Mireille GUETCHO YOMPA

DÉPLOYER ET CONFIGURER MICROSOFT LAPS

SOMMAIRE

I – Définition et les fonctionnalités de LAPS II – Les prérequis de LAPS III – Mise en place de LAPS dans un service de domaine Active Directory IV – La configuration de la GPO LAPS

I -Définition et fonctionnalités de LAPS

LAPS, pour **Local Administrator Password Solution**, est un outil gratuit proposé par Microsoft et qui va venir se greffer sur le domaine Active Directory pour renforcer la sécurité des comptes " Administrateur " locaux de vos postes de travail et serveurs.

L'objectif étant mieux gérer les identités sur les machines de votre système d'information afin de renforcer la sécurité.

La solution Microsoft LAPS va offrir aux administrateurs systèmes des fonctionnalités clés afin de gérer le mot de passe des comptes administrateurs locaux des machines :

- Générer des mots de passe uniques et robustes pour chaque compte administrateur local
- > Définir la durée d'expiration des mots de passe associés à ces comptes
- > Définir la complexité des mots de passe associés à ces comptes
- Régénérer automatiquement un mot de passe quand il expire

II – Les prérequis de LAPS

Afin de pouvoir déployer la solution Microsoft LAPS, vous devez disposer d'un annuaire Active Directory et utiliser les versions de Windows (desktop) et Windows Serveur prise en charge.

Pour la suite de ce TP, vous avez besoin de deux machines au minimum, à savoir :

- . Un contrôleur de domaine Active Directory
- . Un poste de travail sous Windows

Pour ma part je vais utiliser les deux machines virtuelles suivantes : Serveur (DC)

- . Contrôleur de domaine Active Directory pour "btssio.fr"
- . Système d'exploitation : Windows serveur 2022 standard
- . Adresse IP : 10.75.19.10/24

PC -01

- . Poste client intégré au domaine AD et à gérer avec LAPS
- . Système d'exploitation : Windows 11
- . Adresse IP : 10.75.19.101

III - Mise en place de LAPS dans un service de domaine Active Directory

Avant de commencer, téléchargeons LAPS gratuitement sur le site de Microsoft : nous devons télécharger à minima "**LAPS.x64.msi** " pour les machines 64 bits et " **LAPS.x86.msi** " pour les machines de 32 bits, en fonction des besoins.

□ LAPS_TechnicalSpecification.docx 71.0 KB □ LAPS.ARM64.msi 1.1 MB ☑ LAPS.x64.msi 1.1 MB ☑ LAPS.x64.msi 1.1 MB ☑ LAPS.x86.msi 1.0 MB □ LAPS_OperationsGuide.docx 626.3 KB	Choose the download you want	×	
□ LAPS.ARM64.msi1.1 MB✓ LAPS.x64.msi1.1 MB✓ LAPS.x86.msi1.0 MB□ LAPS_OperationsGuide.docx626.3 KB	LAPS_TechnicalSpecification.docx	71.0 KB	l
 ✓ LAPS.x64.msi 1.1 MB ✓ LAPS.x86.msi 1.0 MB □ LAPS_OperationsGuide.docx 626.3 KB 	LAPS.ARM64.msi	1.1 MB	l
 ✓ LAPS.x86.msi 1.0 MB ☐ LAPS_OperationsGuide.docx 626.3 KB 	✓ LAPS.x64.msi	1.1 MB	l
LAPS_OperationsGuide.docx 626.3 KB	✓ LAPS.x86.msi	1.0 MB	ļ
	LAPS_OperationsGuide.docx	626.3 КВ	

1 – Installation de LAPS

Sur le contrôleur de domaine, nous allons installer les outils de gestion LAPS. Cela pourrait être installé sur un autre serveur où vous avez les outils d'administration Active Directory installés.

Exécutons le package MSI correspondant à la version de votre serveur :

32 bits ou 64 bits. Vous allez voir, l'installation est simple et s'effectue en quelque clics..... Cliquez sur " **Next** ".



Cochons l'option " I accept the terms in the license Agreement " et cliquez sur " Next ".

🖟 Local Administrator Password Solution Setup —		×
End-User License Agreement		
Please read the following license agreement carefully		2
MICROSOFT SOFTWARE LICENSE TERMS		^
MICROSOFT LOCAL ADMINISTRATOR PASSWORD SOLUTION		
These license terms are an agreement between Microsoft Corporat (or based on where you live, one of its affiliates) and you. Please ro them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft	tion ead	
updates,		~
☑ I accept the terms in the License Agreement		
Print Back Next	Cance	el

Ensuite, vous devez installer tous les outils d'administration (comme sur l'image ci-dessous) et nous devons désélectionner l'entrée " **AdmPwd GPO Extention** " car elle n'est pas utile sur le contrôleur de domaine.

