# LAPS

## Microsoft

Windows Local Administrator Password Solution (LAPS)

MARGAUX TANET BTS 2 SIO

#### Introduction:

Nous allons installer la fonctionnalité windows LAPS sur un réseau.

Laps (Local Administrator Password Solution) permet de faire la gestion des mots de passe administrateurs locaux de nos postes clients/administrateur. Cela permet de centraliser et ainsi de sécuriser les mots de passe utilisés pour les administrateurs locaux des membres du domaine.

#### Pré requis:

- windows server 2019 mise à jour
- poste client mise à jour
- procédé à une sauvegarde avant

#### 1) Préparer le schéma

Le schéma correspond aux attributs que l'on peut utiliser. Les attributs sont les paramètres par objet. On peut leur donner une valeur. Cette manipulation va permettre de rajouter des attributs dédiés à LAPS.

Mise à jour de schéma:

Lancer le powershell en Administrateur:



Nous remarquons que nous n'avons pas les droits. C'est normal car on ne laisse pas tout le temps la possibilité aux administrateurs de modifier le schéma.



Il suffit de rajouter Administrateur dans le groupe des Administrateur du schéma. Se rendre dans l'AD et dans Utilisateurs et sélectionnez Administrateurs du schéma:

Utilisateurs et ordinateurs Active	Nom	Туре	Description	^
> Providence en la construcción de la construcci	🛃 Administrateur	Utilisateur	Compte d'utilisateur	r
V 🔢 bghm.local	Administrateurs clés	Groupe de séc	Les membres de ce o	ç
> Builtin	Administrateurs clés Enterprise	Groupe de séc	Les membres de ce o	ç
Computers     Domain Controllers	Administrateurs de l'entreprise	Groupe de séc	Administrateurs dési	i
EnceignSecurityPrincipal	Research Administrateurs du schéma	Groupe de séc	Administrateurs dési	
Managed Service Accourt	Admins du domaine	Groupe de séc	Administrateurs dési	i
🗸 🖬 MT	and the contrôleurs de domaine	Groupe de séc	Tous les contrôleurs	
> 🛱 Groupes	Contrôleurs de domaine clonables	Groupe de séc	Les membres de ce <u>c</u>	ŝ
> 📓 Import	Contrôleurs de domaine d'entreprise en lecture seule	Groupe de séc	Les membres de ce <u>c</u>	ŝ
📑 Ordinateurs	Contrôleurs de domaine en lecture seule	Groupe de séc	Les membres de ce g	5
> 🖬 Utilisateurs	A DnsAdmins	Groupe de séc	Groupe des administ	t
> 🖬 ScriptTest	A DnsUpdateProxy	Groupe de séc	Les clients DNS qui s	;
TEST	Kiteurs de certificats	Groupe de séc	Les membres de ce <u>c</u>	5
🛄 Users	Groupe de réplication dont le mot de passe RODC est	Groupe de séc	Les mots de passe de	£
	Groupe de réplication dont le mot de passe RODC est	Groupe de séc	Les mots de passe de	£
	ᡖ Invité	Utilisateur	Compte d'utilisateur	t –
	🕾 Invités du domaine	Groupe de séc	Tous les invités du de	
	Continateurs du domaine	Groupe de séc	Toutes les stations de	
	Ropriétaires créateurs de la stratégie de groupe	Groupe de séc	Les membres de ce g	5
	Reprotected Users	Groupe de séc	Les membres de ce <u>c</u>	۲Y
			>	

Se rendre dans l'onglet "Membre" et ajouter votre Administrateur:

énéral	Membres	Membre de	Géré par					
Membre	s:							
Nom		Dossier S	ervices de do	maine Activ	ve Director	у		
Ad	lministrateur	bghm.loca	al/Users				 	
Ajou	ter	Supprimer						
Ajou	ter	Supprimer	]					
Ajou	ter	Supprimer						

Pour pouvoir prendre en compte la modification il faut fermer puis rouvrir la session. Rouvrir l'invite de commande powershell et refaire la même commande qu'au début. Et cette fois-ci aucune erreur est ressortie:



