



Didacticiel :

Stratégies de mot de passe affinées

Département Mathématiques & Informatique

Table des matières

Introduction
Pré requis à la création de Stratégie de mot de passe affinée2
Fonctionnement technique
Classe Password Settings Container (PSC) : msDS-PasswordSettingsContainer
Classe Password Settings Object : msDS-PasswordSettings7
Le tableau ci-dessous énumère les différentes valeurs d'attribut à renseigner tout au long de la création de l'objet PSO :
Procédure d'installation d'une stratégie de mot de passe affinée9
1. Création d'un objet PSO 10
2. Application des objets PSO aux utilisateurs et aux groupes de sécurité globaux
Création de la stratégie de mot de passe affinée en utilisant l'outil : Centre d'administration Active
Directory
Vérifier l'application de la stratégie de mot de passe affinée
Références ·

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".

		Exécuter	
		Entrez le nom d'un programme, dossier, document ou ressource Internet, et Windows l'ouvrira pour vous.	
	<u>O</u> uvrir :	regsvr32 schmmgmt.dll v	
		😵 Cette tâche sera créée avec les autorisations d'administrateur.	
		OK Annuler Parcourir	
Un message indiquera que	l'enre	egistrement de la DLL est un succès. V	/ali
		RegSvr32	
		DUD anisterConcerdance and some most dill of unci-	1

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).

		Console1 - [Racine de	la console]	_ _ X
	Fich	ier Action Affichage Favoris Fenêtre ?			_ <i>8</i> ×
4		Nouveau	Ctrl+N		
		Ouvrir	Ctrl+0		Actions
		Enregistrer	Ctrl+S	hs cet apercu.	Racine de la console
		Enregistrer sous			Autres actions
	_ L	Ajouter/Supprimer un composant logiciel enfichable	Ctrl+M		
		Options		-	
		1 C:\Windows\System32\gpme			
		2 C:\Windows\system32\HCSCFG			
		3 C:\Windows\system32\dsa			
		4 C:\Windows\system32\dnsmgmt			
		Quitter			
Qui	tte le	programme et confirme l'enregistrement des documents.			

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 apparaitre.

