n Guastamacchia Livio SIO2

#### **Durcissement Serveur :**

### **Introduction :**

Lors de ce TP nous allons effectuer quelque paramètre de base afin de sécurisé nos serveur.

TP:

La première étape de sécurité de ce TP sera d'activé le pare-feu Windows

Réseau avec domaine

Le pare-feu est activé.

Réseau privé

Le pare-feu est activé.

# Seeau public (actif)

Le pare-feu est activé.

Ensuite nous allons faire en sorte que notre serveur soit a jour dans Windows update

Windows Update Demière recherche de mises à jour : Télécharger les mises à jour uniquement à l'aide de Windows Update

Et nous activerons aussi dans les paramètre avancer, le fait de recevoir les mises a jours des produits Microsoft qui permettra de tenir a jours tous les produits Microsoft sur notre serveur.

Recevoir les mises à jour d'autres produits Microsoft lors de la mise à jour de Windows

Activé

L'antivirus doit être aussi activé surtout la protection en temps réel qui montre bien que l'antivirus est actif

# Protection en temps réel

Ce paramètre permet d'identifier et d'empêcher l'installation ou l'exécution de programmes malveillants sur votre appareil. Vous pouvez le désactiver temporairement, mais nous le réactiverons automatiquement.

Activé

Dans les services nous pouvons arrêté le spouleur d'impression si notre serveur n'est pas un serveur d'impression afin d'évité les failles potentielles

Propriétés de Spouleur d'impression (Ordinateur local) ×							$\times$	
Général	Connexion	Récupérati	ion	Dépend	ances			
Nom du	service :	Spooler						
Nom complet : Spouleur d'impression								
Description : Ce service met en spoule les travaux d'impression et gère l'interaction avec l'imprimante. Si vous								
Chemin d'accès des fichiers exécutables : C:\Windows\System32\spoolsv.exe								
Type de	e démarrage	: C	)ésa	ctivé			~	
État du	service : A	nêté						
Dér	marrer	Arrêter		Susp	endre	Repr	endre	
Vous pouvez spécifier les paramètres qui s'appliquent au démarrage du service.								
Paramètres de démarrage :								
			0	K	Annule	r	Applique	r

La vérification de la version du protocole SMB est important car il y a une version ancienne qui n'est plus utilisé « SMBv1 » alors si nous n'utilisons pas ce protocole, nous devons le désactiver et pour voir si il est installé par le biais de l'interface graphique. Nous allons faire ajouter un rôle et regarder dans les fonctionnalités si la case « support de partage de fichier SMB 1.0/CIFS » est cocher si elle ne l'est pas c'est qu'il n'est pas utilisé sur notre serveur. Dans l'autre cas ou elle est cocher, il est préconisé de désinstaller ce rôle et de passer a des versions plus sécurisé de ce protocole.

Þ	Support	de	partage	de fic	hiers	SMB	1.0/CIFS
	A		·				

Sur notre disque local nous pouvons activé les clichés instantanés afin d'avoir une sauvegarde de l'état de notre disque a un moment donné

Propriétés de : Disque local (C:)

Général	Out	ls M	atériel	Partag	je	Sécurité
Clichés instanta	anés	Versions pré	cédentes	Quot	a	Classification
es clichés instar xistait dans le pa liquez ici. Vélectionnez un	ntanés pe assé. Pou volume :	mettent de voir r obtenir plus d'ii	le contenu o nformations	des dossiers sur les clich	partag és insta	és tel qu'il antanés,
Volume	Heur	e de la procha	Partages		Utilisé	
🕮 \\?\Volume	{ Désa	ctivé	0			
🕞 C:\	10/1	2/2024 12:00	2		320 M	lo sur C:\
Activer Désactiver Paramètres						
-Clichés instanta	anés du v	olume sélectionr	né			
10/12/2024	10:09					Créer
					S	upprimer
					F	Rétablir

C'est dans le fichier « Perflogs » ou nous pourrons restauré les sauvegarde précédente

rona ceran	01/10/202411.00	
PerfLogs	08/05/2021 10:20	
Program	Ouvrir	
Program	Ouvrir dans une nouvelle fenêtre	
StorageF	Épingler à Accès rapide	
Utilisater	Accorder l'accès à	
Window	Restaurer les versions précédentes	
	Inclure dans la bibliothèque	
	Épingler à l'écran de démarrage	
	Envoyer vers >	
	Couper	
	Copier	
	Créer un raccourci	
	Supprimer	
	Renommer	
	Propriétés	

Nous pouvons voir que le cliché que j'ai créer a l'instant est affiché dans l'onglet version précédente et en rentrant dans ce dossier nous pourrons naviguer dans la sauvegarde du disque et restaurer ce qui nous intéresse

∽ Aujourd'hui (1)	
- PerfLogs	10/12/2024 10:09

🖌 « Disque local (C:) (Aujourd'hui 10 décembre 2024, il y a 7 min... 🔅 PerfLogs (Aujourd'hui 10 décembre 2024, il y a 7 minutes)

