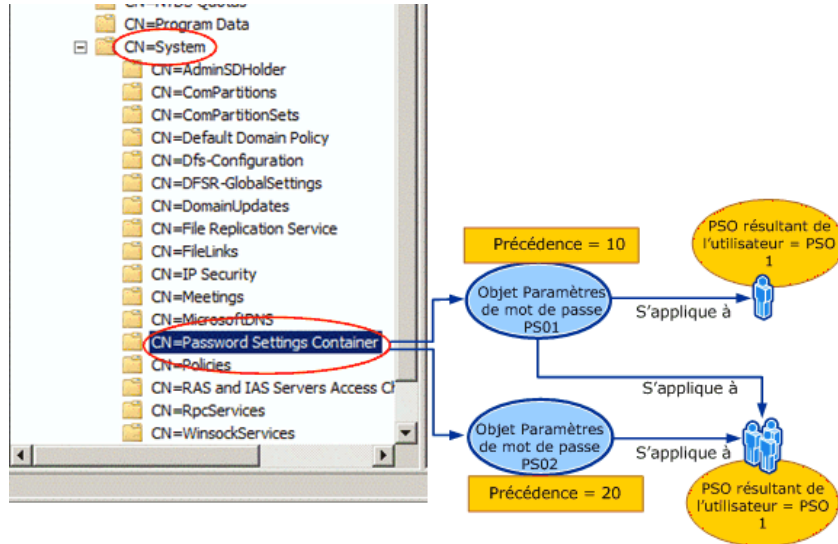
< Précédent Suivant > Annuler Aide

Interface de spécification de la valeur de l'attribut msDS-PasswordSettingsPrecedence

L'attribut **msDS-PasswordSettingsPrecedence** est utilisé pour résoudre les problèmes de conflits si de multiples PSOs sont appliqués sur un utilisateur ou un groupe de sécurité globale. La valeur de cet attribut est un entier supérieur à 0.

En effet, vous pouvez définir plusieurs stratégies de mot de passe affinées sur un même objet, dans ce cas c'est la valeur de l'attribut « **msDS-PasswordSettingsPrecedence** » qui permettra d'appliquer la bonne stratégie à l'objet. La valeur la plus basse aura la priorité. Ainsi un PSO avec une valeur à 1 sur l'attribut « **msDS-PasswordSettingsPrecedence** » sera celui appliqué à l'objet. D'autre part, si plusieurs PSO ayant la même valeur **msDS-**

PasswordSettingsPrecedence sont appliqués sur un utilisateur, le PSO dont le GUID est le plus faible sera appliqué.



Spécifiez la valeur de l'attribut **msDS-PasswordReversibleEncryptionEnabled** en remplissant le champ **Valeur**

Interface de spécification de la valeur de l'attribut msDS-PasswordReversibleEncryptionEnabled

Créer un objet

Attribut : msDS-PasswordReversibleEncryptionEnabled

Syntaxe : Booléen

Description : Password reversible encryption status for user accounts

Valeur : FALSE

< Précédent Suivant > Annuler Aide

Cet attribut représente l'enregistrement des mots de passe en utilisant un chiffrement réversible. La valeur de cet attribut doit être égale à **FALSE** pour des raisons de sécurité. La valeur de cet attribut doit être égale à **TRUE** lors de l'utilisation de l'authentification CHAP (Challenge-Handshake Authentication Protocol) par accès distant ou IAS (Internet Authentication Services). Elle est aussi requise lors de l'utilisation de l'authentification Digest dans IIS (Internet Information Services).

Spécifiez la valeur de l'attribut **msDS-PasswordHistoryLength** en remplissant le champ **Valeur**

Créer un objet

Attribut : msDS-PasswordHistoryLength

Syntaxe : Entier

Description : Password History Length for user accounts

Valeur :

< Précédent Suivant > Annuler Aide

Interface de spécification de la valeur de l'attribut msDS-PasswordHistoryLength

msDSMinimumPasswordLength :

est un entier qui définit la longueur minimale du mot de passe. La valeur par défaut est 7 sur le domaine. Dans notre exemple, la valeur minimale sera indiquée à 3 caractères.

The screenshot shows a dialog box titled "Créer un objet" with a close button (X) in the top right corner. The dialog contains the following information:

- Attribut : msDS-PasswordHistoryLength
- Syntaxe : Entier
- Description : Password History Length for user accounts
- Valeur :

At the bottom of the dialog, there are four buttons: "< Précédent", "Suivant >", "Annuler", and "Aide".

Cet attribut représente le nombre de nouveaux mots de passe uniques devant être associés à un compte d'utilisateur avant qu'un ancien mot de passe puisse être réutilisé. La valeur de cet attribut varie entre 0 et 1024.

Spécifiez la valeur de l'attribut **msDS-PasswordComplexityEnabled** en remplissant le champ **Valeur**

The screenshot shows a dialog box titled "Créer un objet" with a close button (X) in the top right corner. The dialog contains the following information:

- Attribut : msDS-PasswordComplexityEnabled
- Syntaxe : Booléen
- Description : Password complexity status for user accounts
- Valeur :

At the bottom of the dialog, there are four buttons: "< Précédent", "Suivant >", "Annuler", and "Aide".

Interface de spécification de la valeur de l'attribut msDS-PasswordComplexityEnabled

Créer un objet

Attribut : msDS-PasswordComplexityEnabled

Syntaxe : Booléen

Description : Password complexity status for user accounts

Valeur : FALSE

< Précédent Suivant > Annuler Aide

Si la valeur de cet attribut est égale à **TRUE**, les mots de passe doivent respecter les exigences minimales suivantes :

- Comporter au moins 6 caractères
- Contenir des caractères provenant de trois des quatre catégories suivantes :
 - Caractères majuscules anglais (A à Z)
 - Caractères minuscules anglais (a à z)
 - Chiffres en base 10 (0 à 9)
 - Caractères non-alphabétiques (!, ? ...)

Si la valeur de cet attribut est égale à **FALSE**, les mots de passe ne sont pas obligés de respecter les exigences déjà mentionnées

Spécifiez la valeur de l'attribut **msDS-MinimumPasswordLength** en remplissant le champ **Valeur**

Créer un objet

Attribut : msDS-MinimumPasswordLength

Syntaxe : Entier

Description : Minimum Password Length for user accounts

Valeur :

< Précédent Suivant > Annuler Aide

Interface de spécification de la valeur de l'attribut msDS-MinimumPasswordLength

Créer un objet

Attribut : msDS-MinimumPasswordLength

Syntaxe : Entier

Description : Minimum Password Length for user accounts

Valeur :

< Précédent Suivant > Annuler Aide

Cet attribut représente la longueur minimale du mot de passe. Il détermine le nombre minimal de caractères que doit contenir le mot de passe d'un compte d'utilisateur. La valeur de ce paramètre varie entre 1 et 255. Pour permettre l'utilisation de mots de passe vides, spécifiez 0 comme valeur de ce paramètre.

Spécifiez la valeur de l'attribut **msDS-MinimumPasswordAge** en remplissant le champ **Valeur**

Créer un objet

Attribut : msDS-MinimumPasswordAge

Syntaxe : Durée

Description : Minimum Password Age for user accounts

Valeur :

< Précédent Suivant > Annuler Aide

Interface de spécification de la valeur de l'attribut msDS-MinimumPasswordAge

Créer un objet

Attribut : msDS-MinimumPasswordAge

Syntaxe : Durée

Description : Minimum Password Age for user accounts

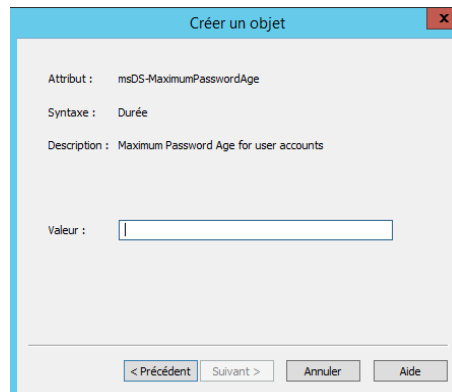
Valeur :

< Précédent Suivant > Annuler Aide

Cet attribut représente la durée de vie minimale du mot de passe. Il détermine la période minimale d'utilisation d'un mot de passe avant que l'utilisateur puisse le changer. La valeur de ce paramètre doit être inférieure à celle du paramètre « Durée de vie maximale du mot de passe ». Si la valeur est égale à 00:00:00:00, des changements immédiats de mots de passe sont permis.

La valeur de cet attribut est écrite sous le format j:hh:mm:ss.

Spécifiez la valeur de l'attribut **msDS-MaximumPasswordAge** en remplissant le champ **Valeur**



Créer un objet

Attribut : msDS-MaximumPasswordAge

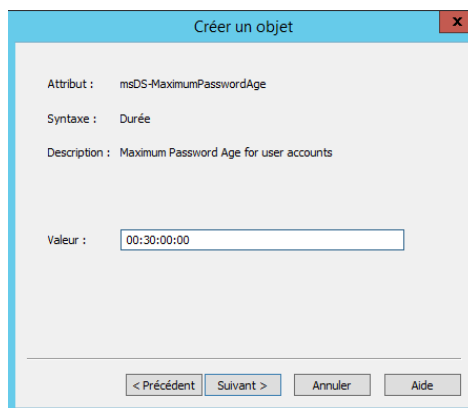
Syntaxe : Durée

Description : Maximum Password Age for user accounts

Valeur :

< Précédent Suivant > Annuler Aide

Interface de spécification de la valeur de l'attribut msDS-MaximumPasswordAge



Créer un objet

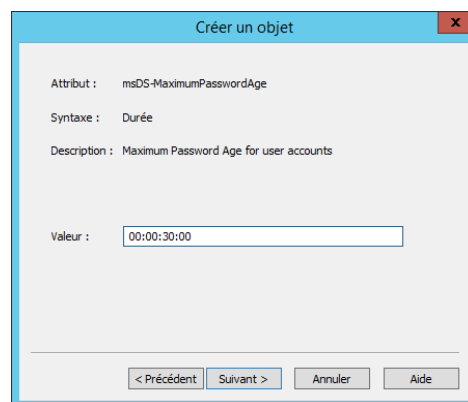
Attribut : msDS-MaximumPasswordAge

Syntaxe : Durée

Description : Maximum Password Age for user accounts

Valeur :

< Précédent Suivant > Annuler Aide



Créer un objet

Attribut : msDS-MaximumPasswordAge

Syntaxe : Durée

Description : Maximum Password Age for user accounts

Valeur :

< Précédent Suivant > Annuler Aide

Créer un objet

Attribut : msDS-MaximumPasswordAge

Syntaxe : Durée

Description : Maximum Password Age for user accounts

Valeur :

< Précédent Suivant > Annuler Aide

Cet attribut représente la durée de vie maximale du mot de passe. Il détermine la période maximale d'utilisation d'un mot de passe avant que l'utilisateur puisse le changer. Si la valeur est égale à 00:00:00:00, les mots de passe n'expirent jamais.