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

Vous pouvez sélectionner des co composants logiciels enfichables	extensibles, vous pouv	hables parn ez spécifier	ni ceux disponibles sur votre ordinateur quelles extensions doivent être activé	r, et les configurer. Pour les es.
Composants logiciels enfichables	disponibles :	c	Composants logiciels enfi. sélectionnés	:
Composant logiciel enfichable	Fournisseur A	[Racine de la console	Modifier les extensions
Planificateur de tâches	Microsoft Co			
🚊 Routage et accès distant	Microsoft C			Supprimer
Sauvegarde locale	Microsoft Co			
Sauvegarde Windows Serve	er Microsoft C			Monter
Serveur NPS (Network Poli	Microsoft C			Descendre
Services	Microsoft Co Aj	jouter >		Debeenare
Services de composants	Microsoft C			
Sites et services Active Dir.	Microsoft C			
😽 Téléphonie	Microsoft C			
Utilisateurs et groupes loc	. Microsoft C			
Utilisateurs et ordinateurs .	Microsoft C			
<	>			Avancé
		L		
Ajout	ter ou supprimer	r des co nables parm	mposants logiciels enficha	ables eur, et les configurer. Pour le
Ajout ls pouvez sélectionner des comp aposants logiciels enfichables ex	ter ou supprimer posants logiciels enfich ttensibles, vous pouve	r des co ables parm z spécifier	mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act	ables eur, et les configurer. Pour le ivées.
Ajout is pouvez sélectionner des comp posants logiciels enfichables ex iposants logiciels enfichables dis	ter ou supprimer posants logiciels enfich ttensibles, vous pouve sponibles :	r des co hables parm zz spécifier	mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act composants logiciels enfi. sélectionn	ables ieur, et les configurer. Pour le ivées. iés :
Ajout s pouvez sélectionner des comp posants logiciels enfichables ex posants logiciels enfichables dis mposant logiciel enfichable	ter ou supprimer posants logiciels enfich ttensibles, vous pouve sponibles : Fournisseur	r des co hables parm z spécifier	mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act Composants logiciels enfi. sélectionn acine de la console	ables eur, et les configurer. Pour le ivées. lés : Modifier les extensions
Ajout s pouvez sélectionner des comp posants logiciels enfichables ex posants logiciels enfichables dis mposant logiciel enfichable Planificateur de tâches	ter ou supprimer posants logiciels enfich ttensibles, vous pouve sponibles : Fournisseur ^ Microsoft C	r des co nables parm zz spécifier	mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act Composants logiciels enfi. sélectionn Racine de la console Schéma Active Directory	ables ieur, et les configurer. Pour le ivées. lés : Modifier les extensions
Ajout s pouvez sélectionner des comp posants logiciels enfichables ex posants logiciels enfichables dis mposant logiciel enfichable Planificateur de tâches Routage et accès distant	ter ou supprimer posants logiciels enfich tensibles, vous pouve sponibles : Fournisseur ^ Microsoft C Microsoft C	r des co hables parm z spécifier	mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act Composants logiciels enfi. sélectionn Racine de la console Schéma Active Directory	ables eur, et les configurer. Pour le ivées. lés : Modifier les extensions Supprimer
Ajout s pouvez sélectionner des comp posants logiciels enfichables ex posants logiciels enfichables dis mposant logiciel enfichable Planificateur de tâches Routage et accès distant Sauvegarde locale	ter ou supprime osants logiciels enfich ttensibles, vous pouve sponibles : Fournisseur ^ Microsoft C Microsoft C Microsoft C	r des co nables parm 22 spécifier (mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act Composants logiciels enfi. sélectionn Racine de la console Schéma Active Directory	ables eur, et les configurer. Pour le ivées. lés : Modifier les extensions
Ajout s pouvez sélectionner des comp posants logiciels enfichables ex posants logiciels enfichables dis mposant logiciel enfichable Planificateur de tâches Routage et accès distant Sauvegarde locale Sauvegarde Windows Server	ter ou supprime ossants logiciels enfich ttensibles, vous pouve sponibles : Fournisseur ^ Microsoft C Microsoft C Microsoft C Microsoft C	r des co nables parm 22 spécifier (mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act Composants logiciels enfi. sélectionn Racine de la console Schéma Active Directory	ables eur, et les configurer. Pour le ivées. hés : Modifier les extensions Supprimer Monter
Ajout s pouvez sélectionner des comp posants logiciels enfichables ex posants logiciels enfichables dis mposant logiciel enfichable Planificateur de tâches Routage et accès distant Sauvegarde locale Sauvegarde Windows Server Schéma Active Directory	ter ou supprime oosants logiciels enfich ttensibles, vous pouve sponibles : Fournisseur ^ Microsoft C Microsoft C Microsoft C Microsoft C Microsoft C	r des co hables parm z spécifier c	mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act Composants logiciels enfi. sélectionn and Racine de la console Schéma Active Directory	ables eur, et les configurer. Pour le ivées. Modifier les extensions Supprimer Monter
Ajout s pouvez sélectionner des comp posants logiciels enfichables ex mposant logiciel enfichables dis mposant logiciel enfichable Planificateur de tâches Routage et accès distant Sauvegarde locale Sauvegarde locale Sauvegarde Windows Server Schéma Active Directory Service	ter ou supprimer oosants logiciels enfich ttensibles, vous pouve sponibles : Fournisseur ^ Microsoft C Microsoft C Microsoft C Microsoft C Microsoft C Microsoft C Microsoft C Microsoft C Microsoft C	r des co hables parm z spécifier (mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act Composants logiciels enfi. sélectionn and Racine de la console Schéma Active Directory	ables reur, et les configurer. Pour le ivées. Modifier les extensions Supprimer Monter Descendre
Ajout s pouvez sélectionner des comp posants logiciels enfichables ex posants logiciel enfichables dis mposant logiciel enfichable Planificateur de tâches Routage et accès distant Sauvegarde locale Sauvegarde locale Sauvegarde Windows Server Schéma Active Directory Serveur NPS (Network Poli Services	ter ou supprimer bosants logiciels enfich tensibles; vous pouve sponibles : Fournisseur ^ Microsoft C Microsoft C Microsoft C Microsoft C Microsoft C Microsoft C Microsoft C	n des con hables parm z spécifier con puter >	mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act Composants logiciels enfi. sélectionn Racine de la console Schéma Active Directory	ables ivées. ivées. Modifier les extensions Supprimer Monter Descendre
Ajout s pouvez sélectionner des comp posants logiciels enfichables ex posants logiciel enfichables dis mposant logiciel enfichable Planificateur de tâches Routage et accès distant Sauvegarde locale Sauvegarde locale Sauvegarde Windows Server Schéma Active Directory Serveur NPS (Network Poli Services Services de composants Sites et services Active Dir	ter ou supprimer posants logiciels enfich tensibles ; vous pouve sponibles : Fournisseur ^ Microsoft C Microsoft C Microsoft C Microsoft C Microsoft C Microsoft C	n des con hables parm z spécifier	mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act Composants logiciels enfi. sélectionn Racine de la console Schéma Active Directory	ables reur, et les configurer. Pour le ivées. Modifier les extensions Supprimer Monter Descendre
Ajout s pouvez sélectionner des comp posants logiciels enfichables ex posants logiciel enfichables dis mposant logiciel enfichable Planificateur de tâches Routage et accès distant Sauvegarde locale Sauvegarde locale Sauvegarde Windows Server Schéma Active Directory Serveur NPS (Network Poli Services Services de composants Sites et services Active Dir Téléphonie	ter ou supprimer bosants logiciels enfich tensibles, vous pouve sponibles : Fournisseur ^ Microsoft C Microsoft C Microsoft C Microsoft C Microsoft C Microsoft C Microsoft C Microsoft C	n des con hables parm z spécifier control (buter >	mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act Composants logiciels enfi. sélectionn Racine de la console Schéma Active Directory	ables eur, et les configurer. Pour le ivées. Modifier les extensions Supprimer Monter Descendre
Ajout s pouvez sélectionner des comp posants logiciels enfichables ex posants logiciel enfichables dis mposant logiciel enfichable Planificateur de tâches Routage et accès distant Sauvegarde locale Sauvegarde locale Sauvegarde Windows Server Schéma Active Directory Services Services de composants Sites et services Active Dir Sites et services Active Dir Téléphonie Utilisateurs et groupes loc	ter ou supprimer bosants logiciels enfich tensibles, vous pouve sponibles : Fournisseur ^ Microsoft C Microsoft C	n des co hables parm z spécifier co buter >	mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act Composants logiciels enfi. sélectionn Racine de la console Schéma Active Directory	ables reur, et les configurer. Pour le ivées. Modifier les extensions Supprimer Monter Descendre
Ajout s pouvez sélectionner des comp posants logiciels enfichables ex posants logiciel enfichables dis mposant logiciel enfichable Planificateur de tâches Routage et accès distant Sauvegarde Vindows Server Schéma Active Directory Services de composants Sites et services Active Dir Services de composants Sites et services Active Dir Téléphonie Utilisateurs et groupes loc Utilisateurs et ordinateurs	ter ou supprimer bosants logiciels enfich trensibles, vous pouve sponibles : Fournisseur ^ Microsoft C Microsoft C	r des co hables parm z spécifier c	mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act Composants logiciels enfi. sélectionn Racine de la console Schéma Active Directory	ables ieur, et les configurer. Pour le ivées. iés : Modifier les extension Supprimer Monter Descendre
Ajout s pouvez sélectionner des comp posants logiciels enfichables ex posants logiciels enfichables dis mposant logiciel enfichable Planificateur de tâches Routage et accès distant Sauvegarde Vindows Server Schéma Active Directory Serveur NPS (Network Poli Services de composants Sites et services Active Dir Téléphonie Utilisateurs et groupes loc Utilisateurs et ordinateurs	ter ou supprimer bosants logiciels enfich trensibles, vous pouve sponibles : Fournisseur ^ Microsoft C Microsoft C	r des co hables parm z spécifier (nuter >	mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act Composants logiciels enfi. sélectionn Racine de la console Schéma Active Directory	ables eur, et les configurer. Pour le ivées. lés : Modifier les extension: Supprimer Monter Descendre
Ajout s pouvez sélectionner des comp posants logiciels enfichables ex posants logiciels enfichables dis mposant logiciel enfichable Planificateur de tâches Routage et accès distant Sauvegarde locale Sauvegarde Windows Server Schéma Active Directory Services de composants Sites et services Active Dir Services Sites et services Active Dir Téléphonie Utilisateurs et groupes loc Utilisateurs et ordinateurs	ter ou supprimer bosants logiciels enfich trensibles : Fournisseur ^ Microsoft C Microsoft C	n des co hables parm z spécifier (nuter >	mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act Composants logiciels enfi. sélectionn Racine de la console Schéma Active Directory	ables eur, et les configurer. Pour le ivées. lés : Modifier les extension: Supprimer Monter Descendre Avancé
Ajout s pouvez sélectionner des comp posants logiciels enfichables ex posants logiciels enfichables dis mposant logiciel enfichable)Planificateur de tâches Routage et accès distant)Sauvegarde Uindows Server Schéma Active Directory Serveur NPS (Network Poli Services de composants Sites et services Active Dir ?Téléphonie Utilisateurs et groupes loc Utilisateurs et ordinateurs	ter ou supprimer posants logiciels enfich trensibles : Fournisseur ^ Microsoft C Microsoft C	n des co hables parm z spécifier outer >	mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act Composants logiciels enfi. sélectionn Racine de la console Schéma Active Directory	ables eur, et les configurer. Pour le ivées.
Ajout s pouvez sélectionner des comp posants logiciels enfichables ex posants logiciels enfichables dis mposant logiciel enfichable)Planificateur de tâches Routage et accès distant Sauvegarde locale Sauvegarde Windows Server Schéma Active Directory Services de composants Sites et services Active Dir Services Services de composants Sites et services Active Dir Téléphonie Utilisateurs et groupes loc Utilisateurs et ordinateurs	ter ou supprime ossants logiciels enfich tensibles, vous pouve sponibles : Fournisseur ^ Microsoft C Microsoft C Mi	n des co hables parm z spécifier outer >	mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act Composants logiciels enfi. sélectionn Racine de la console Schéma Active Directory	ables eur, et les configurer. Pour le ivées.
Ajout s pouvez sélectionner des comp posants logiciels enfichables ex posants logiciels enfichables dis mposant logiciel enfichable (Planificateur de tâches Routage et accès distant Sauvegarde locale Sauvegarde Windows Server Schéma Active Directory Services de composants Sites et services Active Dir Services Services de composants Sites et services Active Dir Téléphonie Utilisateurs et groupes loc Utilisateurs et ordinateurs	ter ou supprime ossants logiciels enfich trensibles, vous pouve sponibles : Fournisseur ^ Microsoft C Microsoft C M	r des co tables parm z spécifier outer >	mposants logiciels enficha ni ceux disponibles sur votre ordinat quelles extensions doivent être act Composants logiciels enfi. sélectionn Racine de la console Schéma Active Directory	ables eur, et les configurer. Pour le ivées.