Nous passons a présent au chiffrement du disque dur via Bitlocker. Pour cela nous allons ajouté une fonctionnalité dans les rôles qui sera « chiffrement de lecteur Bitlocker »

	brancheache
✓	Chiffrement de lecteur BitLocker
	Client d'impression Internet

Après avoir installé la fonctionnalité, nous pouvons activé Bitlocker sur notre disque

Affichage       Outils de lecteur         Ce PC >       Ouvrir         Ouvrir dans une nouvelle fenêtre         Épingler à Accès rapide         Ouvrir BitLocker         Accorder l'accès à         Configurer les clichés instantanés         Bertaurer les versions précédenter		Gérer	Ce PC
Ce PC > Ouvrir dans une nouvelle fenêtre Épingler à Accès rapide Ouvrir dans une nouvelle fenêtre Épingler à Accès rapide Activer BitLocker Accorder l'accès à Configurer les clichés instantanés Bertaurer les versions précédenter	Affichage	Outils de lecteur	Ouvrir
Dossiers (/)      Bureau      Configurer les clichés instantanés      Restaurer les versions précédenter	Ce PC >		Ouvrir dans une nouvelle fenêtre Épingler à Accès rapide Activer BitLocker
Restaurer les versions précédentes	V Dossie	ers (7) Bureau	Accorder l'accès à
Musique Épingler à l'écran de démarrage		Musique	Restaurer les versions précédentes Épingler à l'écran de démarrage
Vidéos Copier		Vidéos	Formater Copier
S v Périphériques et lecteurs ( Renommer	s ∨ Périph	ériques et lecteurs	Créer un raccourci Renommer
Disque local (C:) 22.3 Go libres sur 39.3 Go U octet(s) libres sur 5, 18 Go		Disque local (C:)	Propriétés

Notre poste ne contient pas de puce TPM, nous allons donc procédé a une installation sans puce TPM

🏘 Chiffrement de lecteur BitLocker (C:)

## Démarrage de BitLocker

Ce périphérique ne peut pas utiliser un module de plateforme sécurisée (TPM). Votre administrateur doit définir l'option « Autoriser BitLocker sans un module de plateforme sécurisée compatible » dans la stratégie « Demander une authentification supplémentaire au démarrage » pour les volumes du système d'exploitation.

Pour cela, nous allons ouvrir l'exécuter et ouvrir l'éditeur de stratégie local « gpedit.msc »

٨	Entrez le nom d'un programme, dossier, document ou ressource Internet, et Windows l'ouvrira pour vous.
<u>O</u> uvrir :	gpedit.msc 🗸
	Cette tâche sera créée avec les autorisations d'administrateur.
	OK Annuler Parco <u>u</u> rir

Nous nous rendons dans le chemin « configuration ordinateur » -> « modèle d'administration » -> « Composant Windows » -> « Chiffrement de lecteur Bitlocker » -> « lecteurs du système d'exploitation » Puis nous allons activer « exiger une authentification supplémentaire au démarrage »

	Straté ✓ Me Co > □ > □ ✓ ✓	gie Ordinateur local onfiguration ordinateur Paramètres du logiciel Paramètres Windows Modèles d'administrat Composants Windo Analyse de fiab Analyse de fiab Composants Windo Assistance en li Bac à sable Windo Assistance en li Bac à sable Windo Carte à puce Cartes Cartes Cartes Centre de mobi Centre de sécur Centre de sécur	ion ows ilité Windows soft Defender gne adows dows dows ilité Windows rité lecteur BitLocker données amovibles données fixes système d'exploitation		
Exiger une authe	ntification supplément	taire au démarrage		$ \Box$	×
Exiger une authe	ntification supplément	taire au démarrage	Paramètre précédent	Paramètre suivant	
<ul> <li>Non configuré</li> <li>Activé</li> <li>Désactivé</li> </ul>	Commentaire :				
0	Pris en charge sur :	Au minimum Windows S	erver 2008 R2 ou Windows	7	^ ~
Options :		Aide :			

Nous cochons aussi dans la même interface « autorisé bitlocker » si cela ne s'est pas fait automatiquement

Autoriser BitLocker sans un module de plateforme sécurisée compatible (requiert un mot de passe ou une clé de démarrage sur un disque mémoire flash USB)

Après cela nous pouvons activer bitlocker en lui mettant un mot de passe ainsi que enregistrer sa clé de récupération.

Maintenant lors de l'installation, nous pouvons choisir comment bitlocker fonction. Soit nous prenons chiffré que l'espace utilisé soit chiffrer tout le lecteur qui est meilleur lorsqu'il est en production dans notre cas nous prendrons chiffre que l'espace utilisé et même si de nouvelles données sont rajouté ils seront chiffré au fur et a mesure.

🏘 Chiffrement de lecteur BitLocker (C:)

# Choisir dans quelle proportion chiffrer le lecteur

Si vous configurez BitLocker sur un nouveau lecteur ou un nouveau PC, il vous suffit de chiffrer la partie du lecteur en cours d'utilisation. BitLocker chiffre automatiquement les nouvelles données que vous ajoutez.