### Ne pas oublier d'aller retirer à nouveau votre administrateur des membres d'administrateur du schéma:

Utilisateurs et ordinateurs Active Directory	_		$\times$
Fichier Action Affi	1		
Utilisateurs et ordina Général Membres Membre de Géré par	Descrip	tion	^
> 📔 Requêtes enregi: 🛛 Membres :	Compte	e d'utilisa	teur
V 🏭 bghm.local	Les mer	mbres de	cer
Builtin     Advisite target, John Band / Jack	Les mer	mbres de	cer
> Computers	Admini	strateurs	dési
> 📓 Domain Con	Admini	strateurs	dési
> ForeignSecu	Admini	strateurs	dési
> Managed Sei	Tousles	s contrôle	PUIS
> I MI	Les mer	mbres de	cer
	Les mer	mbres de	cer
	Les mer	mbres de	cer
	Groupe	des adm	inist
	Les clie	nts DNS o	nui s
	Les mer	mbres de	cer
	Les mot	ts de pas	se de
	Les mot	ts de pas	se de
	Compte	e d'utilisa	teur
Ajouter Supprimer	Tous les	invités c	du du
	Toutes	les statio	ns du
	Les mer	mbres de	cer
OK Annuler Appliquer	Les mer	mbres de	ce c V
			>

Vérifier que la mise à jour du schéma a bien été faite en allant vérifier un objet active directory:

Pour cela se rendre dans l'OU "ordinateur" sous l'AD. Clic droit sur notre PC client puis propriété:



Juste avant, sur certains ordinateurs l'onglet "éditeurs d'attributs" n'apparaît pas. Pour cela, dans "Affichage" sélectionner "fonctionnalités avancées" pour que cet onglet apparaît.



Se rendre dans l'onglet "éditeur d'attributs":

ropriétés	de : CLI-V-	)1-MT				7	?	×
LAPS	Emplacemer	t Géré par	Objet	Sécurité	Appel entra	nt Éditeur	r d'att	tributs
Général	Système d	exploitation	Membre de	Déléga	tion Réplic	ation de mo	t de p	oasse
Ņ	CLI-V-01-	MT						
Nom d'o Window	rdinateur (ant s 2000) :	érieur à	CLI-V-	01-MT				
Nom DN	IS :	CLI-V-01-MT	.bghm.local					
Type de contrôleur de domaine : Station de travail ou serveur								
Site :								
Descript	ion :							

Je retrouve bien les attributs msLaps:

Général	Système d'exp	loitation	Membre de	Déléga	tion Rép	Réplication de mot de p		
LAPS	Emplacement	Géré par	Objet	Sécurité	Appel ent	rant	Éditeur d'attributs	
Attribut	s :							
Attribu	ıt	Valeur				^		
msIIS	-FTPDir	<non défi<="" td=""><td>ni&gt;</td><td></td><td></td><td></td><td></td></non>	ni>					
msIIS	-FTPRoot	<non défi<="" td=""><td>ni&gt;</td><td></td><td></td><td></td><td></td></non>	ni>					
mslma	aging-HashAlgor	<non défi<="" td=""><td>ni&gt;</td><td></td><td></td><td></td><td></td></non>	ni>					
mslma	aging-Thumbprin	. <non défi<="" td=""><td>ni&gt;</td><td></td><td></td><td></td><td></td></non>	ni>					
msLA	PS-EncryptedD	<non défi<="" td=""><td>ini&gt;</td><td></td><td></td><td></td><td></td></non>	ini>					
msLA	PS-EncryptedD	<non défi<="" td=""><td>ni&gt;</td><td></td><td></td><td></td><td></td></non>	ni>					
msLA	PS-EncryptedP	<non défi<="" td=""><td>ini&gt;</td><td></td><td></td><td></td><td></td></non>	ini>					
msLA	PS-EncryptedP	<non défi<="" td=""><td>ni&gt;</td><td></td><td></td><td></td><td></td></non>	ni>					
msLA	PS-Password	<non défi<="" td=""><td>ni&gt;</td><td></td><td></td><td></td><td></td></non>	ni>					
msLA	PS-PasswordEx	<non défi<="" td=""><td>ni&gt;</td><td></td><td></td><td></td><td></td></non>	ni>					
mSM	QDigests	<non défi<="" td=""><td>ni&gt;</td><td></td><td></td><td></td><td></td></non>	ni>					
mSM	QDigestsMig	<non défi<="" td=""><td>ni&gt;</td><td></td><td></td><td></td><td></td></non>	ni>					
mSM	QSignCertificates	<non défi<="" td=""><td>ni&gt;</td><td></td><td></td><td></td><td></td></non>	ni>					
mSM	QSignCertificate	<non défi<="" td=""><td>ni&gt;</td><td></td><td></td><td>~</td><td></td></non>	ni>			~		
<					>			

Cela permet de stocker les mots de passe chiffrer, l'historique de mot de passe, le mot de passe si on ne souhaite pas le chiffrer et le temps ou le mot de passe est valide.