La valeur de cet attribut est écrite sous le format j:hh:mm:ss.

Spécifiez la valeur de l'attribut **msDS-LockoutThreshold** en remplissant le champ **Valeur**

Créer un objet

Attribut : msDS-LockoutThreshold

Syntaxe : Entier

Description : Lockout threshold for lockout of user accounts

Valeur :

< Précédent Suivant > Annuler Aide

Interface de spécification de la valeur de l'attribut msDS-LockoutThreshold

Créer un objet

Attribut : msDS-LockoutThreshold

Syntaxe : Entier

Description : Lockout threshold for lockout of user accounts

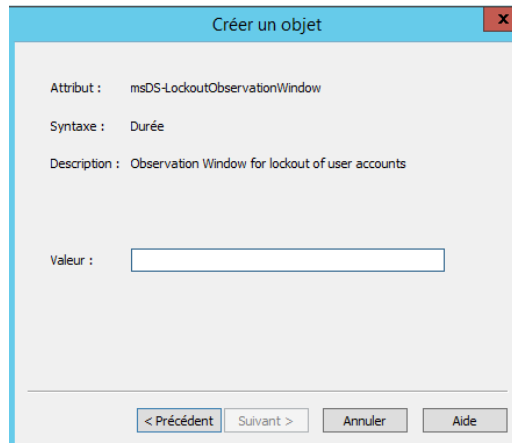
Valeur :

< Précédent Suivant > Annuler Aide

Cet attribut représente le seuil de verrouillage pour le verrouillage des comptes d'utilisateurs. La valeur de cet attribut varie entre 0 et 65535.

Pour désactiver les stratégies de verrouillage de compte, affectez la valeur 0 à l'attribut **msDS-LockoutThreshold**

Spécifiez la valeur de l'attribut **msDS-LockoutObservationWindows** en remplissant le champ **Valeur**

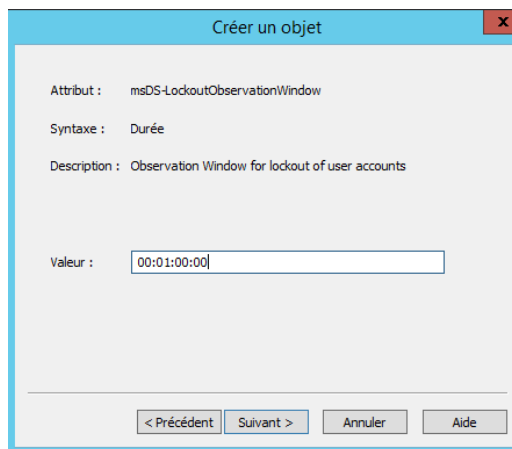


The screenshot shows a dialog box titled "Créer un objet" with a close button (X) in the top right corner. The dialog contains the following information:

- Attribut : msDS-LockoutObservationWindow
- Syntaxe : Durée
- Description : Observation Window for lockout of user accounts
- Valeur : [Empty text input field]

At the bottom of the dialog, there are four buttons: "< Précédent", "Suivant >", "Annuler", and "Aide".

Interface de spécification de la valeur de l'attribut msDS-LockoutObservationWindow



The screenshot shows the same dialog box as above, but the "Valeur" field now contains the text "00:01:00:00".

Cet attribut représente la fenêtre d'observation pour le verrouillage des comptes d'utilisateurs. Il permet de réinitialiser le compteur de verrouillages du compte après la durée de votre choix

La valeur de cet attribut est écrite sous le format j:hh:mm:ss.

Spécifiez la valeur de l'attribut **msDS-LockoutDuration** en remplissant le champ **Valeur**

Créer un objet

Attribut : msDS-LockoutDuration

Syntaxe : Durée

Description : Lockout duration for locked out user accounts

Valeur :

< Précédent Suivant > Annuler Aide

Interface de spécification de la valeur de l'attribut msDS-LockoutDuration

Créer un objet

Attribut : msDS-LockoutDuration

Syntaxe : Durée

Description : Lockout duration for locked out user accounts

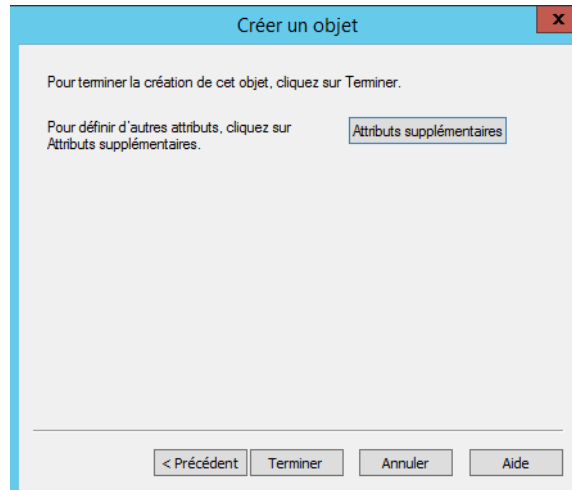
Valeur :

< Précédent Suivant > Annuler Aide

Cet attribut représente la durée de verrouillage pour les comptes d'utilisateurs verrouillés. Indique la durée de verrouillage des comptes en cas de X mauvais mots de passe saisis à plusieurs reprises (X représentant la valeur de msDSLockoutThreshold).

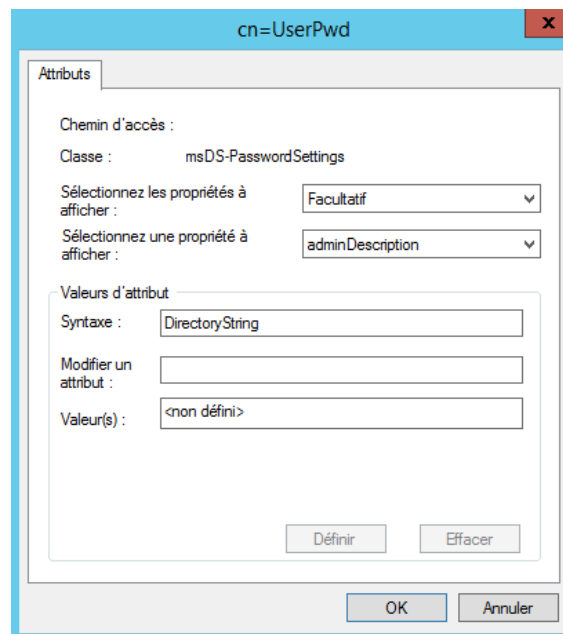
La valeur de cet attribut est écrite sous le format j:hh:mm:ss.

Cliquez sur **Terminer** pour finir la création de l'objet PSO



Interface de la fin de création d'un nouvel objet PSO

Une fois ces valeurs renseignées, l'assistant vous propose de donner une valeur à des attributs supplémentaires. Il reste l'attribut « **msDS-PSOAppliesTo** » à renseigner pour affecter le PSO à un groupe ou utilisateur. Cliquez sur "Attributs supplémentaires" ou « *More attributes* » :



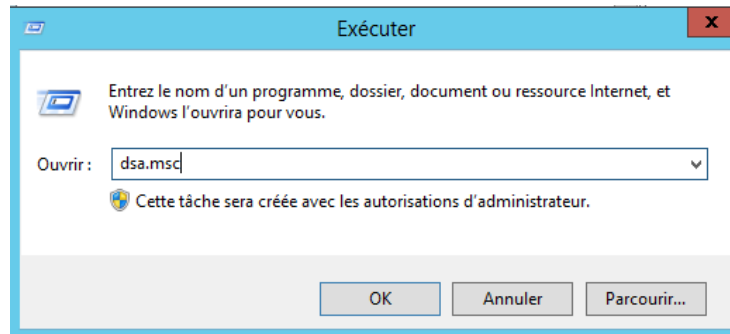
et choisissez l'attribut « **msDS-PSOAppliesTo** » puis dans la partie « *Edit Attribute* » donnez le DN de l'utilisateur ou groupe sur lequel la stratégie va s'appliquer.