Si vous activez BitLocker sur un PC ou un lecteur en cours d'utilisation, chiffrez l'intégralité du lecteur. Le chiffrement de l'intégralité du lecteur garantit la protection de la totalité des données, même des données supprimées qui peuvent contenir des informations récupérables.

Ne chiffrer que l'espace disque utilisé (plus rapide et plus efficace pour les nouveaux PC et lecteurs)

O Chiffrer tout le lecteur (opération plus lente recommandée pour les PC et les lecteurs en service)

Pour le mode de chiffrement nous avons le choix entre le nouveau mode et le mode compatible, le nouveau seras principalement sur les poste récent qui possède la mise a jour bitlocker et qui puisse le faire tourner mais pour le mode compatible ce sera majoritairement pour les poste avec un système d'exploitation antérieur a windows 10. Dans notre cas nous prenons le nouveau mode car il est plus sécurisé.

🙀 Chiffrement de lecteur BitLocker (C:)

# Choisir le mode de chiffrement à utiliser

La mise à jour Windows 10 (Version 1511) présente un nouveau mode de chiffrement de disque (XTS-AES). Ce mode fournit une prise en charge supplémentaire de l'intégrité, mais il n'est pas compatible avec les versions antérieures de Windows.

S'il s'agit d'un lecteur amovible que vous allez utiliser sur une version antérieure de Windows, vous devez choisir le mode Compatible.

S'il s'agit d'un lecteur fixe ou si ce lecteur ne va être utilisé que sur des appareils exécutant au moins Windows 10 (Version 1511) ou version ultérieure, vous devez choisir le nouveau mode de chiffrement

Nouveau mode de chiffrement (recommandé pour les lecteurs fixes sur ce périphérique)

O Mode Compatible (recommandé pour les lecteurs pouvant être déplacés à partir de ce périphérique)

Puis enfin, nous exécuterons la vérification du système bitlocker qui permettras a bitlocker de voir si il est capable de lire la clé de chiffrement et de récupération avant de chiffrer le lecteur.

🏘 Chiffrement de lecteur BitLocker (C:)

# Êtes-vous prêt à chiffrer ce lecteur ?

Le chiffrement peut prendre un moment, selon la taille du lecteur.

Vous pouvez continuer à travailler pendant le chiffrement du lecteur, bien que les performances de votre ordinateur puissent être affectées.

Exécuter la vérification du système BitLocker

La vérification du système permet de s'assurer que BitLocker peut lire correctement les clés de récupération et de chiffrement avant de chiffrer le lecteur.

BitLocker redémarrera votre ordinateur avant d'effectuer le chiffrement.

Remarque : cette vérification peut être longue, mais elle est recommandée pour vous assurer que la méthode de déverrouillage sélectionnée fonctionne sans devoir entrer la clé de récupération.

# **Conclusion :**

Le poste ne possédant pas de puce TPM, il a causé problème lors de l'activation de Bitlocker mais il y a un moyen de contourner le problème ce qui a permis de finalisé cette parti du TP

## **Durcissement AD :**

### **Introduction :**

Le but de cette parti du TP est de procédé a une amélioration de sécurité plus centré sur Active Directory que sur un poste client

### **TP** :

Pour commencer, nous allons activé la corbeille activé directory. Pour cela nous allons dans le centre d'administration active directory.

🛃 Centre d'administration Active Directory 08/05/2021 10:15 Raccourci 2 Ko

Sur notre domaine, nous activons la corbeille

🔛 Vue d'ensemble			
🖬 pologne (local)	•		En savoir p
<ul> <li>Contrôle d'acc</li> <li>Authentificatio</li> <li>Recherche gloi</li> </ul>	Modifier le co Augmenter le Augmenter le Activer la Cor	ntrôleur de domaine niveau fonctionnel c niveau fonctionnel c beille	e la forêt lu domaine IO
	Nouveau Rechercher so Propriétés	ous ce nœud	

On nous précise bien que dès lors qu'on active la corbeille nous ne pourrons plus la désactiver après

	Activer la	confirmation de la Corbe	lle	×	(
		Êtes-vous sûr de vouloir Corbeille activée, elle ne	effectuer cette act peut plus être dé:	ion ? Une fois la sactivée.	
			ОК	Annuler	
itils d'admin	istration <	« modification ADSI »			

Dans les ou

	,,		
🌠 Modification ADSI	08/05/2021 10:15	Raccourci	2 Ko
NALILIA ALI DI LA MANA	00/0E/2021 10.1E	D:	n 1/ -

Lorsque nous nous y rendons pour la première fois, nous arrivons sur une page vide. Pour y remédier nous faisons connexion sur « modification ADSI » et nous laissons par défaut les paramètre, cela nous connectera automatiquement

Modification ADSI		
	Connexion	diteur ADSI
	Affichage	>
	Actualiser	reau pour les services de domaine Active Directory et les
	Aide	D LDS (Active Directory Lightweight Directory Services). rmet d'afficher, de modifier, de créer et de supprimer un
	obj AD Mic Pou cliq	et dans les services de domaine Active Directory ou les services LDS (Active Directory Lightweight Directory Services) de crosoft. ur créer une connexion vers ces services, dans le menu Action, quez sur Connexion.