#### 2) Paramétrage de la stratégie de groupe LAPS

Administrer LAPS c'est donner les paramètres qu'on veut appliquer pour le cas, cela va se faire par stratégies. Se rendre dans "gestion de stratégies de groupes":

🏥 i 🛃 🔚 🖛			Gérer	Gérer	Outils d'administration						
Fichier Accue	eil Parta	age Affichage	Outils de raccourci	Outils d'application							
$\leftarrow$ $\rightarrow$ $\checkmark$ 🏠 > Panneau de configuration > Système et sécurité > Outils d'administration >											
		Nom	^	Modifié le	Туре	Taille					
🖈 Accès rap	ide	Terminal Serv	ices	15/09/2018 09:19	Dossier de fichiers						
E Bureau	R	Analyseur de	performances	15/09/2018 09:12	Raccourci	2 Ko					
🕂 Téléchar	gement: 🖈	📑 Centre d'adm	iinistration Active Director	y 15/09/2018 09:13	Raccourci	2 Ko					
🔮 Docume	ents 🖈	🔁 Configuration	n du système	15/09/2018 09:12	Raccourci	2 Ko					
📰 Images	*	齄 Défragmente	r et optimiser les lecteurs	15/09/2018 09:12	Raccourci	2 Ko					
Scripts		👔 Diagnostic de	e mémoire Windows	15/09/2018 09:13	Raccourci	2 Ko					
System3	2	尤 DNS		15/09/2018 09:13	Raccourci	2 Ko					
	-	😹 Domaines et a	approbations Active Direc	tory 15/09/2018 09:14	Raccourci	2 Ko					
💻 Ce PC		👫 Éditeur du Re	gistre	15/09/2018 09:12	Raccourci	2 Ko					
🔿 Réseau		🔚 Gestion de l'ir	mpression	15/09/2018 09:13	Raccourci	2 Ko					
<u> </u>		╊ Gestion de l'o	ordinateur	15/09/2018 09:12	Raccourci	2 Ko					
		🔏 Gestion des st	tratégies de groupe	15/09/2018 09:13	Raccourci	2 Ko					
		声 Gestionnaire	de serveur	15/09/2018 09:13	Raccourci	2 Ko					
		👰 Informations	système	15/09/2018 09:13	Raccourci	2 Ko					
		👧 Initiateur iSCS	51	15/09/2018 09:12	Raccourci	2 Ko					
		🚌 Lecteur de ré	cupération	15/09/2018 09:12	Raccourci	2 Ko					

On veut appliquer LAPS sur notre unité d'organisation d'ordinateurs .Pour se faire , on va créer une GPO. Se rendre dans l'AD, se mettre sur l'OU "ordinateurs", clic droit "créer un objet GPO:

	Créer un objet GPO dans ce domaine, et le lier ici				
🎼   🛃 🗖 🖛 🖛 I	Lier un objet de stratégie de groupe existant		rer	Outils	d'adm
Fichier Accueil	Bloquer l'héritage		oplication		
📓 Gestion de stratégie de gro	Mise à jour de la stratégie de groupe				
Fichier Action Afficha	Assistant Modélisation de stratégie de groupe				
	Nouvelle unité d'organisation				
Gestion de stratégie de gro	Affichage	>			
✓ A Forêt : bghm.local	Nouvelle fenêtre à partir d'ici		de stratégie d	e amune	Déléa
✓ G Domaines	Supprimer			e groupe	Deleg
bghm.local Default Dom	Renommer		le stratégie de	e groupe	
> 📓 Domain Con	Actualiser				
🗸 📴 MT	Dronriétés				
> 🖬 Groupes					
> G Ordinateurs	Aide				
> Utilisateurs					

Pour modifier la stratégie, clic droit "modifier":

Ordre des liens	Objet de strat	égie d	le groupe	Appliqué	Lien activé	É
1	🗐 Laps			Non	Oui	P
	_		Modifier			
			Appliqué			
		~	Lien activé			
			Enregistrer le rap	port		
			Supprimer			
			Renommer			
			Actualiser			

Puis se rendre dans "configuration ordinateur" > "modèles d'administrateur" > "Système"



#### On retrouve dans cette liste "LAPS":



Nous allons activer LAPS en configurant le répertoire de sauvegarde de mot de passe LAPS tant qu'on active pas cela, nous n'activons pas LAPS car il est installé mais pas utilisé.