2. Application des objets PSO aux utilisateurs et aux groupes de sécurité globaux

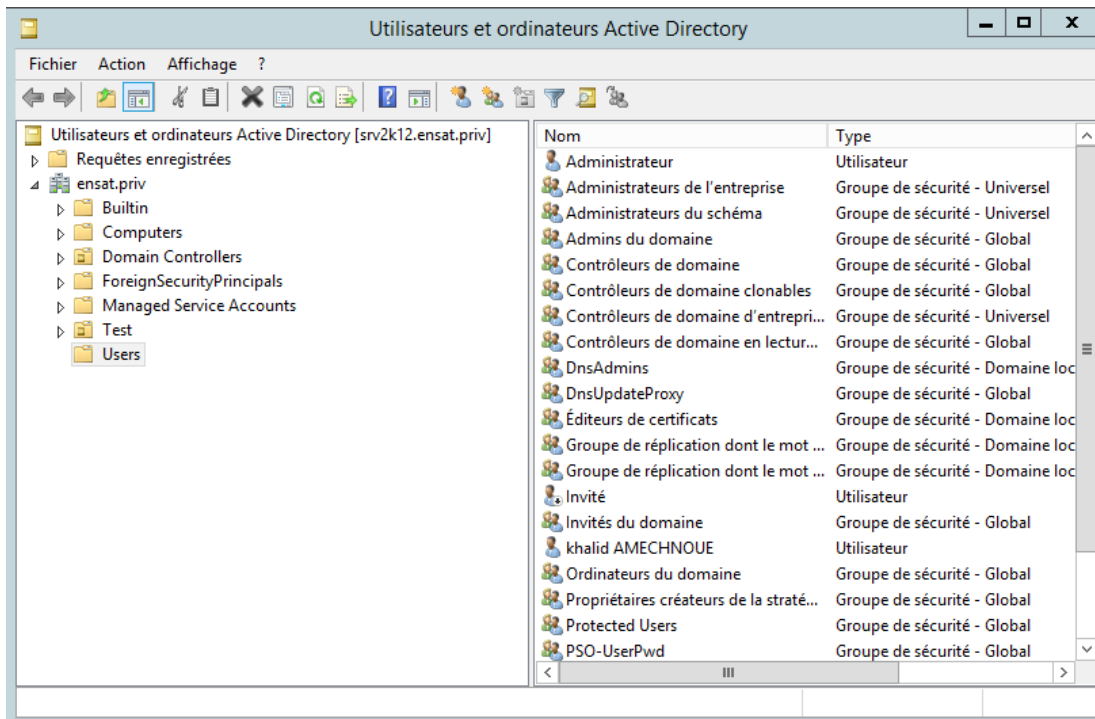
Pour appliquer des objets PSO aux utilisateurs et aux groupes de sécurité globaux, procédez

comme suit :

Cliquez sur **démarrer** > **exécuter**, tapez **dsa.msc** et cliquez sur **OK**

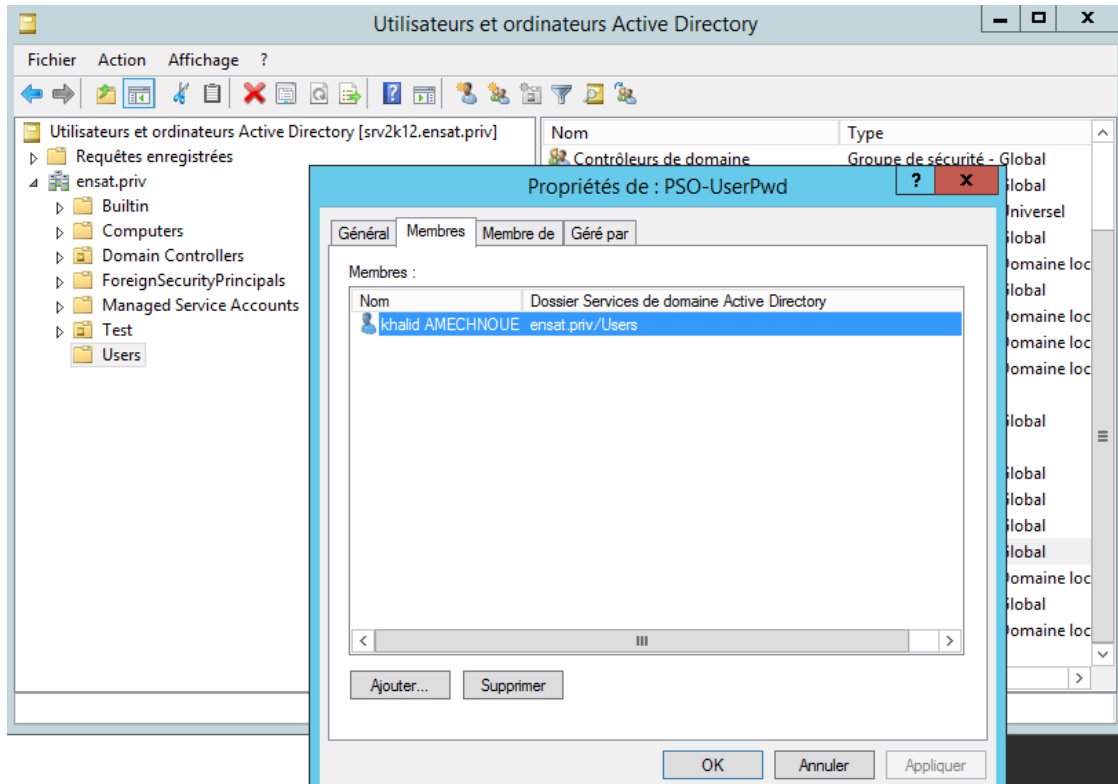


Interface de l'utilitaire Exécuter de Windows

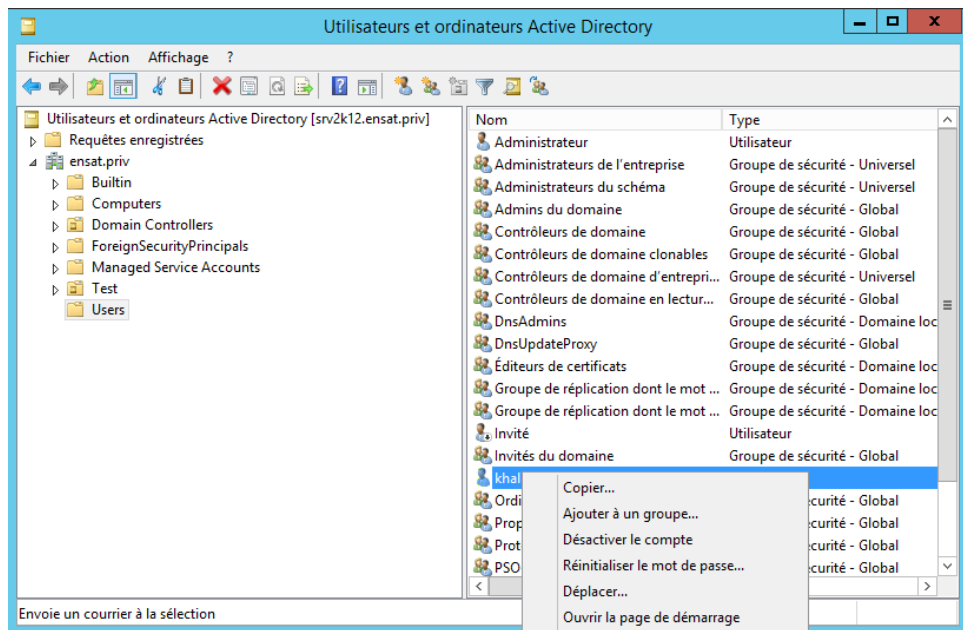


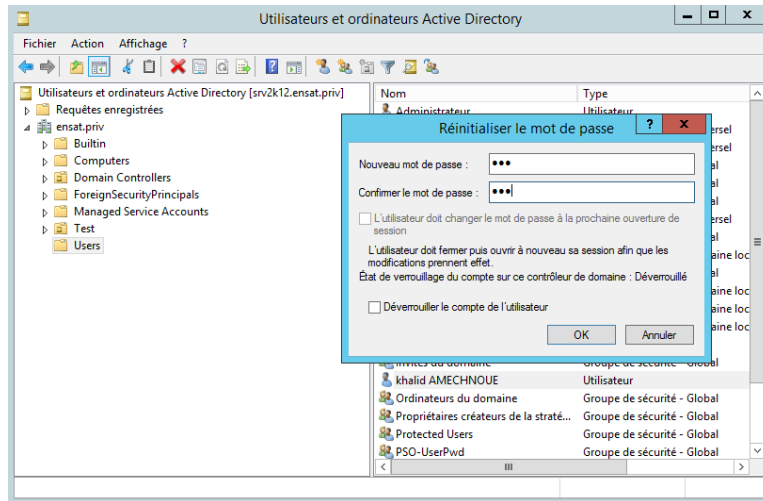
Interface de l'outil d'administration Utilisateurs et ordinateurs Active Directory

On crée un nouveau groupe : PSO-UserPwd,, auquel on ajout un utilisateur :

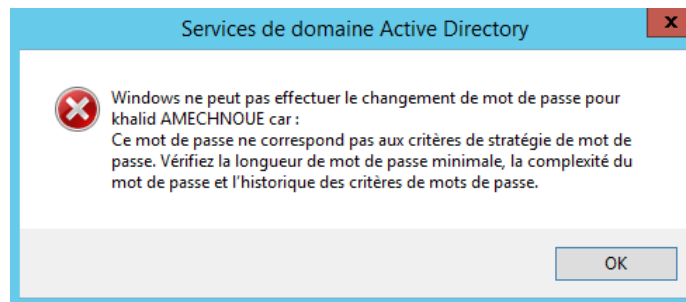


On réinitialise le mot de passe à 1234 :