L'apparence de la console est comme suit :

Console1 - [Racine de la	console\Schéma Activ	e Directory [srv2k12.	ensa	at.priv]\Classes] 💶 🗙
🚟 Fichier Action Affichage Favoris Fer	iêtre ?			_ & ×
🗢 🄿 🙍 🗊 🙆 🔝 🚺				
Racine de la console	Nom	Туре	^	Actions
⊿ Schéma Active Directory [srv2k12.ensat.p	[■] t¦account	Structurel	≡	
Classes	T aCSPolicy	Structurel		Classes
Attributs	aCSResourceLimits	Structurel		Autres actions
	T aCSSubnet	Structurel		
	t addressBookContainer	Structurel		
	T addressTemplate	Structurel		
	T applicationEntity	Structurel		
	applicationProcess	Structurel		
	T applicationSettings	Abstrait		
	T applicationSiteSettings	Abstrait		
	T applicationVersion	Structurel		
	T attributeSchema	Structurel		
	T bootableDevice	Auxiliaire		
	to builtinDomain	Structurel		
	CategoryRegistration	Structurel		
	CertificationAuthority	Type 88		
	ClassRegistration	Structurel		
	ClassSchema	Structurel		
	ClassStore	Structurel		
	ComConnectionPoint	Structurel		
	T; computer	Structurel	$\overline{}$	
< III >	<	>		
	·			

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 :

Utilisateurs et o	rdinateurs Active Directory	_ □	x	
Fichier Action Affichage ?				
← ⇒ 2 🖬 ¼ 🗉 🗙 🖻 🖬 🖬 🖏 🗞 1	bi 🝸 🗾 🐍			
Utilisateurs et ordinateurs Active Directory [srv2k12.ensat.priv] ▶ ■ ■ ensat.priv ▶ ■ ■ ensat.priv ▶ ■ ■ Builtin ▶ ■ ■ <td< th=""><th>Nom AdminSDHolder ComPartitions ComPartitions DomainUpdates P Security Meetings MicrosoftDNS Policies RAS and IAS Servers Access Check WinsockServices WMIPolicy Default Domain Policy DFSR-GlobalSettings File Replication Service</th><th>Type Conteneur Conteneur Conteneur Conteneur Conteneur Conteneur Conteneur Conteneur Conteneur Conteneur Stratégie de domaine dfsConfiguration msDFSR-GlobalSettings Paramètres FRS</th><th></th><th></th></td<>	Nom AdminSDHolder ComPartitions ComPartitions DomainUpdates P Security Meetings MicrosoftDNS Policies RAS and IAS Servers Access Check WinsockServices WMIPolicy Default Domain Policy DFSR-GlobalSettings File Replication Service	Type Conteneur Conteneur Conteneur Conteneur Conteneur Conteneur Conteneur Conteneur Conteneur Conteneur Stratégie de domaine dfsConfiguration msDFSR-GlobalSettings Paramètres FRS		
Policies Policies RAS and IAS Servers Access Check WinsockServices WinIPolicy MiPolicy MiPolicy	Password Settings Container PSPs RpcServices BCKUPKEY_213f725e-53ef-4506-bf III	msDS-PasswordSettingsContainer msImaging-PSPs Services RPC secret	~	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 :

📓 Console1 - [Racine de la console\Schéma Active Directory [srv2k12.ensat.priv]\Classes\msDS 🗖 💌	Utilisateurs et ordinateurs Active Directory
🚡 Fichier Action Affichage Favoris Fenêtre ?	Fichier Action Affichage ?
	(+ +) 2 📰 🗄 🖾 Q 😖 🛛 🗊 🖏 💥 🍸 💆 🍇
*** msDS-ClaimType ^ Nom Type ^ Actions *** msDS-ClaimTypePropertyBase ^ Nom Facultatif msDS-PropertyBase ^ MsDS-PasswordStitopLength Obligatoire Obligatoire MsDS-PasswordStitopLength Obligatoire MsDS-PasswordStitopLength Autres acti > *** msDS-DeviceRegistrationServic * msDS-DeviceRegistrationServic * msDS-DeviceRegistrationServic * MsDS-DeviceRegistrationServic * MsDS-DeviceRegistrationServic * msDS-LockoutDhreshold Obligatoire Vires acti > Autres acti > *** msDS-DeviceRegistrationServic * msDS-LockoutDhreshold Obligatoire Vires acti > Autres acti > *** msDS-DeviceRegistrationServic * msDS-LockoutDhreshold Obligatoire Vires acti > Autres acti > *** msDS-ManagedServiceAccour * msDS-ManimumPasswordAge Obligatoire Vires acti > *** msDS-QuotaContainer * * msDS-MaximumPasswordAge Obligatoire Vires acti > *** msDS-ResourcePropertyList * msDS-ResourcePropertyList * msDS-TDOIngressBL Facultatif *** msDS-ResourcePropertyList * <td< td=""><td>▶ Managed Service Accounts ▶ Managed Service Accounts ▶ Program Data ▲ System ▶ ComPartitions ▶ ComPartitionsets ▶ DomainUpdates ▶ IP Security ▶ Metrings ▶ Metrings ▶ MorrisotRDNS ▶ Policies ▶ Default Domain Policy ▶ DFSA-ColobalSettings ▶ File Replication Service ▶ File Replication Service ▶ File Replication Service ▶ File Replication Service ▶ File Replications Service ▶ RpcServices</td></td<>	▶ Managed Service Accounts ▶ Managed Service Accounts ▶ Program Data ▲ System ▶ ComPartitions ▶ ComPartitionsets ▶ DomainUpdates ▶ IP Security ▶ Metrings ▶ Metrings ▶ MorrisotRDNS ▶ Policies ▶ Default Domain Policy ▶ DFSA-ColobalSettings ▶ File Replication Service ▶ File Replication Service ▶ File Replication Service ▶ File Replication Service ▶ File Replications Service ▶ RpcServices