Dans les propriétés nous chercherons le paramètre « ms-DS-MachineAccountQuota » qui par défaut est a 10 et nous le mettrons a 0 car c'est le paramètre qui dit le nombre de machine maximal qu'un utilisateur peut ajouté au domaine.

🗢 🖦 🔟 🛅 🗶 🗎 🖉 🗟		Propriétés de : DC=pologne,DC=local ?	$\times$
Modification ADSI	Non		
✓  ☐ Contexte d'attribution de no		Editeur d'attributs Sécurité	
> 📔 DC=pologne,DC=local	2	Attribute :	
	9	Autibuts .	_
	🛄 q	Attribut Valeur	^
	🚞 q	msDS-Behavior-Version 7 = (WIN2016)	
	🚞 q	msDS-CloudAnchor <pre><non défini=""></non></pre>	
	📫 d	mS-DS-ConsistencyChildCount <non défini=""></non>	
	📔 d	mS-DS-ConsistencyGuid <non défini=""></non>	
	d	msDS-EnabledFeature <non défini=""></non>	
	d	msDS-ExpirePasswordsOnSmartCardOnlyAccou TRUE	
	d	msDS-LastKnownRDN <non défini=""></non>	
	2	msDS-LogonTimeSyncInterval <non défini=""></non>	
	2	ms-DS-MachineAccountQuota 10	
	2	msDS-NcType 0	
		msDS-ObjectSoa <non défini=""></non>	
	99	msDS-PerUserTrustQuota 1	
		msDS-PerUserTrustTombstonesQuota 10	
		msDS-SourceAnchor <non défini=""></non>	×
		Modifier	
		The second	
		OK Annuler Appliquer Aid	e
msDS-Logo	on Times	SyncInterval <non défini=""></non>	
ms-DS-Mac	chineAc	ccountQuota 0	
msDS-NcT	ype	0	

Pour poursuivre, dans les utilisateurs et ordinateurs active directory dans le dossier « builtin » nous avons le groupe « accès compatible pré-windows 2000 » qui sert a la rétrocompatibilité avec les Windows avant 2000 en leur donnant les droits de lecture

Utilisateurs et ordinateurs Active	Nom	Туре	Description
Requêtes enregistrées	Accès compatible pré-Windows 2000	Groupe de séc	Un groupe de compatibi
pologne.local	Accès DCOM service de certificats	Groupe de séc	Les membres de ce grou
Builtin	Administrateurs	Groupe de séc	Les membres du groupe
> Computers	Administrateurs Hyper-V	Groupe de séc	Les membres de ce grou

Nous irons dans les membres et nous supprimerons les utilisateurs authentifié

Nom	Dossier Services de domaine Active Directory
👫 Utilisateurs au	AUTORITE NT
Ajouter S	upprimer

Tout en restant dans le même endroit dans « user » nous pouvons retrouvé « utilisateur du schéma » qui permet de modifier, créer ou supprimer des objets sur les serveurs donc lorsque nous n'avons pas besoin d'y toucher nous pouvons supprimé l'administrateur local et si nous aurons besoin de modifier quelque chose, il suffira de le rajouter a nouveau.

_							
Utilisateurs et ordinateurs Active	Nom			Туре	Description		
<ul> <li>&gt; ☐ Requêtes enregistrées</li> <li>&gt; ∄ pologne.local</li> <li>▲ Administrateur</li> <li>▲ Administrateurs clés</li> </ul>		[		Utilisateur Groupe de séc	Compte d'utilisateur d'a Les membres de ce grou		
	Administrateurs clés Enterprise	Propriétés de : Admin	istrateurs du	schéma	?	2	×
<ul> <li>Computers</li> <li>Domain Controllers</li> <li>EoreignSecurityPrincipale</li> </ul>	Administrateurs de l'entreprise Administrateurs DHCP	Général Membres Membre de Géré par					
Managed Service Accourt	administrateurs du schéma	Membres :					
> 🖹 pologne	iologne & Admins du domaine Jsers & Contrôleurs de domaine	Nom	Dossier Serv	vices de domaine Acti	ve Directory		
	Contrôleurs de domaine clonables		pologne.loca				

Encore une fois dans les « user » nous pouvons trouvé « protected user » qui est l'endroit ou l'on peut mettre tous les administrateur nominatif ou bien les utilisateurs sensible, ce groupe permet de ne pas enregistré dans le cache le mot de passe lors de la connection. Dans notre cas nous allons ajouté notre administrateur local.