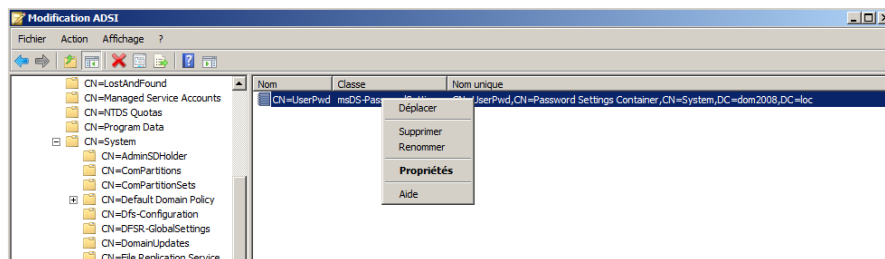


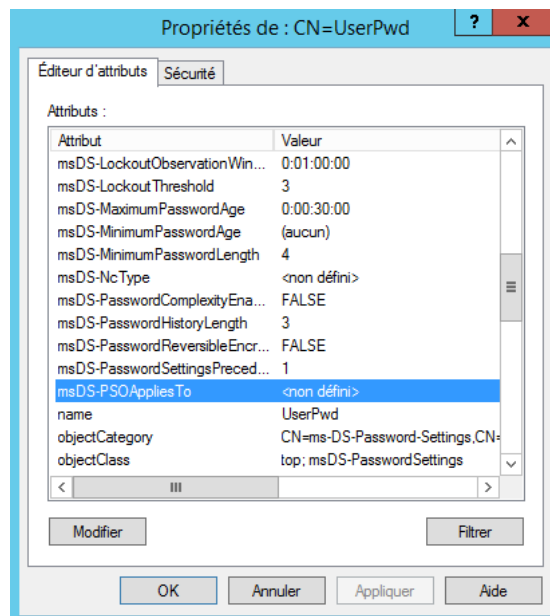
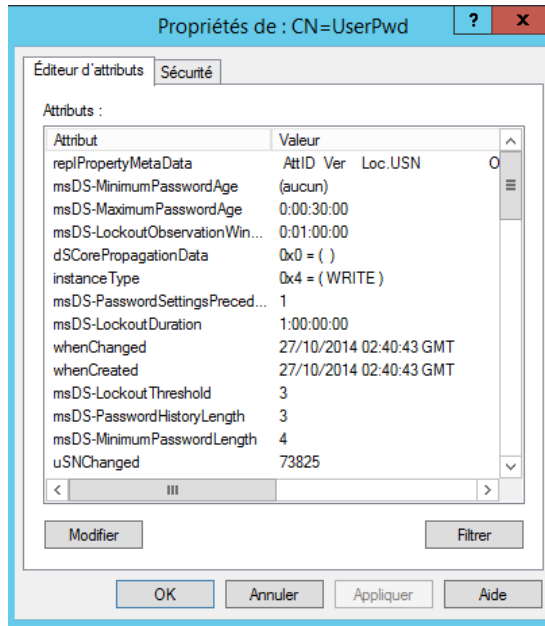


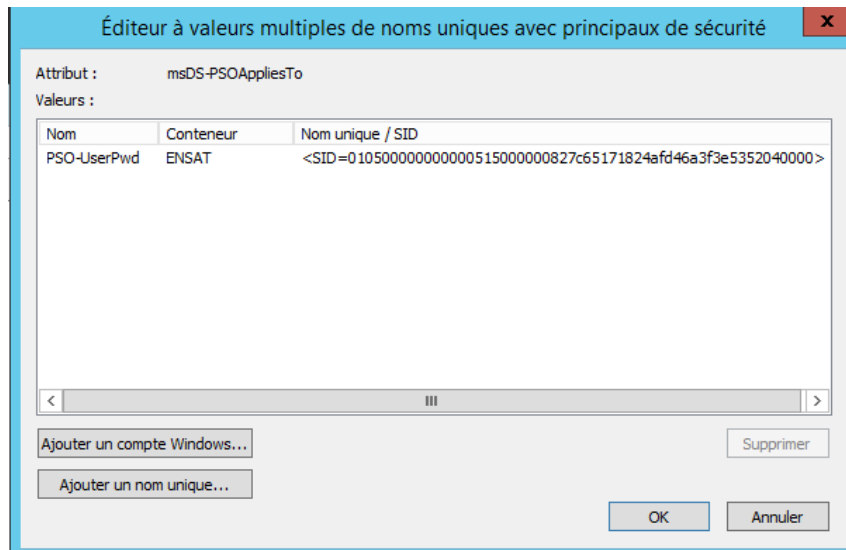
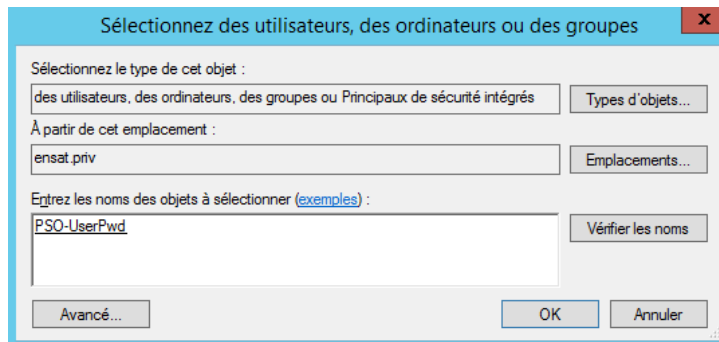
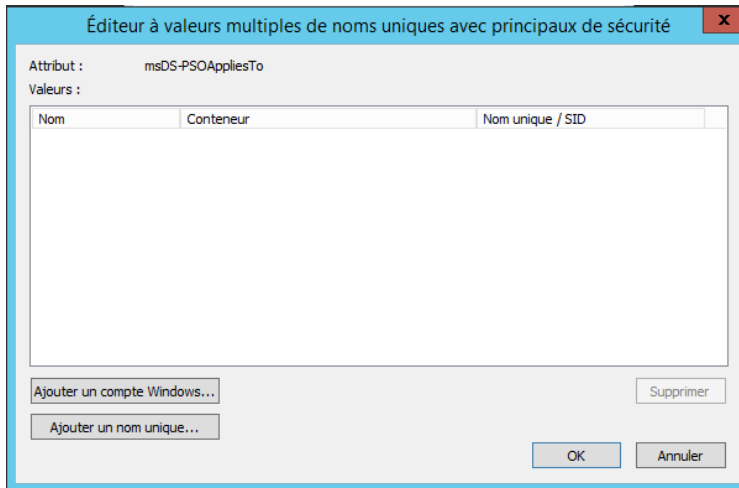
Mot de passe 1234

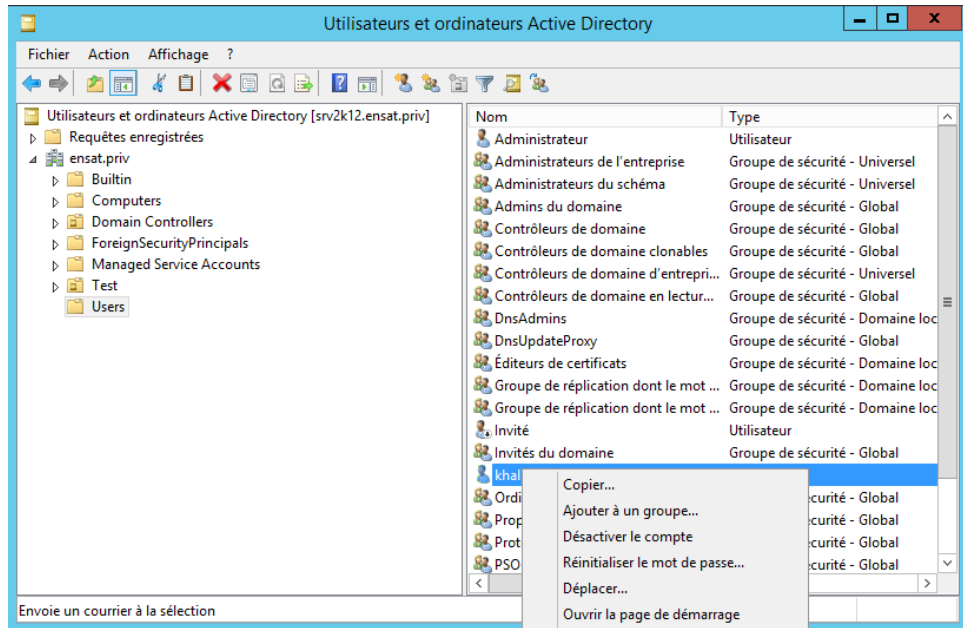
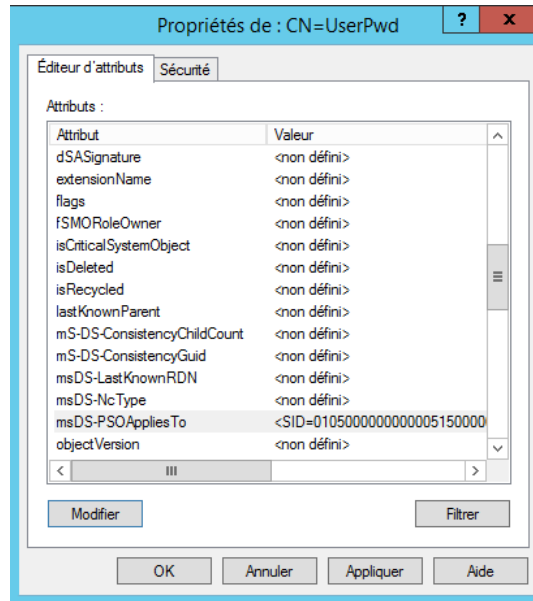


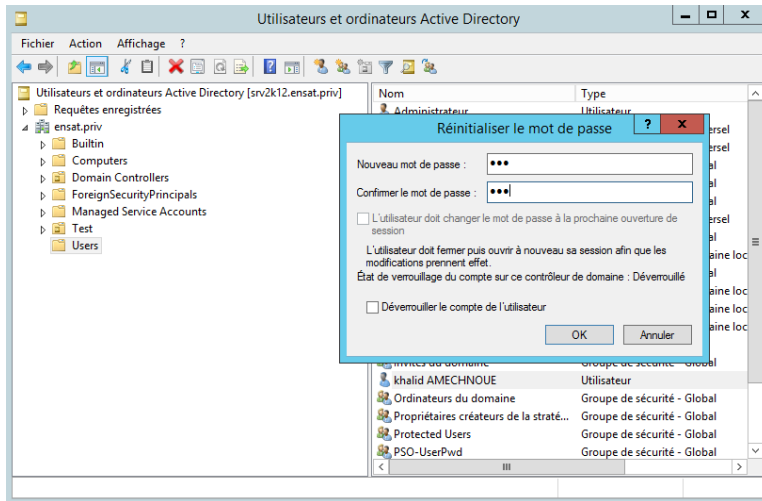
Pour pouvoir réinitialiser le mot de passe à 1234 il faut appliquer la PSO : UserPwd au groupe PSO-UserPwd :