En fait, le composant " **AdmPwd GPO Extension** " doit être déployé sur l'ensemble des machines à gérer via LAPS.

🕼 Local Administrator Password Solution Setup	- 🗆 🗙
Custom Setup Select the way you want features to be installed.	
Click the icons in the tree below to change the way	y features will be installed.
AdmPwd GPO Extension Management Tools Fat dient UI PowerShell module GPO Editor templates	Installs management tools. This component does not need to be installed on managed machines. It is meant to be installed on admin or user machines This feature requires 0KB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 217KB on your hard drive.
<u> </u>	Browse
Reset Disk Usage	Back Next Cancel

Voici l'utilité des différents outils de gestion :

- > Fat client UI : Outil graphique pour la gestion de LAPS
- > PowerShell module : Commande PowerShell pour LAPS
- > GPO Editor templates : Modèle ADMX de LAPS

😥 Local Administrator Password Solution Setup 🛛 —	
Ready to install Local Administrator Password Solution	
Click Install to begin the installation. Click Back to review or change any of y installation settings. Click Cancel to exit the wizard.	our
Back Install	Cancel



La première étape est faite, passons à la suite.

2 - Présentation de l'Active Directory pour LAPS

La phase de préparation de l'Active Directory se déroule en plusieurs sous-étapes, dont voici la liste d'aperçu de ce que nous allons faire :

- Mettre à jour le schéma de Active Directory
- Déléguer l'accès à certains objets " computers " pour qu'ils puissent mettre à jour le mot de passe et la date d'expiration dans l'annuaire Active Directory
- ➢ Gérer les permissions par défaut / actuelles
- Autoriser certains utilisateurs ou groupes de sécurité à lire les mots de passe
- Autoriser certain utilisateurs ou groupes de sécurité à réinitialiser le mot de passe d'un ordinateur

A – Mise à jour le schéma Active Directory

Ouvrez une console **Windows Powershell** sur votre contrôleur de domaine. Il faut que ce soit un contrôleur de domaine en écriture (donc pas un simple serveur !!!) et qu'il dispose du rôle FSMO "**Maître de schéma** " puisque l'on va modifier le schéma Active Directory.

Si nous avons besoins de localiser le contrôleur de domaine qui dispose du rôle FSMO, voici une commande Powershell qui nous donnera la réponse : " Get-ADForest | Select-Object Name, SchemaMaster "



Cette modification du schéma Active Directory va ajouter deux attributs au sein des objets de la class " **computers** " :

- ms-MCS-AdmPwd : Stocker le mot de passe en clair
- > ms-MCS-AdmPwdExpirationTime : stocker la date d'expiration du mot de passe

Exécutons la commande **Import-module Admpwd. PS** pour importer le module PowerShell de LAPS :

Ensuite, exécutons

PS C:\Users\Administrateur> Import-module AdmPwd.PS PS C:\Users\Administrateur> 🗕

Ensuite, exécutons la commande **Update-AdmPwdADSchema** pour mettre à jour le Schéma de AD :



Si nous ouvrons la console " **Utilisateur et ordinateurs Active Directory** " et que nous regardons les propriétés d'un ordinateur membre du domaine, on peut voir la présence de deux nouveaux attributs. Voici un exemple :

iénéral	Systè	me d'expl	oitation	Mem	bre de	Délé	gation	Répl	licatio	on de r	not de	pa
Emplace	ment	Géré p	ar O	bjet	Sécu	rité	Appel	entrant	t	Édite	ur d'att	trik
Attributs Attribut	:		Valeur						^			
msDS- msDS- msDS- msExch msExch	Source Support Sync Sei Assista House	DbjectDN edEncr rverUrl intName Identifier	<non dé<br="">0x1C = (<non dé<br=""><non dé<br=""><non dé<="" td=""><td>fini> (RC4_I fini> fini> fini></td><td>HMAC_I</td><td>MD5 A</td><td>ES128<u>.</u></td><td>_CTS_I</td><td></td><td></td><td></td><td></td></non></non></non></non>	fini> (RC4_I fini> fini> fini>	HMAC_I	MD5 A	ES128 <u>.</u>	_CTS_I				
msExch msIIS-F msIIS-F msImag msImag	TPDir TPDir TPRoo jing-Has jing-Thu	dURI t shAlgor	<non dé<br=""><non dé<br=""><non dé<br=""><non dé<br=""><non dé<="" td=""><td>tini> fini> fini> fini> fini></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></non></non></non></non></non>	tini> fini> fini> fini> fini>								
ms-Mcs ms-Mcs mSMQI	s-AdmPo s-AdmPo Digests	wd wdExpi	<non dé<br=""><non dé<br=""><non dé<="" td=""><td>fini> fini> fini></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></non></non></non>	fini> fini> fini>								
< <	Digests	DIID	<non de<="" td=""><td>fini></td><td></td><td></td><td></td><td>></td><td></td><td></td><td></td><td></td></non>	fini>				>				
Modi	fier							Filtrer				