Il faut faire attention aussi lorsqu'un utilisateur protéger veux se connecter en bureau a distance il est possible qu'il doit écrire le nom complet du serveur donc : nom du srv « . » le domaine

Administrateurs DHCP	Cititititi	Hombro do Goro par			
🎕 Administrateurs du schéma	Membres :				
🄁 Admins du domaine	New	Dession Consistent de dem			
🔁 Contrôleurs de domaine	Nom	Dossier Services de dom	name Active Director	у	
🗱 Contrôleurs de domaine clonables	Administrateur	pologne.local/Users			
🗟 Contrôleurs de domaine d'entreprise en l					
🗟 Contrôleurs de domaine en lecture seule					
🔁 DnsAdmins					
🔁 DnsUpdateProxy					
🗟 Éditeurs de certificats					
🗟 Groupe de réplication dont le mot de pas					
🗱 Groupe de réplication dont le mot de pas					
😓 Invité					
🔁 Invités du domaine					
🗟 Ordinateurs du domaine					
Ropriétaires créateurs de la stratégie de					
Rotected Users					
😤 Serveurs RAS et IAS	Ajouter	Supprimer			
🔁 Utilisateurs DHCP					
🗟 Utilisateurs du domaine					
			OK	Annuler	Appliquer

Pour continuer le durcissement de notre serveur, nous pouvons allé dans la gestion des stratégie de groupe et ajouté un GPO nommé « désactiverNTLM » qui vas nous désactivé les anciens protocoles d'authentification (NTLM v1 et v2), il est d'abord nécessaire de vérifier qu'aucun logiciel n'utilise ce protocole avant de le désactiver

🛃 Gestion de stratégie de groupe	Utilisa	teurs					
✓ ▲ Forêt : pologne.local	Objets	de stratégie de groupe liés	Héritage de stratégie de groupe	Délégation			
✓ A Domaines	l 1	~					
🗸 🙀 pologne.local		Ordre des liens	Objet de stratégie de groupe	F	ppliqué	Lien activé	État GPO
🛒 Default Domain Policy	会	1	🛒 deploiementimprimante	1	lon	Oui	Activé
🗸 📴 Domain Controllers							
🛒 Default Domain Controllers I							
🗸 💼 pologne	$\nabla$						
> 🖬 Groupes							
> 📓 Ordinateurs	¥						
> 🖬 Utilisateurs							
> 📑 Objets de stratégie de groupe			Nouvel obiet GPO				×
> 📴 Filtres WMI			·····,-···				
> 🧊 Objets GPO Starter			Nom :				
> 📑 Sites			DésactiverNTLM				
👸 Modélisation de stratégie de groupe			· · ·				
Résultats de stratégie de groupe			Objet Starter GPO sour	ce :			
			(aucun)				~
						OK	Annuler

Pour vérifier si il nous reste de l'authentification via NTLM, nous pouvons laisser tourner la stratégie de groupe qui permet d'audité toute les authentifications NTLM pendant 15 jours a 1 mois afin d'être sur qu'il n'y a aucune trace du NTLM dans l'observateur d'événement.



Dès lors ou nous n'avons plus de trace de cette authentification nous pouvons a présent la restreindre



### **Conclusion :**

TP effectuer sans la réinitialisation du mdp Kerberos car l'utilisateur krbtgt n'était pas présent dans les utilisateurs de l'AD sinon a part ça aucun soucis rencontrer.

Gestion de l'authentification local LAPS :

**Introduction :** 

TP:

Pour débuter, nous allons voir le niveau fonctionnel de notre domaine est assez élever. Dans les utilisateur active directory nous faisons un clique droit sur le domaine et cliquons « augmenter le niveau fonctionnel du domaine » Notre serveur a un niveau fonctionnel de 2016 ce qui est le maximum a la date du tp.

> 💻	Kequetes enregistrees
× 📖	Délégation de contrôle
	Rechercher le mot de passe de récupération BitLocker
>	Rechercher
>	Changer de domaine
>	Changer de contrôleur de domaine
~	Augmenter le niveau fonctionnel du domaine

Augmenter le niveau fonctionnel du domaine

 $\times$ 



Quand nous allons dans les propriétés d'un ordinateur nous pouvons voir l'onglet LAPS qui n'est pas encore paramétrer

Pro	priétés de :	W10-V-	CLIENT-I	LG					?		$\times$
	Emplaceme	nt	Géré	par	Ap	pel entrant		Récupération	BitL	ocker	
	Général Solution du Expiration a Définir l'exp mardi Nom du co Mot de pas	Systemot de participactuelle de piration de mars mpte d'ar ese du co	ème d'exp passe de l' du mot de lu nouvea 18, 20; administrat	loitation administra passe LA u mot de p 25 11:59 eur local I dministrate	ateur loc PS : LAPS : eur loca	APS :	E	Délégation		LAPS	
			[	OK		Annuler		Appliquer		Aide	

La première étape du paramétrage du schéma active directory sera lancer une fenêtre powershell en administrateur



La commande a utilisé pour mettre a jours est « Update-LapsADSchema ». Il faut bien attendre que tout les serveurs en replication, on leur replication a jour. Nous voyons que nous avons pas les droits.