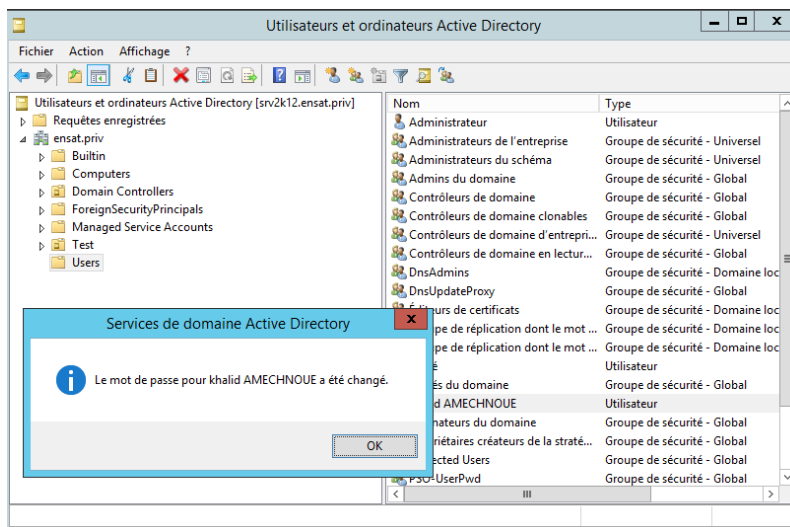


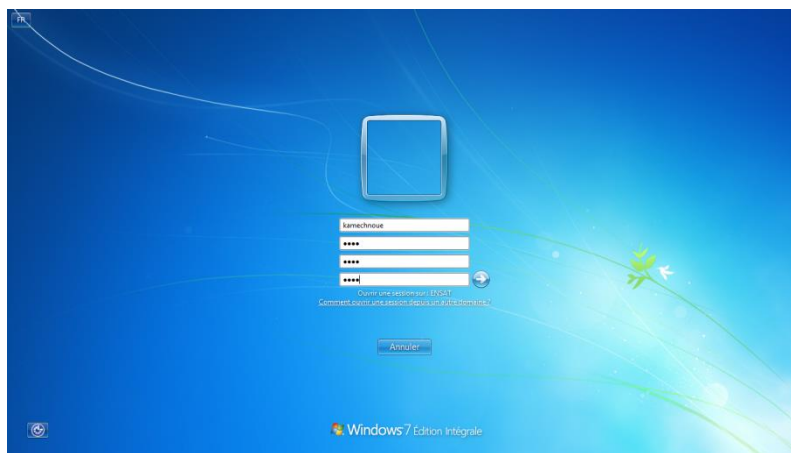
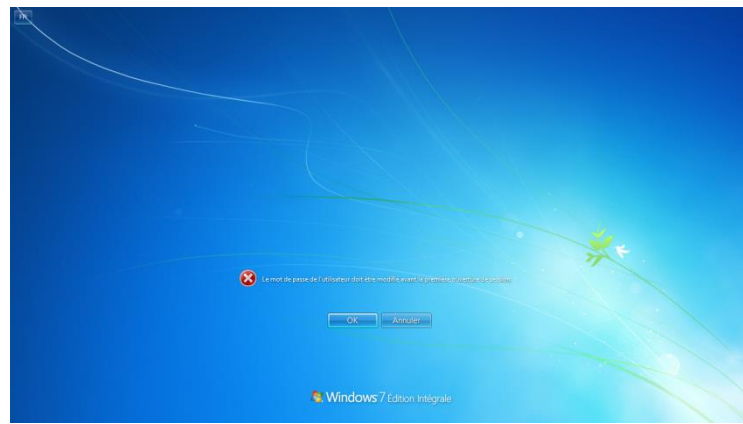
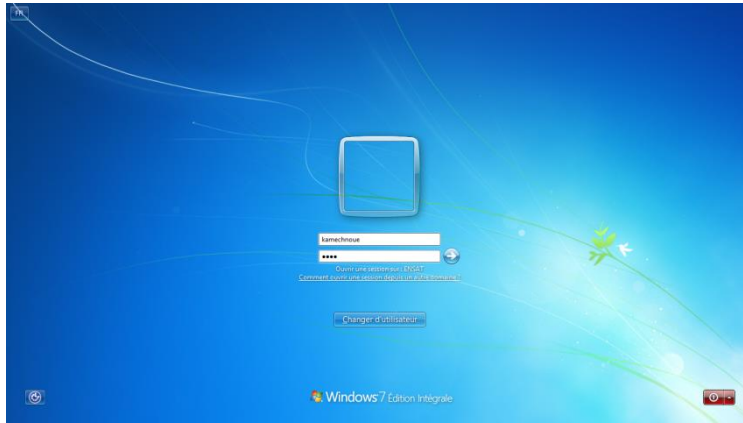




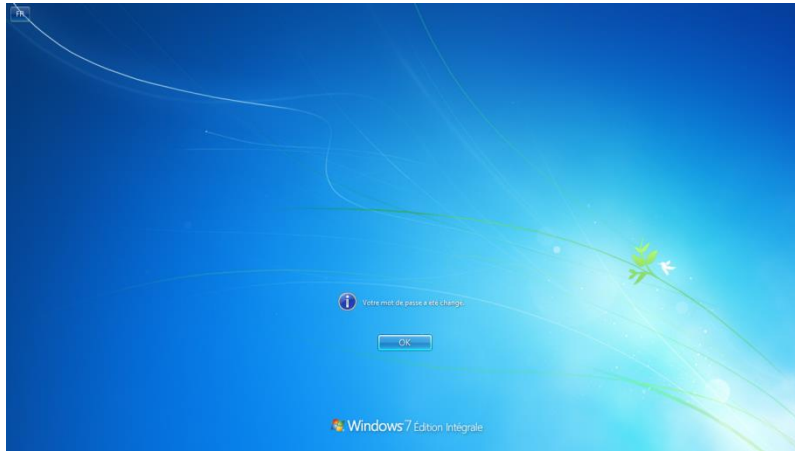


Mot de passe 1234





Mot de passe : azer



Si plusieurs PSO sont appliqués sur un utilisateur ou un groupe. Le PSO résultant appliqué est déterminé en utilisant la technique suivante :

- Si un objet PSO est directement appliqué sur un utilisateur, le PSO résultant sera cet objet PSO (Il n'est pas recommandé d'appliquer directement plusieurs PSO sur le même utilisateur).
- Si aucun objet PSO n'est directement appliqué sur un utilisateur et des objets PSO sont appliqués sur les groupes de sécurité dont cet utilisateur est membre, le PSO résultant sera le PSO disposant la valeur minimale de l'attribut **msDS-PasswordSettingsPrecedence**.
- Si aucun objet PSO n'est appliqué directement sur un utilisateur ou un groupe de sécurité dont cet utilisateur est membre, la stratégie de mot de passe / de verrouillage du compte sera appliquée.

Pour pouvoir utiliser la technique mentionnée dans cet article, le niveau fonctionnel du domaine doit être égal ou supérieur à **Windows Server 2008**

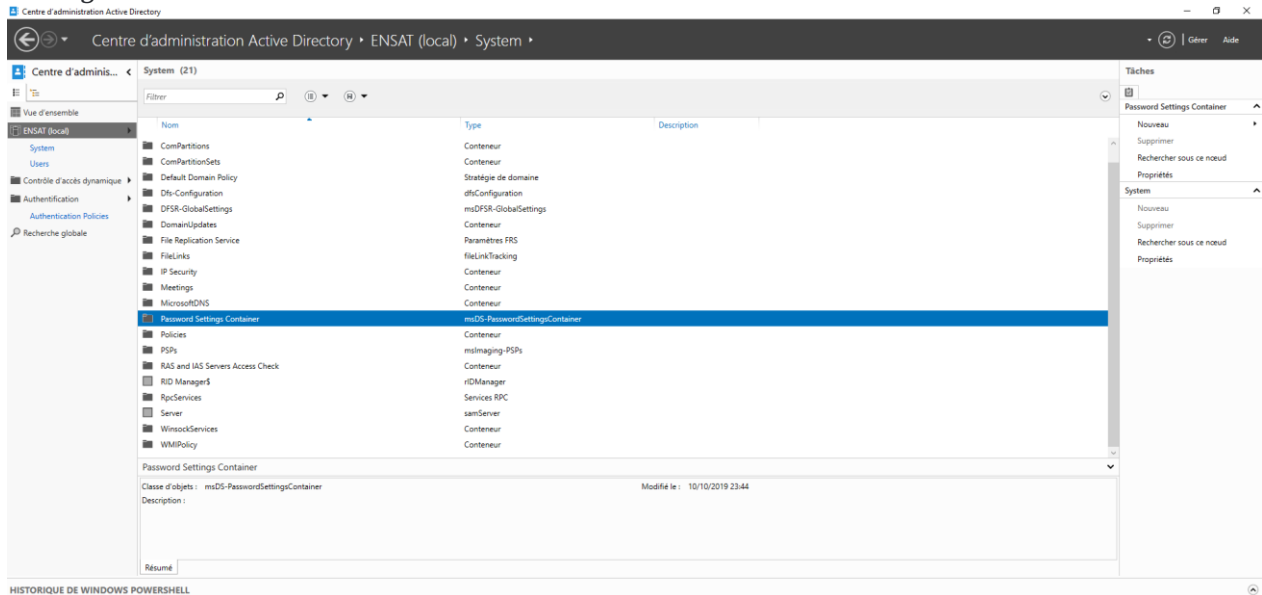
Attention : Les PSO, contrairement à des GPO classiques ne s'appliquent pas directement aux unités organisationnelles (OU). Si vous souhaitez appliquer ce type de stratégie à tous les utilisateurs d'une OU particulière, il vous faudra créer un groupe appelé « groupe intermédiaire » (ou shadow) contenant tous les utilisateurs de l'OU, afin d'y appliquer votre PSO.

Evidemment, sachant que l'opération est manuelle, vous devrez mettre à jour le groupe à chaque déplacement de ou vers l'OU en question. Toutefois, gardez en tête d'une part que Windows 2008 peut gérer des tâches planifiées basées sur des événements, et de l'autre part le scripting. Les deux mélangés devraient vous permettre d'automatiser correctement les gestions de shadow groups.