sole1 - [Racine de la console\Schéma Activ	e Directory [DCserveur.dom2008.loc]\Classes	\msDS-Passv	wordSettir	ngs]		
t msDS-AzScope	Nom	Type	Système	Description		
t msDS-AzTask	msDS-PSOAppliesTo	Facultatif	Oui	Links to objects that this password settings object applies to		
msDS-ManagedServiceAccount	msDS-PasswordHistoryLength	Obligatoire	Oui	Password History Length for user accounts		
t ^a msDS-OptionalFeature	msDS-PasswordSettingsPrecedence	Obligatoire	Oui	Password Settings Precedence		
T ^a msDS-PasswordSettings	msDS-PasswordReversibleEncryptionEnable	d Obligatoire	Oui	Password reversible encryption status for user accounts		
t msDS-PasswordSettingsContainer	msDS-LockoutThreshold	Obligatoire	Oui	Lockout threshold for lockout of user accounts		
msDS-QuotaContainer	msDS-LockoutDuration	Obligatoire	Oui	Lockout duration for locked out user accounts		
C msDS-QuotaControl	MsDS-LockoutObservationWindow	Obligatoire	Oui	Observation Window for lockout of user accounts		
C msExchConfigurationContainer	msDS-PasswordComplexityEnabled	Obligatoire	Oui	Password complexity status for user accounts		
- C msFvE-RecoveryInformation	msDS-MinimumPasswordLength	Obligatoire	Oui	Minimum Password Length for user accounts		
T msteeeou211+Policy	msDS-MinimumPasswordAge	Obligatoire	Oui	Minimum Password Age for user accounts		
T msImaging-PSRs	msDS-MaximumPasswordAge	Obligatoire	Oui	Maximum Password Age for user accounts		
T mSMOConfiguration	msDS-EnabledFeatureBL	Facultatif	Oui	Scopes where this optional feature is enabled.		
T" msMO-Custom-Recipient	msDS-LastKnownRDN	Facultatif	Oui	Holds original RDN of a deleted object.		
T mSMOEnterpriseSettings	msDS-HostServiceAccountBL	Facultatif	Oui	Service Accounts Back Link for linking machines associated with the service account.		
T msMO-Group	msDS-OIDToGroupLinkBl	Facultatif	Oui	Backlink for ms-DS-OIDToGroup-Link; identifies the issuance policy, represented by an OID object, which is		
mSMOMigratedUser	msDS-LocalEffectiveRecycleTime	Facultatif	Oui	Recycle time of the object in the local DIT.		
mSMQQueue	msDS-LocalEffectiveDeletionTime	Facultatif	Oui	Deletion time of the object in the local DIT.		
mSMQSettings	msDS-PSOApplied	Facultatif	Qui	Password settings object applied to this object		
T mSMQSiteLink	msDS-NcType	Facultatif	Qui	A bit field that maintains information about aspects of a NC replica that are relevant to replication.		
ms-net-ieee-80211-GroupPolicy	msDS-PrincipalName	Facultatif	Qui	Account name for the security principal (constructed)		
ms-net-ieee-8023-GroupPolicy	msDS-Revealed istBl	Facultatif	Oui	backlink attribute for ms-DS-Revealed-List.		
msPKI-Enterprise-Oid	msDS-NC-RO-Replica-Locations-BL	Facultatif	Oui	backlink attribute for ms-DS-NC-RO-Renlica-Locations.		
msPKI-Key-Recovery-Agent	msDS-AuthenticatedToAccountlist	Facultatif	Oui	Backlink for ms-DS-AuthenticatedAt-DC: for a Computer, identifies which users have authenticated to this		
T msPKI-PrivateKeyRecoveryAgent	msDS-IsPartialReplicaFor	Facultatif	Oui	Backlink for has-Partial-Replica-NCs; for a partition root object, identifies which Directory instances (DSA) b		
T msPrint-ConnectionPolicy	meDS-IcDomainEor	Facultatif	Oui	Backlink for meDS-Hae-Domain-NCe; for a partition root object, identifies which Directory instances (DSA) i		
T msSFU30DomainInfo	msDS-IsEulRenicaEor	Facultatif	Oui	Backlink for ms-Ds-Has-Full-Renlica-NCs: for a partition root object, identifies which Directory instances (DSA)		
msSFU30MailAliases	T mcDS-RevealedDSAs	Facultatif	0	Backlink for ms-DS-Revealed J loers: for a user, identifies which Directory instances (DSA) hold that user's s		
TT msSEU3UNETIG		, ocalitatul	00	busine for the bol revealed overag for a data procedures which billectory instances (boxy) for a data procedure size		

Classe Password Settings Object : msDS-PasswordSettings

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.

🖀 Console1 - [Racine de la conso	le\Schéma Active Directory [srv2k12.ens	at.priv]\Cla	sses\msDS-	PasswordSettings]	_ D X
藩 Fichier Action Affichage Favoris Fe	nêtre ?				_ & ×
🗢 🏟 🖄 📰 🖾 🗟 🖬					
T msDS-ClaimType	Nom	Туре	Système	Description ^	Actions
T msDS-ClaimTypePropertyBase	🛃 msDS-PSOAppliesTo	Facultatif	Oui	Links to objects tha	msDS-Pass
T msDS-ClaimTypes	🛃 msDS-PasswordHistoryLength	Obligatoire	Oui	Password History L∈ ≡	A described in the second seco
T msDS-CloudExtensions	MsDS-PasswordSettingsPrecedence	Obligatoire	Oui	Password Settings P	Autres acti 🕨
T msDS-Device	Kan Schemen Scheme Sche	Obligatoire	Oui	Password reversible	
T msDS-DeviceContainer	🛃 msDS-LockoutThreshold	Obligatoire	Oui	Lockout threshold f	
T msDS-DeviceRegistrationServic	🛃 msDS-LockoutDuration	Obligatoire	Oui	Lockout duration fc	
msDS-DeviceRegistrationServic	🛃 msDS-LockoutObservationWindow	Obligatoire	Oui	Observation Windo	
-L msDS-GroupivianagedServiceA	Main Market Ma	Obligatoire	Oui	Password complexit	
T msDS OntionalEasture	🛃 msDS-MinimumPasswordLength	Obligatoire	Oui	Minimum Password	
T" msDS-PasswordSettings -	🛃 msDS-MinimumPasswordAge	Obligatoire	Oui	Minimum Password	
T" msDS-PasswordSettingsContai	🛃 msDS-MaximumPasswordAge	Obligatoire	Oui	Maximum Password	
T msDS-OuotaContainer	🛃 msDS-ReplValueMetaDataExt	Facultatif	Oui	ms-DS-Repl-Value-	
T msDS-OuotaControl	🛃 msDS-parentdistname	Facultatif	Oui	ms-DS-Parent-Dist-	
T msDS-ResourceProperties	🛃 msds-memberTransitive	Facultatif	Oui	msds-memberTran	
T msDS-ResourceProperty	🛃 msds-memberOfTransitive	Facultatif	Oui	msds-memberOfTr	
T msDS-ResourcePropertyList	🛃 msDS-TDOEgressBL	Facultatif	Oui	Backlink to TDO Egi	
T msDS-ValueType	🛃 msDS-TDOIngressBL	Facultatif	Oui	Backlink to TDO Ing	
T ^a msExchConfigurationContaine	🛃 msDS-ValueTypeReferenceBL	Facultatif	Oui	This is the back link	
■ [™] t ^a msFVE-RecoveryInformation	🛃 msDS-IsPrimaryComputerFor	Facultatif	Oui	Backlink atribute fo	
T msieee80211-Policy	Z msDS-ClaimSharesPossibleValuesWithBL	Facultatif	Oui	For a claim type obj	
T msImaging-PostScanProcess	MsDS-MembersOfResourcePropertyListBL	Facultatif	Oui	Backlink for ms-DS	
Comparing and an intermediate and a second and a sec	<			>	
	L •				,

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- PasswordReversibleEncryptionEna bled	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	 (Aucune) De 00:00:00:00 à la valeur msDS- MaximumPassw ordAge 	1:00:00:00 (1 jour)

msDS-MaximumPasswordAge	Durée de vie maximale du mot de passe pour les comptes d'utilisateurs	 (Jamais) De la valeur msDS- MinimumPassw ordAge à (Jamais) La valeur de msDS- MaximumPassw ordAge 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	 (Aucune) De 00:00:00:01 à la valeur msDS- LockoutDuratio n 	0:00:30:00 (30 minutes)
msDS-LockoutDuration	Durée de verrouillage pour les comptes d'utilisateurs verrouillés	 (Aucune) (Jamais) De la valeur msDS- LockoutObserva tionWindow 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=conto so,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

				Modification ADSI		_ 🗆 X
Fichier	Action	h Affichage	?			
<	C	Connexion				
📝 Modi	A	ctualiser			Actions	
	A	lide		Éditeur ADSI	Modification ADSI	•
				L'Éditeur ADSI (Active Directory Services Interfaces) est un éditeur de bas niveau pour les services de domaine Active Directory et les services AD LDS (Active Directory Lightweight Directory Services). Il vous permet d'afficher, de modifier, de créer et de supprimer un objet dans les services de domaine Active Directory ou les services AD LDS (Active Directory Lightweight Directory Services) de Microsoft. Pour créer une connexion vers ces services, dans le menu Action, cliquez sur Connexion.	Autres actions	•
Affiche l'ai	fiche l'aide pour l'élément sélectionné.					