$\widetilde{\mathfrak{a}}$ 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 est « O ») : o
AVERTISSEMENT : Add request for 'CN=ms-LAPS-Password,CN=Schema,CN=Configuration,DC=pologne,DC=local' threw exception:
AVERTISSEMENT : System.DirectoryServices.Protocols.DirectoryOperationException: L'utilisateur ne dispose pas de droits
d'accès suffisants.
à System.DirectoryServices.Protocols.LdapConnection.ConstructResponse(Int32 messageId, LdapOperation operation,
ResultAll resultType, TimeSpan requestTimeOut, Boolean exceptionOnTimeOut)
à System.DirectoryServices.Protocols.LdapConnection.SendRequest(DirectoryRequest request, TimeSpan requestTimeout)
à Microsoft.Windows.LAPS.UpdateLapsADSchema.AddSchemaAttribute(String schemaAttributeDN, LAPSSchemaAttribute
lapsSchemaAttribute)
Update-LapsADSchema : L'utilisateur ne dispose pas de droits d'accès suffisants.
Au caractere Ligne:1 : 1
+ Update-LapsAUSchema
+ NARANANANANANANA
+ CategoryInto : Notspecified; (:) [Update-LapsADSchema]; DirectoryOperationException
datalang/DEFitederroru - System.Directoryservices.Protocols.Directoryoperationexception, Microsoft, Windows.LAPS.up
PS (·\llsens\Administrateur)

Pour y remédier, il nous suffit de rajouter l'administrateur dans les administrateurs du schéma

🗙 🏥 pologne local					ounsateur	compre a aunsarear a am		
Builtin	Kadministrateurs clés				Groupe de séc	Les membres de ce arou		
	Administrateurs clés Enterprise	Propriétés de : Administrateurs du schéma ?						
Domain Controllers	👫 Administrateurs de l'entreprise							
EoreignSecurityPrincipal	Administrateurs DHCP	Gén	éral Membr	es	Membre de Géré par			
Managed Service Accourt	🌉 Administrateurs du schéma	Me	embres :					
	🕮 Admins du domaine				Destine Consistent de domaios	Astive Dimeters		
Groupes	a Contrôleurs de domaine		Nom		Dossier Services de domaine	Active Directory		
G Ordinateurs	a Contrôleurs de domaine clonables	1	🐁 Administrat	teur	pologne.local/Users			
RDS	🧟 Contrôleurs de domaine d'entreprise en lectu							
> 📓 Utilisateurs	A Contrôleurs de domaine en lecture seule							
Serveur	A DnsAdmins							
📔 Users	A DnsUpdateProxy							
	A Éditeurs de certificats							
	🚇 Groupe de réplication dont le mot de passe R							
	🚇 Groupe de réplication dont le mot de passe R							
	Invité							
	🚇 Invités du domaine							
	🕮 Ordinateurs du domaine							
	Ropriétaires créateurs de la stratégie de grou							
	Reprotected Users							
	Serveurs RAS et IAS		Aiouter		Supprimer			
	at Utilisateurs DHCP	1.5						
	a Utilisateurs du domaine							
						OK Annuler	Applic	quer

Nous voyons que nous n'avons plus d'erreur, nous pouvons mettre « t » pour dire oui a tout



Après il ne faut pas oublier de supprimer a nouveau l'administrateur dans les administrateurs du schéma

énéral I	Membres	Membre de	Géré par				
Membres	:						
Nom		Dossier S	ervices de don	naine Active Direc	ctory		
Adm 💍	inistrateur	pologne.lo	ocal/Users				
							1
	Services	de domaine	Active Direct	ory		×	
	Services	de domaine	Active Direct	tory		×	
	Services	de domaine Voulez-vou	Active Direct	ory e ou les membro	es sélectionnés	× du	
	Services	de domaine Voulez-vou groupe ?	Active Direct	ory e ou les membro	es sélectionnés	× du	
	Services	de domaine Voulez-vou groupe ?	Active Direct	ory e ou les membro	es sélectionnés	× du	
	Services o	de domaine Voulez-vou groupe ?	Active Direct	e ou les membro Oui	es sélectionnés	du	
	Services o	de domaine Voulez-vou groupe ?	Active Direct	e ou les membro Oui	es sélectionnés	du	
	Services o	de domaine Voulez-vou groupe ?	Active Direct	e ou les membro Oui	es sélectionnés	du	
Ajoute	Services o	de domaine Voulez-vou groupe ? Supprimer	Active Direct	e ou les membro Oui	es sélectionnés	du	

La mise a jour du schéma nous affiche maintenant dans l'éditeur d'attribut nous pouvons voir maintenant les attribut « msLAPS »

msimaging-Thumbprn	<non defini=""></non>
msLAPS-EncryptedD	<non défini=""></non>
msLAPS-EncryptedD	<non défini=""></non>
msLAPS-EncryptedP	<non défini=""></non>
msLAPS-EncryptedP	<non défini=""></non>
msLAPS-Password	<non défini=""></non>
msLAPS-PasswordEx	<non défini=""></non>
CHOD: 1	1205.05

Le paramétrage a été effectué, la deuxième étape est l'administration via stratégie de groupe ou nous allons créé un GPO sur l'UO ordinateur. Je l'ai nommé « LAPS-activation ».



