

## Introduction :

Dans ce TP, nous allons aborder la solution LAPS au sein du contexte. Une installation complète suivie d'un test de fonctionnement d'un utilisateur ayant un mot de passe généré par l'Active-Directory.

## Qu'est-ce que LAPS :

La solution LAPS permet de gérer les mots de passe aléatoires en mettant directement à jour les mots de passe de façon régulière directement dans Active Directory.

## Prérequis :

- PowerShell
- Active Directory (Windows Server 2003 ou une version supérieure)
- Stratégie de groupe

# Installation de LAPS :

Cliquer sur Windows Powershell (admin)



Taper : « Update-LapsADSchema »



La commande est vite bloquée donc aller dans « Users » puis « Administrateur du schéma »



Mettre « Administrateur » dans l'onglet « Membres » et fermer et rouvrir la session.



Puis retaper la commande, ensuite il faut dire 4 fois « o » et ensuite un « t »

🔀 Administrateur : Windows PowerShell	_		×
Windows PowerShell Copyright (C) Microsoft Corporation. Tous droits réservés.			^
PS C:\Users\Administrateur.MANCHESTER> Update-LapsADSchema			
The 'ms-LAPS-Password' schema attribute needs to be added to the AD schema. Do you want to proceed? [O] Oui [T] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre [?] Aide (la valeur par défaut e:	st « O	»):o	
The 'ms-LAPS-PasswordExpirationTime' schema attribute needs to be added to the AD schema. Do you want to proceed?			
[O] Oui [T] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre [?] Aide (la valeur par défaut e: The 'ms-LAPS-EncryptedPassword' schema attribute needs to be added to the AD schema.	st « O	») : o	
Do you want to proceed? [O] Oui [T] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre [?] Aide (la valeur par défaut e:	st « O	») : o	
The 'ms-LAPS-EncryptedPasswordHistory' schema attribute needs to be added to the AD schema. Do you want to proceed?			
[O] Oui [T] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre [?] Aide (la valeur par défaut e	st « O	») : o	
The 'ms-LAPS-EncryptedDSRMPassword' schema attribute needs to be added to the AD schema. Do you want to proceed? [0] Oui [T] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre [?] Aide (la valeur par défaut e: PS C:\Users\Administrateur.MANCHESTER> _	st « O	»):t	

## Puis enlever le membre « Administrateur » :

Propriétés de : Admin	ropriétés de : Administrateurs du schéma ? >					
Général Membres	Membre de Géré par					
Membres :						
Nom	Dossier Services de domaine Active Directory					
🔱 Administrateur	manchester.local/Users					
Services de dom	Services de domaine Active Directory					
Voule: group	e-vous supprimer le ou les membres sélectionnés du e ? Oui Non	]				

On retrouve bien les attributs LAPS dans les propriétés de l'ordinateur :



#### Créer une GPO dans le groupe ordinateur :

Gestion de stratégie de groupe	?	- 🗆 ×
Gestion de stratégie de groupe Gestion de groupe Gestion de stratégie de groupe Gestion	Gestion des stratégies de groupe         Cortenu         Nom	
Sélectionner un objet de stratégie		

#### Le nommer :

Nouvel objet GPO	×
Nom :	
LAPS-Activation	
Objet Starter GPO source :	
(aucun)	~

#### Puis modifier :

ojets de s	stratégie de groupe liés	Héritage de stratégie de group	be	Déléga	tion	
	Ordre des liens	Objet de stratégie de group	e		Appliqué	Lien act
	1	E LAPS-Activation	~	Moo App Lien Enre Sup Ren Acto	Men difier liqué activé sgistrer le rap primer ommer ualiser	port
<						>

Aller dans « Configuration ordinateur », puis « Stratégies » ensuite « Modèles d'administration » puis dans « Système »



Puis cliquer dans la liste sur « LAPS » :

📔 LAPS

Pour l'activation de LAPS, veuillez-vous rendre dans « Configurer le répertoire de sauvegarde de mot de passe », cocher la case « Activé », puis bien indiquer dans le répertoire de sauvegarde « Active Directory » puis appliquer cela.