	Modification ADSI		x
Fichier Action Affichage ?	Paramètres de connexion	[
Modification ADSI	Nom : Contexte d'attribution de noms par défaut Chemin d'accès : LDAP://srv2k12.ensat.priv/Contexte d'attribution de nom Point de connexion Sélectionnez ou entrez un nom unique ou un contexte d'attribution de noms : Sélectionnez ou entrez un nom unique ou un contexte d'attribution de noms : v Sélectionnez un contexte d'attribution de noms connu : v Ordinateur Sélectionnez ou entrez un domaine ou un serveur : (Serveur Domaine [:port])	cation ADSI es actions	•
	Par défaut (le domaine ou le serveur auquel vous vous êtes connecté) Utiliser le chiffrement SSL OK Annuler		

2	Modification ADSI				_ 🗆 X
Fichier Action Affichage ? Image: State of the stat	Nom CN=AdminSDHolder CN=ComPartitions	Classe container container	Nom unique CN=AdminSDHolder, CN=System, DC=ense CN=ComPartitions, CN=System, DC=ensat, CN=ComPartitions for CN=System, DC=ensat,	^	Actions CN=Syst ▲ Autre ▶
 CN=Computers OU=Domain Controllers CN=ForeignSecurityPrincipals CN=LostAndFound CN=Managed Service Accounts CN=NTDS Quotas CN=Program Data CN=Frogram Data OU=Test CN=USers 	CN= Contraction Policy CN=Default Domain Policy CN=Dfs-Configuration CN=DFSR-GlobalSettings CN=File Replication Service CN=FileReplication Service CN=FileLinks CN=IP Security CN=Meetings CN=Meetings CN=Possword Settings Con CN=Policies CN=PSPs	domainPolicy dfsConfigura msDFSR-Glo container nTFRSSettings fileLinkTrack container container container msDS-Passw container msDmainer	CN=Default Domain Policy, CN=System, DC=Ent CN=Default Domain Policy, CN=System, DC CN=Dfs-Configuration, CN=System, DC=ens CN=DF8-GlobalSettings, CN=System, DC= CN=DomainUpdates, CN=System, DC=ensat, DC=p CN=FileLinks, CN=System, DC=ensat, DC=p CN=IP Security, CN=System, DC=ensat, DC=p CN=Meetings, CN=System, DC=ensat, DC=p CN=MicrosoftDNS, CN=System, DC=ensat, C CN=Password Settings Container, CN=Syste CN=Policies, CN=System, DC=ensat, DC=pri CN=PSPs CN=System, DC=ensat, DC=pri	=	
	CN=RAS and IAS Servers Ac	container	CN=RAS and IAS Servers Access Check,CN:	~	

Interface de l'outil de modification ADSI

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

	n ADSI			Ľ		
Fichier Action Affichage ?						
🗢 🏟 🙍 📰 💥 🗐 🧔 😹 🛛 🗊						
⊿ 📋 CN=System	Déplacer		Classe	Nom unique		Actions
CN=AdminSDHolder	Nouvelle connexion à partir d'ici	Aucun élér	ment à afficher dan	ıs cet aperçu.		CN=Pas 🔺
CN=ComPartitionSets	Nouveau 🔸	Objet				Autre 🕨
CN=Default Domain Policy	Affichage +					
CN=Dfs-Configuration	Supprimer					
CN=DomainUpdates	Renommer					
CN=File Replication Service	Actualiser					
CN=FileLinks	Exporter la liste					
CN=IP Security						
CN=Meetings	Propriétés					
CN=MicrosoftDNS	Aide					
CN=Password Settings Contains						
CN=Policies						
CN=PSPs						
CN=RAS and IAS Servers Access	Check					
CN=RpcServices						
CN=WinsockServices	× <	Ш			>	
rée un nouvel élément dans ce conteneur.						

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

Sélectionnez msDS-PasswordSettings et cliquez sur Suivant :

Créer un objet
Sélectionnez une dasse :
< Précédent Suivant > Annuler Aide

Interface de création d'un objet PSO

	Créer un objet 🛛 🗙
Attribut :	cn .
Syntaxe :	Chaîne Unicode
Description :	Common-Name
Valeur :	
	< Précédent Suivant > Annuler Aide

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
	<pre>verte suivant > Annuler Alde</pre>

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-PasswordReversibleEncrytionEnabled en remplissant le champ Valeur

	Créer un objet
Attribut :	msDS-PasswordReversibleEncryptionEnabled
Syntaxe :	Booléen
Description :	Password reversible encryption status for user accounts
Valeur :	
	< Précédent Suivant > Annuler Aide

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

		Créer un objet
Attrib	out :	msDS-PasswordReversibleEncryptionEnabled
Synta	axe :	Booléen
Descr	ription :	Password reversible encryption status for user accounts
Valeu	ir :	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-PasswordHistoryl enath
Syntaxe :	Entier
Description :	Password History Length for user accounts
Valeur :	
	Defendent Outure Annular Aide
	Annuer Alde

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.

	Créer un objet
Attribut :	msDS-PasswordHistoryLength
Syntaxe :	Entier
Description :	Password History Length for user accounts
Valeur :	3
	< Précédent Suivant > Annuler 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

	Créer un objet 🛛 🗙
Attribut :	msDS-PasswordComplexityEnabled
Syntaxe :	Booléen
Description :	Password complexity status for user accounts
Valeur :	
	<précédent suivant=""> Annuler Aide</précédent>

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
	< 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 :	4
	< 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 :	
-		
		< Precedent 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 :	00:00:00:00
	< 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 :	1
	< Précédent Suivant > Annuler Aide

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

	Créer un objet	x
Attribut :	msDS-MaximumPasswordAge	
Syntaxe :	Durée	
Description :	Maximum Password Age for user accounts	
Valeur :	00:30:00:00	
	< Précédent Suivant > Annuler Aide	
	Créer un objet	x
Attribut :	msDS-MaximumPasswordAge	_

Attribut :	msDS-MaximumPasswordAge
Syntaxe :	Durée
Description :	Maximum Password Age for user accounts
valeur :	00:00:30:00
	< Précédent Suivant > Annuler Aide

	Créer un objet
Attribut :	msDS-MaximumPasswordAge
Syntaxe :	Durée
Description :	Maximum Password Age for user accounts
Valeur :	00:00:00
	< 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 :	3
	< 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

	Créer un objet
Attribut :	msDS-LockoutObservationWindow
Syntaxe :	Durée
Description :	Observation Window for lockout of user accounts
Valeur :	
	< Précédent Suivant > Annuler Aide

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

		Créer un objet
	Attribut :	msDS-LockoutObservationWindow
	Syntaxe :	Durée
	Description :	Observation Window for lockout of user accounts
	Valeur :	00:01:00:00
-		< Précédent Suivant > Annuler Aide

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 :	1
	< 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 :	01:00:00:00
	<pre>< Précédent Suivant > Annuler Aide</pre>

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

Créer un obj	et 🛛 🗙
Pour terminer la création de cet objet, cliquez sur	Terminer.
Pour définir d'autres attributs, cliquez sur Attributs supplémentaires.	Attributs supplémentaires
< Précédent Terminer	Annuler Aide

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* » :