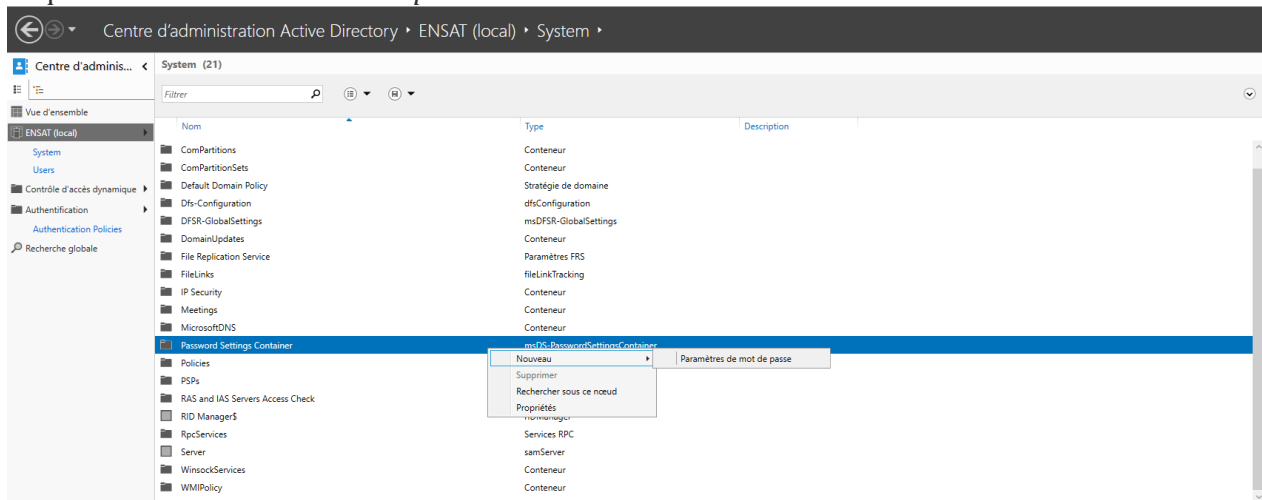
Création de la stratégie de mot de passe affinée en utilisant l'outil : Centre d'administration Active Directory

Pour créer la politique de mot de passe affinée, connectez-vous au contrôleur de domaine en utilisant un compte d'administrateur du domaine et cliquez sur Gestionnaire de serveur . Pour activer la stratégie de mot de passe affinée, vous devez ouvrir le **Centre d'administration**

Active Directory, passer en mode arborescence et accédez au dossier système, puis *Password Settings Container*.



Effectuez alors un clic-droit sur *»Password Setting Container»* et sélectionnez *Nouveau* enfin, cliquez sur *Paramètres mot de passe*.



Vous voici dans l'interface de création d'une stratégie de mot de passe.

Créer Paramètres de mot de passe :

Paramètres de mot de passe

S'applique directement à

Nom : *

Priorité : *

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 :

Options d'âge du mot de passe :

Appliquer l'âge minimal de mot de passe
L'utilisateur ne peut pas changer le mot de passe d'i... * 1

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 : *
Réinitialiser le nombre de tentatives de connexion écho... * 30

Le compte va être verrouillé

Pendant une durée de (mins) : * 30

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

S'applique directement à

Nom Courrier

Ajouter...
Supprimer

Informations supplémentaires... OK Annuler

Définissez un nom puis la priorité. A savoir que, **selon Microsoft**, une valeur inférieure pour l'attribut de priorité indique un rang plus élevé, ou une priorité plus élevée. C'est à dire qu'ici par exemple, mon **PSO (Password Setting Object)** une valeur de priorité de 2. Si un autre PSO a une valeur de priorité supérieure (de 4 par exemple) et bien c'est le PSO qui a la valeur de priorité 2 qui est prioritaire et donc appliqué à l'objet.

Créer Paramètres de mot de passe : GINF2

Paramètres de mot de passe

S'applique directement à

Nom : * GINF2

Priorité : * 1

Appliquer la longueur minimale du mot de passe
Longueur minimale du mot de passe (caractères) : * 1

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 :

Options d'âge du mot de passe :

Appliquer l'âge minimal de mot de passe
L'utilisateur ne peut pas changer le mot de passe d'i... * 1

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... * 5

Le compte va être verrouillé

Pendant une durée de (mins) : * 30

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

S'applique directement à


Nom Courrier

Ajouter...
Supprimer

Informations supplémentaires... OK Annuler

Créez un groupe dans l'AD «GINF2 users».

Nouvel objet - Utilisateur ✕

 Créer dans : ENSAT.loc/ENSAT/GINF2

Prénom : Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur :

@ENSAT.loc ▾

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

< Précédent Suivant > Annuler

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Utilisateurs et ordinateurs Active Directory

- Requêtes enregistrées
- ENSAT.loc
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Managed Service Accounts
 - Users
 - ENSAT
 - GINF2

Nom	Type	Description
Khalid Amechnoue	Utilisateur	

Context menu options:

- Délégation de contrôle...
- Déplacer...
- Rechercher...
- Nouveau** >
 - Ordinateur
 - Contact
 - Groupe
 - InetOrgPerson
 - msDS-ShadowPrincipalContainer
 - mslmaging-PSPs
 - Alias de file d'attente MSMQ
 - Unité d'organisation
 - Imprimante
 - Utilisateur
 - Dossier partagé
- Toutes les tâches >
- Actualiser
- Exporter la liste...
- Affichage >
- Réorganiser les icônes >
- Aligner les icônes
- Propriétés
- Aide

Nouvel objet - Groupe

Créer dans : ENSAT.loc/ENSAT/GINF2

Nom du groupe : GINF2 users

Nom de groupe (antérieur à Windows 2000) : GINF2 users

Étendue du groupe

Domaine local

Globale

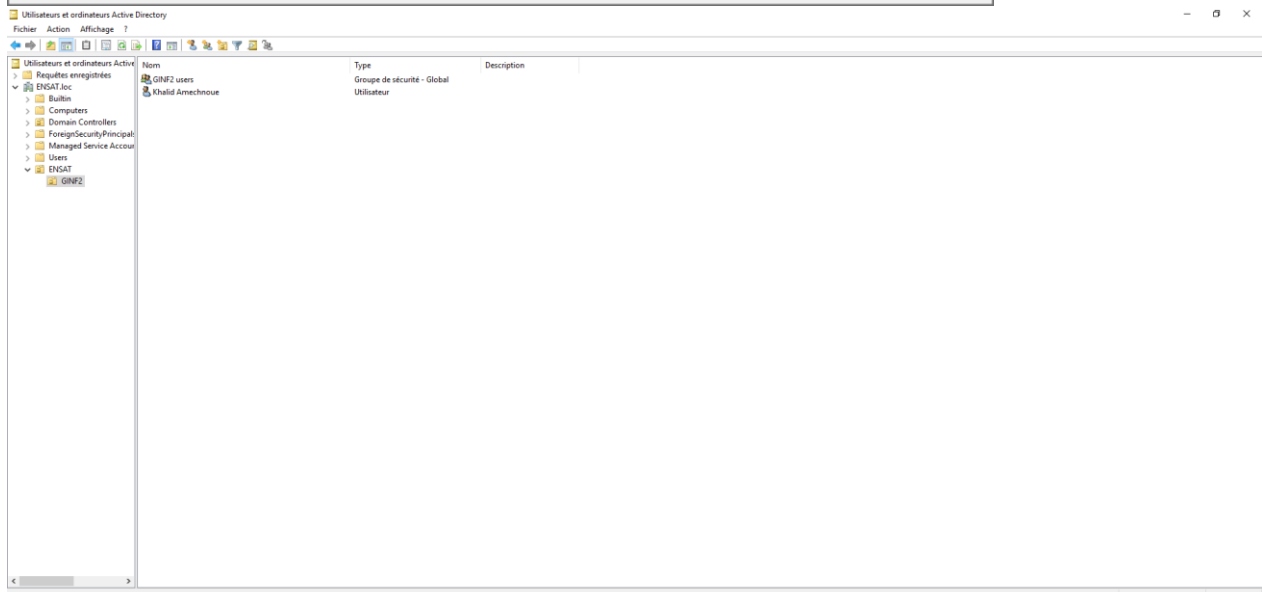
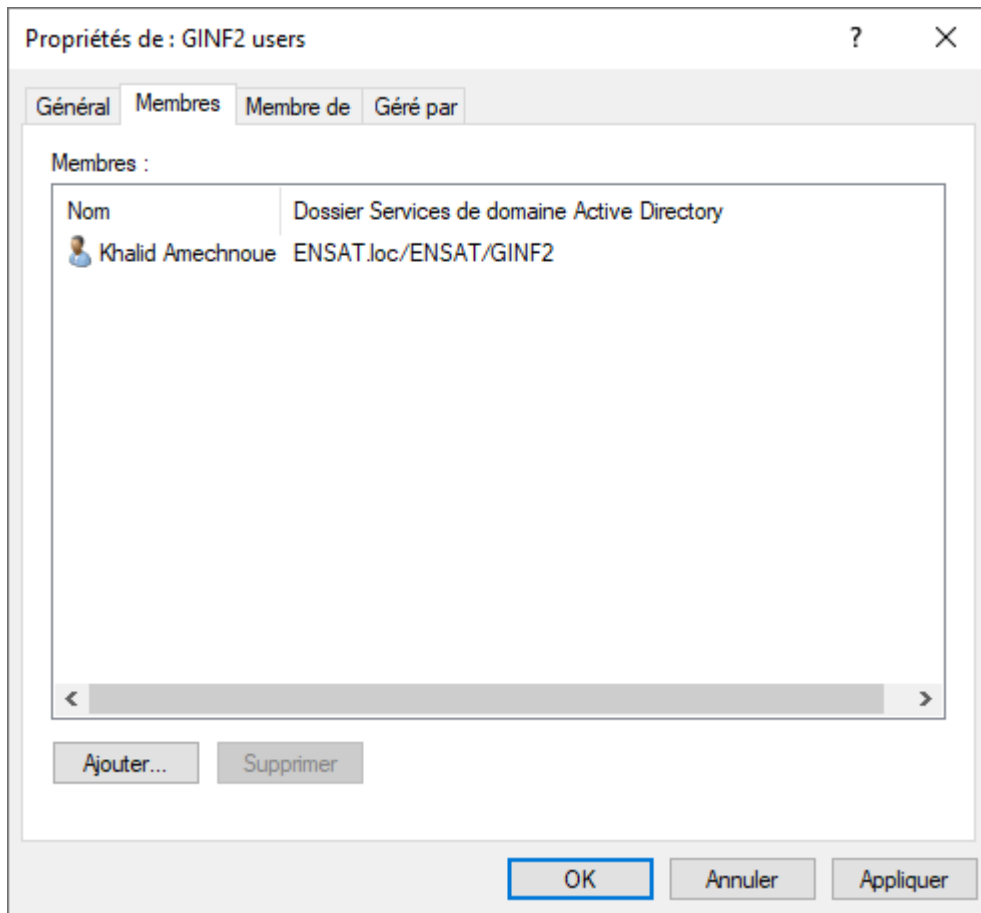
Universelle