Pour ce faire, clique droit "configurer le répertoire de sauvegarde de mot de passe" et cliquer sur "activer" et sélectionner comme répertoire de sauvegarde "active directory" comme nous sommes en local.

Configurer le rép	pertoire de sauvegarde	de mot de passe	- 0	×	
Configurer le ré	pertoire de sauvegarde	de mot de passe Paramètre précédent	Paramètre suivant		dministration
Non configuré	Commentaire :			^	1
🔿 Activé					
<ul> <li>Désactivé</li> </ul>	Pris on charge sur l			~	
	Pris en charge sur :	Au moins Microsoft Windows 10 ou version ultérie	eure	<u></u>	
Ortional		A		v	الأوعان المراجع
Options :		Alde:			Annliqué Lien.activé État.GPO Filtre WMI Modifié le
Répertoire de sauve	garde	Utilisez ce paramètre pour configure mot de passe du compte d'administ	er le répertoire dans lequel le crateur local est sauvegardé.	^	
	~	Les paramètres autorisés sont :			
		0=Désactivé (le mot de passe ne sera	a pas sauvegardé)		
		1=Sauvegarder le mot de passe dans	s Azure Active Directory		vire de Paramètre
		2=Sauvegarder le mot de passe pour	r Active Directory		Activer la sauvegarde de mot de passe pour les comptes I     Configurer la taille de l'historique des mots de passe chiff
		Si ce paramètre n'est pas spécifié, la	valeur par défaut est 0		de strategie
		Ci co poromètro est configuré sur 1 e	t que l'appareil géré p'est pa	_	i: E Configurer les déchiffreurs de mot de passe autorises findows 10 E Nom du compte administrateur à gérer
		relié à Azure Active Directory, le mot	t de passe de l'administrateu	r	Configurer le répertoire de sauvegarde de mot de passe N'autorisez pas le délai d'expiration du mot de passe plus
		Si ce paramètre est configuré sur 2 e relié à Active Directory. le mot de pa	t que l'appareil géré n'est pa sse de l'administrateur local	s	our E Paramètres du mot de passe e dans E Actions de post-authentification
		ne sera pas géré.		~	est
		OK	Annuler Appliqu	ier	iés sont :

Grâce à cela tous les ordinateurs membres de l'unité d'organisation "ordinateurs" pourront stocker leur mot de passe administrateur locaux dans l'AD. Nous avons activé LAPS.

Dans un deuxième temps, nous allons décider de quel administrateur et de qui on veut gérer. Par défaut si on n'active pas cette stratégie, le compte administrateur en local c'est le compte administrateur.

On va chiffrer le mot de passe. Par défaut, il n'est pas chiffré il est en clair: Choisir "activer le chiffrement du mot de passe" puis "activé":

Activer le chiffre	ment du mot de passe					×	tion
Activer le chiffre	ement du mot de passe		Paramètre précédent	Paramètre sui	vant		-
○ Non configuré	Commentaire :					^	
O Désactivé	Pris en charge sur :	Au moins Microso	ft Windows 10 ou version ultérie	ure		< >	pliqué Lien.activé État.GPO Filtre WMI Mr
Options :		Aide	:				
		Lors: cryp L'act pass et 2) Wind Si ce	que vous activez ce paramètre, le té avant d'étre envoyé à Active D ivation de ce paramètre n'a auce e a été configuré pour être sauve le niveau fonctionnel du domai dows Server 2016 ou supérieur. paramètre est activé et que le ni	e mot de passe gé lirectory. un effet sauf si 1) egardé dans Activ ne Active Director iveau fonctionnel	ré est le mot de e Directory y est du	^	de Paramètre E Activer la sauvegarde de mot de passe pour l Configurer la taille de l'historique des mots d Activer le chiffrement du mot de passe

Cliquer "configurer la taille de l'historique des mots de passes chiffrés" et activé et mettre "2" en taille:

Configurer la tai	lle de l'historique des n										
Configurer la tai	lle de l'historique des n	nots de passe	chiffrés Paramètre précédent	Paramètre sui	vant						× - 8 ×
🔿 Non configuré	Commentaire :					^					
<ul> <li>Activé</li> <li>Désactivé</li> </ul>	Activé     Désactivé										
	Pris en charge sur :	Au moins N	ins Microsoft Windows 10 ou version ultérieure				Lien activé	État GPO	Filtre WMI	Modifié le	Dr
Options :			Aide :								
Taille de l'historique du mot de passe chiffré			Utilisez ce paramètre pour configurer le passe chiffrés précédents stockés dans . La configuration de ce paramètre n'a au de passe a été configuré pour être sauv Active Directory et 2) le chiffrement de	nombre de mo Active Directon ucun effet sauf egardé sur mot de passe a	ots de y. si 1) le m été activ	not /é.	Paramètre E Activer la s	auvegarde de r la taille de l'his	not de passe p storique des m	our les comp ots de passe (	ites DS chiffrés

## Cliquer sur "paramètres du mot de passe" puis "activer" et mettre en longueur du mot de passe "20".

Paramètres du r	not de passe					$\times$	
Paramètres du n	not de passe		Paramètre précédent Para	imètre sui	vant		
Non configuré  Activé	Commentaire :					<u>^</u>	
() Désactivé	Pris en charge sur :	Au moins M	icrosoft Windows 10 ou version ultérieure			Ŷ	Lien activé État GPO Filtre WMI
Options :			Aide :			_	
Complexité du mot Lettres minuscules Longueur du mot du Âge du mot de pass	de passe + lettres minuscules e passe 20 e (jours) 30	A V	Configure les paramètres de mot de passe Complexité des mots de passe : quels caract de la génération d'un nouveau mot de passe Par défaut : lettres majuscules + lettres minu caractères spéciaux Longueur du mot de passe : Minimum : 8 caractères Maximum : 64 caractères Défaut : 14 caractères Âge du mot de passe en jours Minimum : 1 jour (7 jours lorsque le réperto	ères sont iscules +	utilisés lor chiffres + rvegarde	rs	aramètre Activer la sauvegarde de mot de pass Configurer la taille de l'historique des Activer le chiffrement du mot de pas Configurer les déchiffreurs de mot de Nom du compte administrateur à gé Configurer le répertoire de sauvegarc N'autorisez pas le délai d'expiration d Paramètres du mot de passe

#### 3) Modification des droits d'accès à l'OU ordinateurs pour LAPS

Il faut donc que le pc client ait le droit d'écrire sur *msLAPS* par défaut il n'a pas le droit. On va lui donner les droits et donc de pouvoir les communiquer à Active Directory.

Ouvrir une invite de commande Powershell en admin, taper la commande "**Set -**LapsADComputerSelfPermission". Cela donne à l'ordinateur de modifier les droits lui même ses attributs LAPS. Et indiquer l'OU dans laquelle se faire en ajoutant "- Identity OU=Ordinateurs, OU=MT, DC=bghm, DC=local".



Les droits ont bien été modifiés.

<u>Conseil</u>: Bien vérifier qu'il n'y a pas de droits complémentaires en amont sur l'OU: commande: "find-LapsADExtendedRights "*- Identity OU=Ordinateurs, OU=MT, DC=bghm, DC=local*"

Nous pouvons regarder que le laps a bien été activé sur notre poste client:



Se rendre sur le poste client et faire la mise à jour de la stratégie en faisant "*gpupdate /force*".

En se rendant sur les propriétés puis dans l'onglet éditeurs d'attributs, il est renseigné le mot de passe LAPS pour le compte Administrateur.

priété	s de :						?		
énéral	Système d'exploitation		Membre de	Délégation		Réplicati	on de mot	mot de pas	
APS	Emplacement	Géré par	Objet	Sécurité	Арр	el entrant	Éditeur	d'attrib	21
Expire	ation actuelle du	mot de pas	se LAPS :						
Défin	ir l'expiration du r	nouveau mo	ot de passe l	APS :					
					Ex	pirer mainte	enant		
Nom	du compte d'adn	ninistrateur l	ocal LAPS :						
Admi	inistrateur								
Mot o	le passe du com	ote d'admin	istrateur loca	I LAPS :					
•••	•••••	•••••	•••						
opie	r le mot de passe	ficher le	mot de pass						

#### **Conclusion :**

On a donc paramétré LPAS sur notre serveur AD en mettant à jour le schéma, on a paramétré les stratégies de groupes. Nous avons défini comment on voulait chiffrer le mot de passe et la complexité du mot de passe. Nous avons mis les droits de modifications du mot de passe LAPS sur l'OU ordinateurs. Enfin nous avons pu se rendre compte que cela fonctionnait bien.