Attributs	Cir-		
Chemin d'ac	cès :		
Classe :	msDS-Passw	ordSettings	
Sélectionnez afficher :	les propriétés à	Facultatif	¥
Sélectionne: afficher :	une propriété à	adminDescription	~
Valeurs d'att	ribut		
Syntaxe :	DirectoryString		
Modifier un attribut :			
Valeur(s) :	<non défini=""></non>		
		Définir Effac	er

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

—	nateurs Active Directory		- -	1 3	x
Fichier Action Affichage ? Image: Second Secon	nateurs Active Directory	Type Utilisateur Groupe de sécurité Groupe de sécurité Groupe de sécurité Groupe de sécurité Groupe de sécurité Groupe de sécurité Groupe de sécurité	- Unive - Unive - Globa - Globa - Globa - Unive - Globa - Doma - Globa	rsel I I I I I I I I I I I I I I I	×
	DisupdateProxy Section 2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.	Groupe de sécurité Groupe de sécurité Groupe de sécurité Utilisateur Groupe de sécurité Utilisateur Groupe de sécurité Groupe de sécurité Groupe de sécurité Groupe de sécurité	- Globa - Doma - Doma - Doma - Globa - Globa - Globa - Globa	I iine lo iine lo I I I I I	

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

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

	Utilisateurs et oro	dinateurs Active Directory		- 🗆 X
Fichier Action Affichage ?				
♦ ♦ 2 🖬 ¼ 🗎 🗙 🗐	a 🗟 👔 🖬 🕺	i 🔻 🗾 🍇		
 Utilisateurs et ordinateurs Active Dir Requêtes enregistrées Builtin Computers Domain Controllers ForeignSecurityPrincipals Test Users 	ectory [srv2k12.ensat.priv]	Nom Contrôleurs de domaine Propriétés de : PSO-UserPwd de de Géré par Dossier Services de domaine Active Directory ensat priv/Users III ter	Type Groupe de sécurité ? X	- Global lobal lobal lomaine loc lobal lomaine loc lobal
		OK Ann	uler Appliquer	

On réinitialise le mot de passe à 1234 :

Utilisateurs et	ordinateurs Active Directory
Utilisateurs et Fichier Action Affichage ? Image: Second Seco	ordinateurs Active Directory
	Compare de Securité - Global Compare de sécurité - Global Propriétaires créateurs de la straté Groupe de sécurité - Global Producted Users Groupe de sécurité - Global PSO-UserPwd Groupe de sécurité - Global C III Securité - Global Securité - Global

Mot de passe 1234



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



Propriétés de	e : CN=UserPwd ? ×			
Éditeur d'attributs Sécurité				
Attributs :				
Attribut	Valeur ^			
replPropertyMetaData	AttID Ver Loc.USN O			
msDS-MinimumPasswordAge	(aucun) =			
msDS-MaximumPasswordAge	0:00:30:00			
msDS-LockoutObservationWin	0:01:00:00			
dSCorePropagationData	0x0 = ()			
instanceType	0x4 = (WRITE)			
msDS-PasswordSettingsPreced	1			
msDS-LockoutDuration	1:00:00:00			
whenChanged	27/10/2014 02:40:43 GMT			
whenCreated	27/10/2014 02:40:43 GMT			
msDS-LockoutThreshold	3			
msDS-PasswordHistoryLength	3			
msDS-MinimumPasswordLength	4			
uSNChanged	73825			
<	> ·			
Modifier	Filtrer			
OK Anr	nuler Appliquer Aide			

Propriétés de	e : CN=UserPwd ? X		
Éditeur d'attributs Sécurité			
Attributs :			
Attribut	Valeur ^		
msDS-LockoutObservationWin	0:01:00:00		
msDS-LockoutThreshold	3		
msDS-MaximumPasswordAge	0:00:30:00		
msDS-MinimumPasswordAge	(aucun)		
msDS-MinimumPasswordLength	4		
msDS-NcType	<non défini=""></non>		
msDS-PasswordComplexityEna	FALSE		
msDS-PasswordHistoryLength	3		
msDS-PasswordReversibleEncr	FALSE		
msDS-PasswordSettingsPreced	1		
msDS-PSOAppliesTo	<non défini=""></non>		
name	UserPwd		
objectCategory	CN=ms-DS-Password-Settings,CN=		
objectClass	top; msDS-PasswordSettings 🗸		
<	>		
Modifier			
OK Anr	nuler Appliquer Aide		

Édit	eur à valeurs multiples de	noms uniques avec principaux de sécurité
Attribut : Valeurs :	msDS-PSOAppliesTo	
Nom	Conteneur	Nom unique / SID
Ajouter un cor	mpte Windows	Supprimer
Ajouter un	nom unique	
		OK Annuler

Sélectionnez des utilisateurs, des ordinateurs ou de	s groupes 🛛 🗙
Sélectionnez le type de cet objet :	
des utilisateurs, des ordinateurs, des groupes ou Principaux de sécurité intégrés	Types d'objets
À partir de cet emplacement :	
ensat.priv	Emplacements
E <u>n</u> trez les noms des objets à sélectionner (<u>exemples</u>) :	
PSO-UserPwd	Vérifier les noms
I	
Avancé 0)	K Annuler

Éditeu	ur à valeurs mu	ultiples de noms uniques avec principaux de sécurité
Attribut : Valeurs :	msDS-PSOApplies	ъто
Nom	Conteneur	Nom unique / SID
PSO-UserPwd	ENSAT	<sid=010500000000051500000827c65171824afd46a3f3e5352040000></sid=010500000000051500000827c65171824afd46a3f3e5352040000>
<		III >
Ajouter un compi	te Windows	Supprimer OK Annuler

Propriétés d diteur d'attributs Sécurité	e : CN=UserPwd ? X
Attributs :	
Attribut	Valeur ^
dSASignature	<non défini=""></non>
extensionName	<non défini=""></non>
flags	<non défini=""></non>
fSMORoleOwner	<non défini=""></non>
isCriticalSystemObject	<non défini=""></non>
isDeleted	<non défini=""></non>
isRecycled	<non défini=""></non>
last Known Parent	<non défini=""></non>
mS-DS-ConsistencyChildCount	<non défini=""></non>
mS-DS-ConsistencyGuid	<non défini=""></non>
msDS-LastKnownRDN	<non défini=""></non>
msDS-NcType	<non défini=""></non>
msDS-PSOAppliesTo	<sid=010500000000005150000< td=""></sid=010500000000005150000<>
objectVersion	<non défini=""></non>
<	>
Modifier	Filtrer
OK An	nuler Appliquer Aide

Utilisateurs et ordi	inateurs Act	ive Directory			x
Fichier Action Affichage ?					
🗢 🔿 🙍 🚮 🤾 📋 🗙 🖾 🧔 🕞 🔟 🖬 % % 🖆	1 🍸 🗾 🐍				
 Utilisateurs et ordinateurs Active Directory [srv2k12.ensat.priv] Requêtes enregistrées ensat.priv Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accounts Test Users 	Nom Administr Admini	ateur ateurs de l'entreprise ateurs du schéma u domaine urs de domaine clonables urs de domaine d'entrepri urs de domaine en lectur ns teeProxy le certificats e réplication dont le mot domaine Copier Ajouter à un groupe Désactiver le compte Désignet de la destactiver domaine	Type Utilisateur Groupe de s Groupe de s Utilisateur Groupe de s	écurité - Universel écurité - Global écurité - Domaine lo écurité - Domaine lo écurité - Domaine lo écurité - Global curité - Global curité - Global curité - Global	
	<	Déplacer		cunte - Global	>
Envoie un courrier à la sélection	_	Ouvrir la page de démarra	ge		