Dans « Activer le chiffrement de mot de passe », cocher la case pour l'activer :

👰 Activer le chiffre	ment du mot de passe	- 0	$\times$
Activer le chiffre	ement du mot de passe	Paramètre précédent Paramètre suivant	
🔿 Non configuré	Commentaire :		^
Activé			
O Désactivé			$\sim$
	Pris en charge sur :	Au moins Microsoft Windows 10 ou version ultérieure	~
			~
Options :		Aide :	

Puis dans « Configurer la taille de l'historique des mots de passe chiffrés », activer et mettre indiquer « 2 » dans la taille de l'historique du mot de passe chiffré :

Configurer la taille de l'historique de	mots de passe ch	hiffrés		_		×
Configurer la taille de l'historique de	s mots de passe ch	hiffrés Pa	ramètre précédent	Paramètre su	iivant	
○ Non configuré Commentaire :						~
<ul> <li>Activé</li> </ul>						
◯ Désactivé						$\sim$
Pris en charge sur :	Au moins Micr	rosoft Windows	10 ou version ultérie	ure		~
						$\sim$
Options :	А	Aide :				
Taille de l'historique du mot de passe chi	ffré I	Utilisez ce paran passe chiffrés pr La configuratior de passe a été co	nètre pour configure écédents stockés dan n de ce paramètre n'a ponfiguré pour être sa	r le nombre de m ns Active Directo a aucun effet sau uvegardé sur	nots de ry. f si 1) le m	not

Dans « Paramètres du mot de passe », activer et adapter la ligne « longueur du mot de passe » selon ses besoins et la complexité aussi :

Paramètres du n	not de passe				_		$\times$
Paramètres du n	not de passe			Paramètre précédent	Paramètre su	ivant	
<ul> <li>Non configuré</li> <li>Activé</li> <li>Désactivé</li> </ul>	Commentaire : Pris en charge sur :	Au moins N	licrosoft Win	dows 10 ou version ultérie	eure		< >
Options :			Aide :				
Complexité du mot c Lettres majuscules + Longueur du mot de Âge du mot de passe	le passe lettres minuscules + c passe 20 e (jours) 30	hiffres + spé	Configure l Complexit de la génér Par défaut caractères Longueur o Minimum	les paramètres de mot de é des mots de passe : que ation d'un nouveau mot : lettres majuscules + lett spéciaux du mot de passe : : 8 caractères	passe Is caractères sont de passe res minuscules +	utilisés lo chiffres +	ors

Dans « Actions de post-authentification », activer et modifier selon ses besoins :

Actions de post-authentifie	ation		— D	×
Actions de post-authentifie	tation	Paramètre précédent	Paramètre suivant	
<ul> <li>Non configuré Commen</li> <li>Activé</li> <li>Désactivé</li> </ul>	taire :			<b>^</b>
Pris en cl	harge sur : Au moins N	Aicrosoft Windows 10 ou version ultérie	ure	$\hat{}$
Options :		Aide :		
Période de grâce (jours) : 24 Actions : Réinitialiser le mot de passe et	文	Cette stratégie configure les actions p seront exécutées après la détection d' compte géré. Période de grâce : spécifie le temps (r	post-authentification qui une authentification par le en heures) à attendre après	
		une authentification avant d'executer authentification spécifiées.	les actions post-	

Pour donner les droits à l'utilisateur de communiquer son mot de passe à Active Directory, il faut se rendre sur Powershell et taper cette commande :



Pour vérifier les autorisations il faut taper :

PS C:\Users\Administrateur.MANCHESTER> Find-	-LapsADExtendedRights	-Identity "OU=Ordinateurs,OU=DB,DC=manchester,DC=local"
ObjectDN	ExtendedRightHolders	
OU=Ordinateurs,OU=DB,DC=manchester,DC=local	{AUTORITE NT\Système,	MANCHESTER\Admins du domaine}

On voit bien que les seuls autorisés sont les Admins du domaine et le Système.

opriétés de : CLIENT ? ×	
énéral Système d'exploitation Membre de Délégation Réplication de mot de passe APS Emplacement Géré par Objet Sécurité Appel entrant Éditeur d'attributs Solution du mot de passe de l'administrateur local	
Expiration actuelle du mot de passe LAPS : jeudi 29 février 2024 17:46	Mot de passe du compte d'administrateur local LAPS :
Définir l'expiration du nouveau mot de passe LAPS : jeudi . février 29, 2024 5-46 □ ▼ Expirer maintenant	b.y\$3MbLw72,hS3{zhtX
Nom du compte d'administrateur local LAPS : [Administrateur Mot de passe du compte d'administrateur local LAPS :	opier le mot de pass
opier le mot de pass	
OK Annuler Appliquer Aide	

## <u>Conclusion :</u>

En définitive, la solution LAPS est un bon moyen pour générer des mots de passe robustes automatiquement ce qui permet de sécuriser les comptes à privilège et donc de protéger les données. C'est une solution assez facile à mettre en place et très utile.