Type de groupe

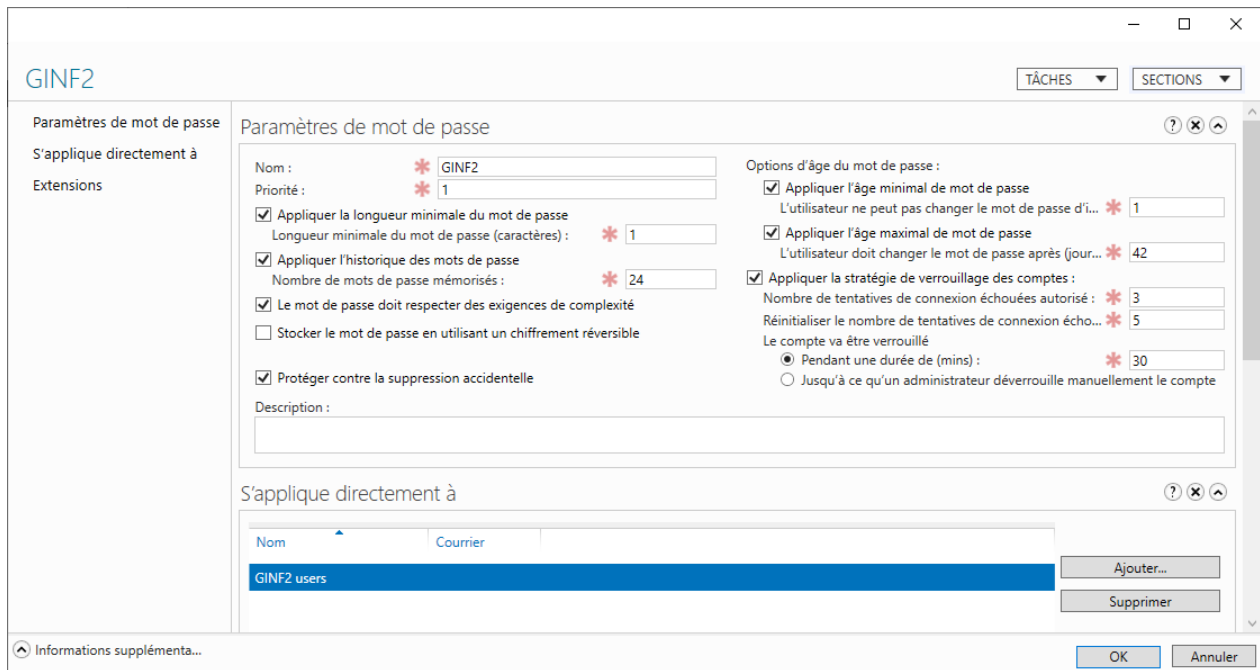
Sécurité

Distribution

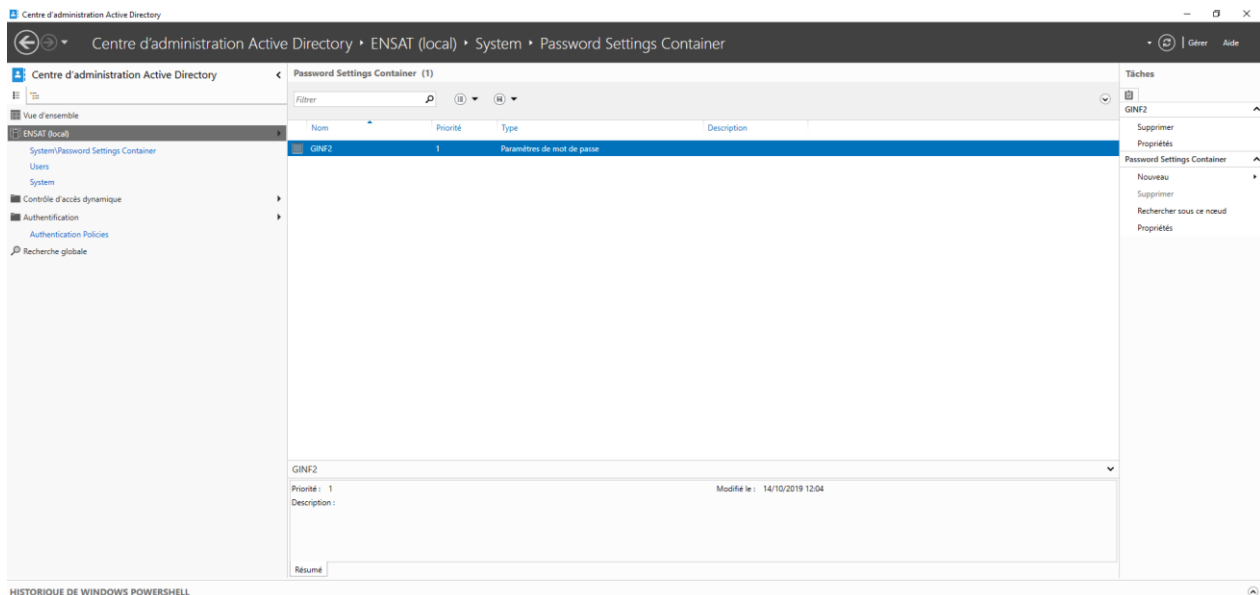
OK Annuler



Maintenant, vous devez appliquer ce PSO à un ou plusieurs groupes. Dans mon cas, j'appliquerai ce PSO aux utilisateurs d'ordinateurs portables.



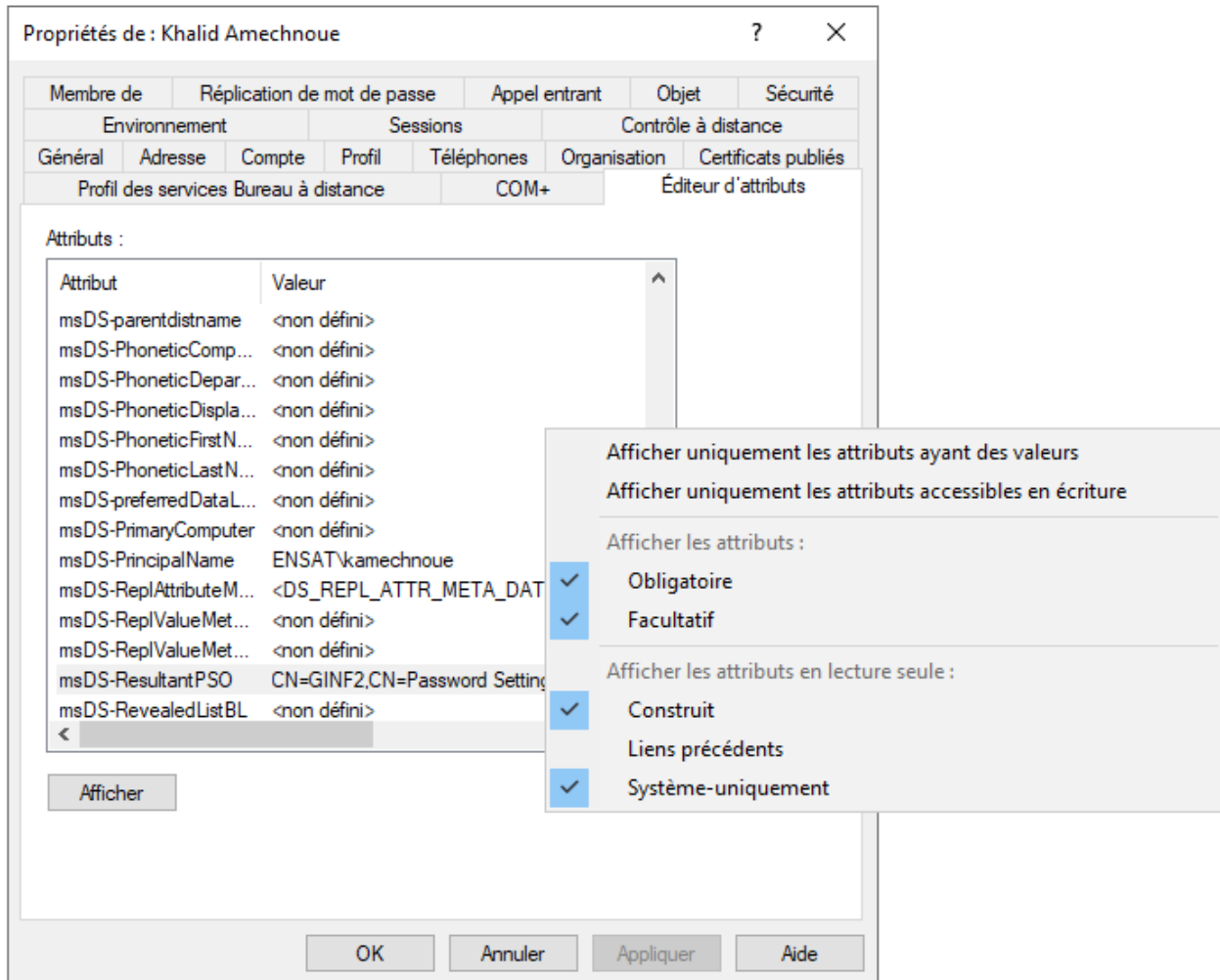
Cliquez sur *Ajouter* et ajouter le groupe puis cliquez sur OK.