Utilisateurs et	ordinateurs Active Directory
Picher Action Affichage ? Image: State and Sta	A and a controller le compte au rec controller de domaine : Déverouiller le compte de l'utilisateur
	Compared a comment of the second of the

Mot de passe 1234

Utilisateurs et ordin	ateurs Active Directory		x
Fichier Action Affichage ?			
🗢 🔿 📶 🤏 📋 🗙 🖻 🖬 🕞 🖉 🖬 % 🗞 🛍	7 🧕 🔽		
Utilisateurs et ordinateurs Active Directory [srv2k12.ensat.priv] ▶ Requêtes enregistrées ▲ mensateurs ▶ Builtin ▶ Computers ▶ Computers ▶ ForeignSecurityPrincipals ▶ Managed Service Accounts ▶ Users	Nom Administrateur Administrateurs de l'entreprise Administrateurs du schéma Administrateurs du schéma Adminis du domaine Contrôleurs de domaine clonables Contrôleurs de domaine d'entrepri Contrôleurs de domaine en lectur Dosdröleurs Dosdupise DnsJupdateProxy	Type Utilisateur Groupe de sécurité - Universel Groupe de sécurité - Universel Groupe de sécurité - Global Groupe de sécurité - Global Groupe de sécurité - Universel Groupe de sécurité - Universel Groupe de sécurité - Donaine I Groupe de sécurité - Global	
Services de domaine Active Directory	x pe de réplication dont le mot	Groupe de sécurité - Domaine Groupe de sécurité - Domaine	oc loc
le mot de passe pour khalid AMECHNOUE a été changé.	pe de réplication dont le mot é és du domaine d AMECHNOUE	Groupe de sécurité - Domaine Utilisateur Groupe de sécurité - Global Utilisateur	oc
ОК	riétaires créateurs de la straté ected Users es rou-UserPwd	Groupe de sécurité - Global Groupe de sécurité - Global Groupe de sécurité - Global Groupe de sécurité - Global	~
			2







Mot de passe : azer



Si plusieurs PSOs 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 appliqué 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'un 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 évènements, 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.

Centre d administration Active Di	rectory			- 0 ^
Centre	d'administration Active Directory + ENSAT (local)) • System •		• 🗭 Gérer Aide
Centre d'adminis <	System (21)			Täches
E E			0	e l
We desception			·	Password Settings Container
The other development	Nom	Туре	Description	Nouveau •
Curture Curture	ComPartitions	Costeneur		 Supprimer
System	ComPartitionSets	Conteneur		Rechercher sous ce nœud
Osers	Default Domain Policy	Stratégie de domaine		Propriétés
Controle d'acces dynamique	Dfs-Configuration	dfsConfiguration		System ^
Authentification	DFSR-GlobalSettings	msDFSR-GlobalSettings		Nouveau
Authentication Policies	DomainUpdates	Conteneur		Supprimer
P Recherche globale	File Replication Service	Paramètres FRS		Rechercher sous ce nœud
	FileLinks	fileLinkTracking		Propriétés
	IP Security	Conteneur		
	Meetings 1	Conteneur		
	MicrosoftDNS	Conteneur		
	Password Settings Container	msDS-PasswordSettingsContainer		
	Policies	Conteneur		
	PSPs	msImaging-PSPs		
	RAS and IAS Servers Access Check	Conteneur		
	RID Manager\$	riDManager		
	RpcServices	Services RPC		
	Server	samServer		
	WinsockServices	Conteneur		
	WMIPolicy	Conteneur		~
	Password Settings Container		、 、	
	Classe d'objets : msDS-PasswordSettingsContainer		Modifié le : 10/10/2019 23:44	
	Description :			
	Résumé			
HISTORIQUE DE WINDOWS P	OWERSHELL			۲

Effectuez alors un clic-droit sur »Password Setting Container » et sélectionnez Nouveau enfin,

cliquez sur Paramètres mot de passe.

Centre	d'administration Active Directory + ENSAT (lo	ocal) • System •		
Centre d'adminis <	System (21)			
11 'Te	Filtrer			S
Vue d'ensemble				
ENSAT (local)	Nom	Туре	Description	
System	ComPartitions	Conteneur		\sim
Users	ComPartitionSets	Conteneur		÷
Contrôle d'accès dynamique 🕨	Default Domain Policy	Stratégie de domaine		
Authentification	Dfs-Configuration	dfsConfiguration		
Authentication Policies	DFSR-GlobalSettings	msDFSR-GlobalSettings		
Recharche globale	DomainUpdates	Conteneur		
- Necherche globale	File Replication Service	Paramètres FRS		
	FileLinks	fileLinkTracking		
	IP Security	Conteneur		
	Meetings 1	Conteneur		
	MicrosoftDNS	Conteneur		
	Password Settings Container	msDS-PasswordSettingsContaine		
	Policies	Nouveau >	Paramètres de mot de passe	
	PSPs PSPs	Supprimer		
	RAS and IAS Servers Access Check	Rechercher sous ce nœud		
	RID Manager\$	nomenager		
	RpcServices	Services RPC		
	Server	samServer		
	WinsockServices	Conteneur		
	WMIPolicy	Conteneur		Ų

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

Créer Paramètres d	de mot de passe :	- □ × TÂCHES ▼ SECTIONS ▼
Paramètres de mot de passe S'applique directement à	Paramètres de mot de passe 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 C 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 : S'applique directement à Nom Courrier	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 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 L'utilisateur doit changer le mot de passe L'utilisateur 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 ① Jusqu'à ce qu'un administrateur déverrouille <u>Ajouter Xioupprimer Ajouter Supprimer </u>
lnformations supplémenta		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 : GINE2	- □ ×
Paramètres de mot de passe S'applique directement à	Paramètres de mot de passe Nom :	 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
Informations supplémenta	S'applique directement à	⑦ ⊗ ⊙ Ajouter Supprimer

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

ouvel objet - Utilisa	ouvel objet - Utilisateur				
Créer dans	s : ENSAT.loc/ENSAT/GINF2				
Prénom :	Khalid Initiales :				
Nom :	Amechnoue				
Nom complet :	Khalid Amechnoue				
Nom d'ouverture de	session de l'utilisateur :				
kamechnoue	@ENSAT.loc ~				
Nom d'ouverture de	session de l'utilisateur (antérieur à Windows 2000) :				
ENSAT	kamechnoue				
	< Précédent Suivant > Ann	uler			

Utilisateurs et ordinateurs Active I	Directory				
Fichier Action Affichage ?					
🗢 🄿 🔁 📆 📋 🗐 🧔 🗉	è 🛛 🔽 👘	% 🐮 🍸 🗵 🗞			
 Utilisateurs et ordinateurs Active Requêtes enregistrées ENSAT.loc Builtin Computers Domain Controllers ForeignSecurityPrincipal: 	Nom			Type Utilisateur	Description
 Managed Service Accour Users ENSAT GINF2 		Délégation de contrôle Déplacer Rechercher			
		Nouveau	>	Ordinateur	
		Toutes les tâches	>	Contact	
		Actualiser Exporter la liste		Groupe InetOrgPerson msDS-ShadowPrincipalContainer msImaging-PSPs	
		Affichage	>		
		Réorganiser les icônes Aligner les icônes Propriétés	>	Alias de file d'attente MSMQ Unité d'organisation Imprimante	
		Aide		Utilisateur Dossier partagé	

Nouvel ob	ouvel objet - Groupe					
8	Créer dans :	ENSAT.loc/ENSAT/GINF2				
Nom du <u>c</u>	roupe :					
GINF2 u	isers					
Nom de c	noune (antérieur	à Windows 2000) ·				
GINF2 u	isers					
Étendu	e du groupe	Type de groupe				
ODon	naine local	Sécurité				
Glob	oale	ODistribution				
Univ	/erselle					
		OK Ann	uler			