Nous la modifions et allons dans config ordi -> stratégie -> modèles d'administration -> Système -> LAPS



Vue que notre LAPS n'est que installé pour le moment. Il faudra donc l'activer, pour l'activer nous activerons « configurer le répertoire de sauvegarde de mot de passe » et choisissons ou stocker. Dans notre cas ce sera active directory car nous somme en local

🥵 Configurer le répertoire de sauvegarde de mot de passe — 🛛 🔿 🗙						$\times$
Configurer le rép	pertoire de sauvegarde	de mot de passe	Paramètre précédent	Paramètre su	ivant	
O Non configuré	Commentaire :					^
Activé						
○ Désactivé						~
	Pris en charge sur :	Au moins Microsoft Wi	ndows 10 ou version ultérieur	e		^
						~
Options :		Aide :				
Répertoire de sauves Active Directory	garde V	Utilisez ce mot de p Les paran	e paramètre pour configurer le asse du compte d'administrat nètres autorisés sont :	e répertoire dar eur local est sa	ns lequel le uvegardé.	-
		0=Desact	ive (le mot de passe ne sera pa jarder le mot de passe dans A:	as sauvegarde) zure Active Dire	ectory	
		2=Sauveg	jarder le mot de passe pour A	ctive Directory		
		Si ce para (Désactiv	mètre n'est pas spécifié, la val é).	leur par défaut	est 0	
		Si ce para joint à Az local n'es	mètre est configuré sur 1 et q ure Active Directory, le mot de t pas géré.	ue l'appareil ge e passe de l'adi	éré n'est pa ministrate	as ur
		Si ce para joint à Ac n'est pas	mètre est configuré sur 2 et q tive Directory, le mot de passe géré.	ue l'appareil ge e de l'administ	éré n'est p rateur loca	as I <sup>I</sup> Açti
			ОК	Annuler	Appliq	<b>uer</b> ind

Par rapport a la configuration nous pouvons choisir l'option « nom du compte administrateur à gérer ». en l'activant nous pourrons rentré le nom que l'on a donner aux comptes administrateur sur les postes. Dans notre cas ça ne sera pas utile.

Nom du compte	e administrateur à gére		— [	- X
📷 Nom du compte	administrateur à gérer	Paramètre précédent Param	iètre suivar	nt
<ul> <li>Non configuré</li> <li>Activé</li> <li>Désactivé</li> </ul>	Commentaire : Pris en charge sur :	Au moins Microsoft Windows 10 ou version ultérieure		~
Options :		Aide :		
Nom du compte adr	ninistrateur	Ce paramètre de stratégie spécifie un nom de Administrateur personnalisé pour lequel gérer Si ce paramètre de stratégie est activé, LAPS gé d'un compte local portant ce nom. Si ce paramètre de stratégie est désactivé ou s' configuré, LAPS gère le mot de passe du comp connu. NE PAS activer ce paramètre de stratégie pour administrateur intégré. Le compte Administrat automatiquement détecté par un SID connu et nom du compte. Pour plus d'informations, consultez https://go.microsoft.com/fwlink/?linkid=2188	compte le mot de j ire le mot d il n'est pas ste Admini gérer le co ceur intégré t ne dépend 435.	passe. de passe strateur mpte é est d pas du Activel Accédez Wind bw
		OK Ann	uler	Appliquer

Pour sécuriser le stockage des mots de passe dans active directory, nous activons le chiffrement des mot de passe

🕵 Activer le chiffre	ment du mot de passe	— 🗆 X
📑 Activer le chiffre	ement du mot de passe	Paramètre précédent Paramètre suivant
🔿 Non configuré	Commentaire :	^
Activé		
○ Désactivé		×
	Pris en charge sur :	u moins Microsoft Windows 10 ou version ultérieure
Options :		Aide :
		Lorsque vous activez ce paramètre, le mot de passe managé est chiffré avant d'être envoyé à Active Directory.         L'activation de ce paramètre n'a aucun effet, sauf si 1) le mot de passe a été configuré pour être sauvegardé dans Active Directory et 2) le niveau fonctionnel du domaine Active Directory et 2) le niveau fonctionnel du domaine Active Directory et 2) le niveau fonctionnel du domaine Active Directory et 2) le niveau fonctionnel du domaine est supérieur ou égal à Windows Server 2016, le mot de passe du compte géré est chiffré.         Si ce paramètre est activé et que le niveau fonctionnel du domaine est supérieur ou égal à Windows Server 2016, le mot de passe du compte géré n'est pas sauvegardé dans l'annuaire.         Si ce paramètre est activé, le mot de passe du compte géré n'est pas sauvegardé dans l'annuaire.         Si ce paramètre est désactivé, le mot de passe du compte géré n'est pas chiffré.         Ce paramètre est activé par défaut s'il n'est pas configuréActive
		OK Annuler Appliquer

Si nous activons l'option ci-dessus, il faudra alors dire qui pourra les déchiffrer grâce à « configurer les déchiffreur de mot de passe autorisés » par defaut ce sont les admin du domaine si nous ne l'activons pas