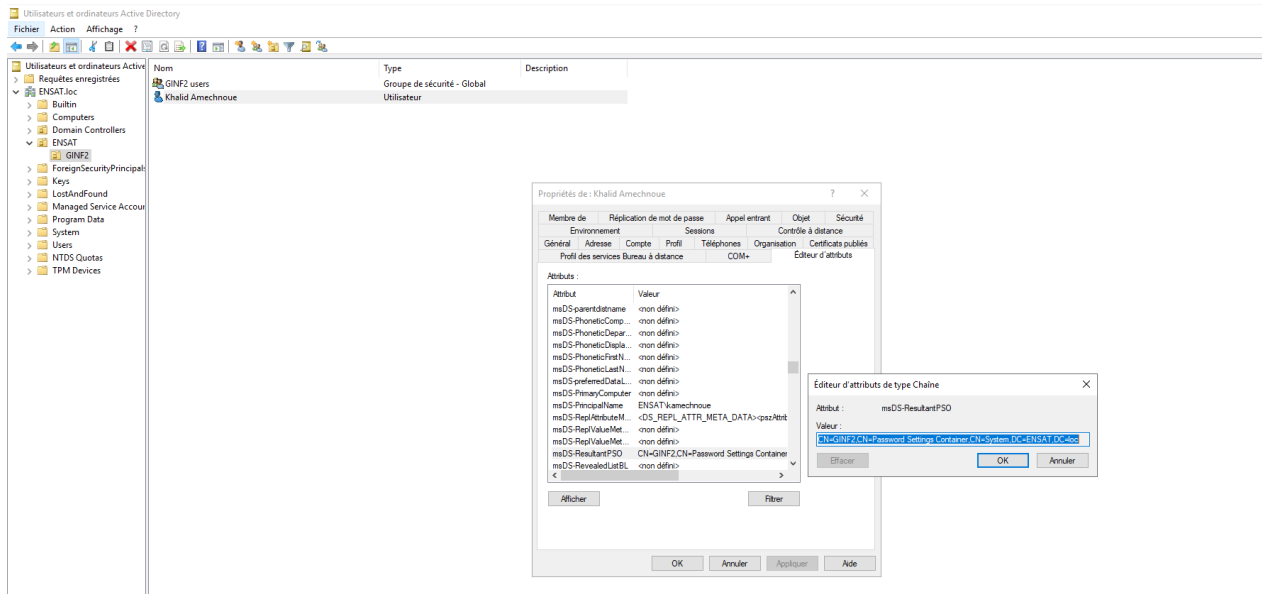
Vérifier l'application de la stratégie de mot de passe affinée

Il est possible de vérifier si le PSO est bien activé sur nos utilisateurs. Pour cela, lancer la console **Utilisateurs et ordinateurs Active Directory**. Dans le menu Affichage, assurez-vous

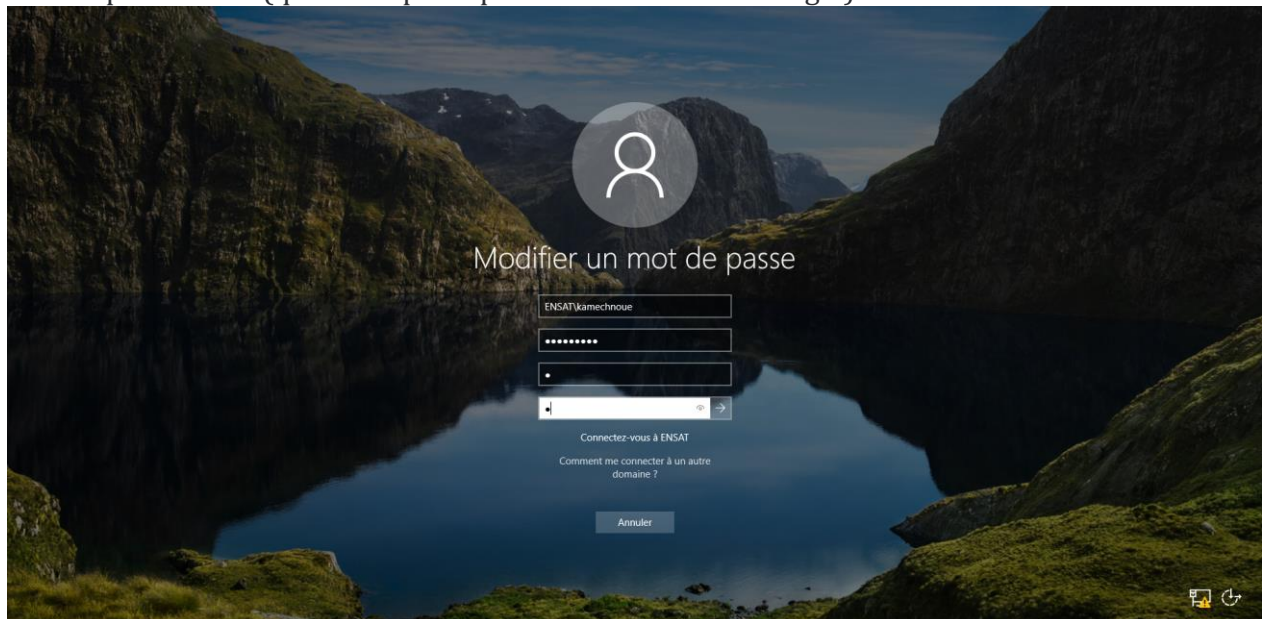
que les Fonctionnalités avancées soient activées. Dans l'arborescence de la console, cliquez sur ENSAT puis GINF2, puis double cliquez sur un utilisateur faisant partie du groupe GINF2 Users. Cliquez sur l'onglet *Éditeur d'attributs*, puis cliquez sur *Filtrer*. Vérifiez que la case *Construit* est sélectionnée.



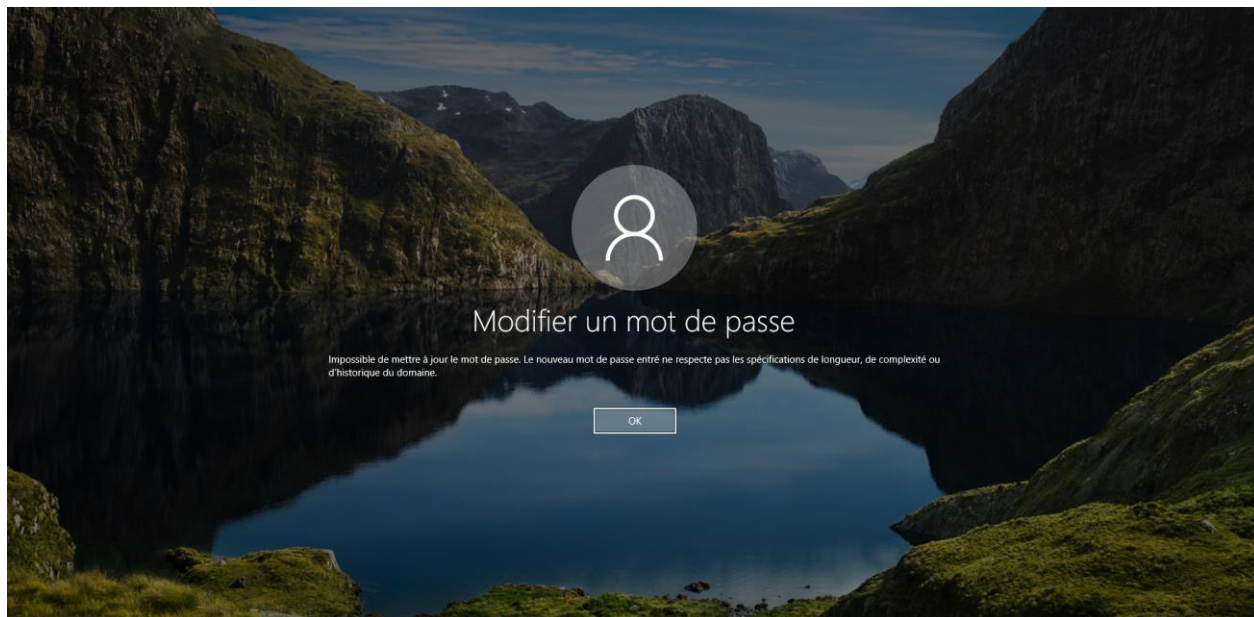
Recherchez l'attribut msDS-ResultantPSO dans la liste. Ici, on peut voir que la PSO est appliquée.



Et si on essaie de changer le mot de passe de notre utilisateur depuis son ordinateur avec un mot de passe court (qui ne respecte pas notre nouvelle stratégie)



On obtient un message d'erreur.



C'est un comportement tout à fait normal puisque nous avons spécifié dans notre PSO que le mot de passe doit répondre aux exigences de complexité.

Pour faire on décoche la case « Le mot de passe doit respecter des exigences de complexité »

GINF2

TÂCHES SECTIONS

Paramètres de mot de passe

S'applique directement à

Extensions

Paramètres de mot de passe

Nom : * GINF2

Priorité : * 1

Appliquer la longueur minimale du mot de passe

Longueur minimale du mot de passe (caractères) : * 1

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 :

Options d'âge du mot de passe :

Appliquer l'âge minimal de mot de passe

L'utilisateur ne peut pas changer le mot de passe d'i... * 1

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... * 5

Le compte va être verrouillé

Pendant une durée de (mins) : * 30

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

S'applique directement à

Nom Courrier

GINF2 users

Ajouter...

Supprimer

Informations supplémentaires...

OK Annuler

Références

<http://www.ahmedmalek.com/web/fr/doc.asp?docid=1493&mcat=4&mrub=41&msrub=63>

[http://technet.microsoft.com/fr-fr/library/bb643109\(EXCHG.80\).aspx](http://technet.microsoft.com/fr-fr/library/bb643109(EXCHG.80).aspx)

<http://blog.le-pi.com/?p=683>

<http://blog.portail-mcse.net/index.php?post/2008/05/18/Active-Direrctory-2008-%3A-configurer-plusieurs-strategies-de-mot-de-passe2>

<http://www.ahmedmalek.com/web/fr/home.asp>