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

GINF2		− □ × TÂCHES ▼ SECTIONS ▼
Paramètres de mot de passe S'applique directement à Extensions	Paramètres de mot de passe Nom : GINF2 Priorité : Appliquer la longueur minimale du mot de passe Longueur minimale du mot de passe (caractères) : Appliquer l'historique des mots de passe Nombre de mots de passe mots de passe Nombre de mots de passe en values 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 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
Informations supplémenta	S'applique directement à Nom Courrier GINF2 users	() (S) (S) Ajouter Supprimer

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

Centre d'administration Active Directory		- 6 ×
Centre d'administration Active	Directory + ENSAT (local) + System + Password Settings Container	• 🗭 Gérer Aide
Centre d'administration Active Directory	Password Settings Container (1)	Tâches
E 15		ē.
Wue d'ensemble		GINF2
ENSAT (local)	Nom Priorité Type Description	Supprimer
System\Password Settings Container	GINF2 1 Paramètres de mot de passe	Propriétés
Users		Password Settings Container
System		Nouveau •
Contrôle d'accès dynamique		Supprimer
Authentification		Rechercher sous ce nœud
Authentication Policies		Propriétés
μ καιτατίτα gooble	GNP2	
	Résumé	
HISTORIQUE DE WINDOWS POWERSHELL		(

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.

Membre (de Ré	plication de	mot de pass	se Appel	entrant	Obje	t S	écurité	
En	vironnement	t	Ses	sions		Contrôle	à distance	e	
Général Adresse Compte Profil Téléphones		Organi	sation	Certificate	s publiés	s			
Profil	des services	s Bureau à c	distance	COM	+	Édit	eur d'attrib	outs	
Attributs :									
Attribut		Valeu	r			^			
msDS-p	arentdistnar	ne <non< td=""><td>défini></td><td></td><td></td><td></td><td></td><td></td><td></td></non<>	défini>						
msDS-P	honeticCom	ip <non< td=""><td>défini></td><td></td><td></td><td></td><td></td><td></td><td></td></non<>	défini>						
msDS-P	honeticDep	ar <non< td=""><td>défini></td><td></td><td></td><td></td><td></td><td></td><td></td></non<>	défini>						
msDS-P	honeticDisp	la <non< td=""><td>défini></td><td></td><td></td><td></td><td></td><td></td><td></td></non<>	défini>						
msDS-P	honetic First	N <non< td=""><td>défini></td><td></td><td>^</td><td>fficher</td><td>iniqueme</td><td>ant les a</td><td>attributs avant des valeurs</td></non<>	défini>		^	fficher	iniqueme	ant les a	attributs avant des valeurs
msDS-P	honeticLast	N <non< td=""><td>défini></td><td></td><td></td><td>unicher e</td><td>inqueine</td><td>cite ies a</td><td>stributs ayant des valeurs</td></non<>	défini>			unicher e	inqueine	cite ies a	stributs ayant des valeurs
msDS-p	referredData	aL <non< td=""><td>défini></td><td></td><td>A</td><td>fficher u</td><td>iniqueme</td><td>ent les a</td><td>attributs accessibles en écriture</td></non<>	défini>		A	fficher u	iniqueme	ent les a	attributs accessibles en écriture
msDS-P	rimaryComp	uter <non< td=""><td>défini></td><td></td><td></td><td>fficherl</td><td>ar attribu</td><td>+c .</td><td></td></non<>	défini>			fficherl	ar attribu	+c .	
msDS-P	rincipalNam	e ENSA	T\kamechn	oue	A	meneri	es attribu	ts ;	
msDS-F	ReplAttribute	M <ds_< td=""><td>REPL_ATT</td><td>R_META_DAT</td><td>~</td><td>Obligat</td><td>oire</td><td></td><td></td></ds_<>	REPL_ATT	R_META_DAT	~	Obligat	oire		
msDS-F	ReplValueMe		défini>		~	Faculta	tif		
msDS-F	ReplValueMe	t <non< td=""><td>défini></td><td></td><td>_</td><td></td><td></td><td></td><td></td></non<>	défini>		_				
msDS-F	ResultantPS(D CN=G	INF2,CN=P	assword Setting	A	fficher l	es attribu	ts en leo	ecture seule :
msDS-F	RevealedList	BL <non< td=""><td>défini></td><td></td><td>~</td><td>Constru</td><td>uit</td><td></td><td></td></non<>	défini>		~	Constru	uit		
<					_	Liens p	récédent	s	
Affich	ier				\checkmark	Systèm	e-unique	ement	

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

1000 and a strand sector And		-	
 Utilisateurs et ordinateurs Active Requêtes enregistrées ENSAT.loc 	Nom	Туре	Description
	GINF2 users	Groupe de sécurité - Global	
> 📔 Builtin	S Khalid Ameenhode	Otinsateur	
Computers			
> Domain Controllers			
GINF2			
> 🧾 ForeignSecurityPrincipal:			
> 🧮 Keys			
> CostAndFound			Propriétés de : Khalid Amechnoue ? ×
Managed Service Accourt Reparate Data			Membre de Réplication de mot de passe Appel entrant Obiet Sécurité
> System			Environnement Sessions Contrôle à distance
> 🛄 Users			Général Adresse Compte Profil Téléphones Organisation Certificats publiés
> 🧾 NTDS Quotas			Profil des services Bureau à distance COM+ Editeur d'attributs
> iii TPM Devices			Attributs :
			Attribut Valeur
			msDS-parentdistname <non défini=""></non>
			msDS-PhoneticComp <non défini=""></non>
			meDS-PhonetoCleparono.de/ini>
			msUs-rhonetcutgia
			msDS-PhoneticLastN <pre>cnon défni></pre>
			msDS-preferedDataL <a href="https://www.anandefinitation-contentio-contention-contentio-contenti-contentio-contentio-contentio-contentio-contentio-contentio-contentio-contentio-contentio-contentio-contentio-contentio-contentio-contentio-contentio-contentio-contentio-contentio-contenti-contentio-contentio-contentio-contentio-conten</td></tr><tr><td></td><td></td><td></td><td>msDS-PrimaryComputer onon definition</td></tr><tr><td></td><td></td><td></td><td>msUS-rmcpairvame erisAl vamechnoue Attribut : msDS-ResultantPSO</td></tr><tr><td></td><td></td><td></td><td>msDS-ReplVabeMet. valeur:
			msDS-ReplValueMet <non défni=""> (EN=GINE2.CN=Password Settings Container.CN=System.DC=ENSAT.DC=loc</non>
			msDS-ResultantPSO CN-GINF2/CN-Password Settings Container
			mBUS-HevealedListBL anon dern>
			Afficher Filtrer

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 avions 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 »

		- 🗆 X		
GINF2		TÂCHES V SECTIONS V		
GINE2 Paramètres de mot de passe S'applique directement à Extensions	Paramètres de mot de passe Nom : GINF2 Priorité : Appliquer la longueur minimale du mot de passe Longueur minimale du mot de passe (caractères) : Appliquer l'historique des mots de passe Nombre de mots de passe mémorisés : Catalante de mots de passe Nombre de mots de passe en utilisant un chiffrement réversible	IACHES SECTIONS IACHES SECTIONS Image: Section of the se		
	S'applique directement à Nom Courrier GINF2 users	Jusqu'à ce qu'un administrateur deverrouille manuellement le compte ① ③ ④ Ajouter Supprimer		
 Informations supplémenta 		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://blog.le-pi.com/?p=683

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

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