🜉 Configurer les déchiffreurs de mot de passe autorisés 🛛 👘 🗘					
📷 Configurer les d	échiffreurs de mot de p	asse autorisés Paramètre précédent Paramètre	e suivant		
Non configuré	Commentaire :			^	
Active					
<ul> <li>Désactivé</li> </ul>	Pris en charge sur :	Au moins Microsoft Windows 10 ou version ultérieure		* *	
Options :		Aide :			
Déchiffreur de mot d	de passe autorisé	Configurez ce paramètre pour contrôler l'utilisateu         spécifique autorisé à déchiffrer les mots de passe d         La configuration de ce paramètre n'a aucun effet,         chiffrement de mot de passe a été activé.         Si ce paramètre est activé, les mots de passe chiffr         déchiffrables par le groupe spécifié.         Si ce paramètre est désactivé ou n'est pas configu         passe chiffrés sont déchiffrables par le groupe d'au         de domaine.         Ce paramètre doit être configuré avec un SID au fr         « S-1-5-212127521184-1604012920-1887927527-35         nom d'un groupe ou d'un utilisateur au format « c         \(groupe ou utilisateur) ». L'utilisateur ou le group         être résolu par l'appareil géré, sinon les mots de passe sauvegardés.         Consultez https://go.microsoft.com/fwlink/?linking	rr ou le group chiffrés. sauf si le és seront ré, les mots d dministrateur ormat chaîne 197 ») ou le Jomaine le spécifié doi asse ne seron d=2188435	e s ( it	
		OK Annule	r Applio	uer	

En cas de restauration d'un poste client activer l'historique de mot de passe serait judicieux afin d'avoir encore les anciens mot de passe. La taille de l'historique sera juste le nombre de mot de passe retrouvable dans l'historique.

Configurer la taille de l'historique des mots de passe chiffrés – 🛛 🗙						×	
📷 Configurer la tai	lle de l'historique des r	nots de passe chiffrés	Paramètre	précédent	Paramètre su	iivant	
🔿 Non configuré	Commentaire :						~
Activé							
🔿 Désactivé							~
	Pris en charge sur :	Au moins Microsoft	Windows 10 ou v	ersion ultérieur	re		^
							~
Options :		Aide :					
Taille de l'historique	du mot de passe chiffr	é Utilise passe La cor de pas Active Si ce p plus a Si ce p de pas Ce pal passe. Pour p https;	c ce paramètre po chiffrés précéden figuration de ce ; se a été configure Directory et 2) le aramètre est activ cciens sera stocké aramètre est désa se plus ancien ne amètre a une vale amètre a une vale lus d'informatior /go.microsoft.co	ur configurer li ts stockés dans paramètre n'a a 5 pour être sauv chiffrement de ré, le nombre sj 6 dans Active Di octivé ou n'est p sctivé ou n'est p sctiv	e nombre de m Active Directo vegardé sur e mot de passe pécifié de mots irectory. pas configuré, i ns Active Direc utorisée de 0 m utorisée de 12 n id=2188435.	iots de ry. f si 1) le m a été activ s de passe aucun mo tory. iot de pas mots de	not vé. 2 ot ;se.
				ОК	Annuler	Applie	quer

Passons au paramètre de la spécificité du mot de passe, nous l'activons et prenons « lettres majuscule + lettres minuscule + chiffre + cara spéciaux » la longueur nous la définissons sur 12 afin d'être dans les norme. L'age dépendera de la politique de la boite.

Paramètres du m	not de passe		— D X
📑 Paramètres du m	not de passe		Paramètre précédent Paramètre suivant
<ul> <li>Non configuré</li> <li>Activé</li> <li>Désactivé</li> </ul>	Commentaire : Pris en charge sur :	Au moins M	icrosoft Windows 10 ou version ultérieure
Options :			Aide :
Complexité du mot d Lettres majuscules + Longueur du mot de Âge du mot de passe	e passe lettres minuscules + o passe 12 (jours) 30	chiffres + spé	Configure les paramètres de mot de passe Complexité des mots de passe : quels caractères sont utilisés lors de la génération d'un nouveau mot de passe Par défaut : lettres majuscules + lettres minuscules + chiffres + caractères spéciaux Longueur du mot de passe : Minimum : 8 caractères Défaut : 14 caractères Âge du mot de passe en jours Minimum : 1 jour (7 jours lorsque le répertoire de sauvegarde est configuré pour être Azure AD) Maximum : 30 jours Par défaut : 30 jours Pour plus d'informations, consultez https://go.microsoft.com/fwlink/?linkid=2188435.
			OK Annuler Appliquer

La dernière étape sera l'autorisation aux utilisateurs de changer leurs mot de passe et de le communiquer a active directory. Pour cela nous ouvrons a nouveau une fenêtre powershell en admin et rentrons la commande « Set-LapsADComputerSelfPermission -Identity "OU=Ordinateurs,OU=GA,DC=geek-advisor,DC=local" »