B – Attribuer les droits d'écriture aux machines

Les machines qui doivent être managées via LAPS ont besoin de mettre à jour les attributs **ms-MCS-AdmPwdExpirationTime** et **ms-MCS-AdmPwd** au sein de notre annuaire Active Directory. Sinon, il ne sera pas possible de stocker dans l'Active Directory la date d'expiration et le mot de passe.

Le module LAPS de PowerShell contient un cmdlet pour réaliser cette action. Pour l'utiliser, c'est tout simple nous devonsidiquer le nom de l'OU cible. Pour nous, nous ciblons l'OU "**Ordinateur**" (visible sur la copie d'écran ci-dessus) car elle contient les machines que je souhaite gérer avec LAPS. Nous recommandons de préciser le **DistinguishedName** de l'OU pour être sûr de cibler la bonne OU, sauf s'il n'y en a qu'une seule qui a ce nom.

La commande est **Set-AdmPwdComputerSelfPermission -OrgUnit** "OU=PC,DC=iticsio2,DC=fr"

Nous devons obtenir un retour dans la console avec le statut " Delegated "



C – Gérer les permissions par défaut / actuelles

En fonction de la configuration de votre annuaire Active Directory, certains utilisateurs ou groupes ont probablement les permissions pour lire les attributs étendus. Afin d'éviter que les attributs créés par LAPS soient accessibles par n'importe qui, nous devons contrôler et adapter les permissions. Nous devons **retirer les permissions aux utilisateurs/groupes qui ont accès aux attributs étendus** sur l'OU "**PC**", s'il y a des entrées correspondantes à des utilisateurs non habilités.

Plutôt que de parcourir les droits via l'interface graphique, on peut s'appuyer sur PowerShell pour visualiser quels sont les comptes qui ont un accès à ces attributs étendus. Pour ma part, je vais auditer l'OU "PC" qui contient mes postes à manager avec LAPS.



Voyons comment gérer cette permission.....

Ouvrons la console "**Modification ADSI**" puis effectuons un clic droit sur "**Modification ADSI**" afin de cliquer sur "**Connexion**". Une fenêtre s'ouvre... nous Laissons le choix par défaut, à savoir "**Contexte d'attribution de noms par défaut**" et après nous validons.

SCDN2 - [Racine de la console\Modification AD	511	_	σ×
Fichier Action Affichage Favoris Fenêti	e ?		- 5 ×
🔶 🖄 📰 🔯 🔽 📷			
Racine de la console		Actions	
Utilisateurs et ordinateurs Active Directory [DUCD	GCDN2.itic Éditeur ADSI	Modification ADSI	^
Schema Active Directory Gestion des stratégies de groupe Schema Active Directory 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 Paramètres de connexion	Autres actions	*
	Nom : Contexte d'attribution de noms par défaut Chemin d'accès : LDAP://SCDN2.iticsio2.fr/Contexte d'attribution de noms ; 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 ; Sélectionnez un contexte d'attribution de noms connu : Contexte d'attribution de noms par défaut Ordinateur Sélectionnez ou entrez un domaine ou un serveur : (Serveur Domaine [:port]) © Par défaut (le domaine ou le serveur auquel vous vous êtes connecté) Utiliser le chiffrement SSL Avancé OK		

Ensuite, nous parcourons l'Active Directory jusqu'à trouver l'**OU qui contient les ordinateurs managés par LAPS** (et donc qui vont venir écrire leur mot de passe). Effectuons un clic droit sur cette OU, pour ma part c'est l'OU "**PC**" et accédons aux propriétés via un clic droit.

SCDN2 - [Racine de la	a console\Modification ADSI\Contexte	e d'attribution de noms p	ar défaut [SCDN2.iticsio2	2.fr] \DC=iticsio2,DC=f	fr\OU=PC] -
Fichier Action A	ffichage Favoris Fenêtre ?				
🔿 🖄 📰 🗙	🗐 🖸 🚔 🔽 📷				
Racine de la console		Nom	Classe	Nom unique	Actions
Utilisateurs et ord	dinateurs Active Directory [SCDN2.itic	CN=CLIENT	computer	CN=CLIENT,OU=I	OU=PC
DHCP Domaines et app Gestion des stratu Gestion des stratu Gestion ACI: Modification ADI: Onderste d'at DC=iticsio CN=B CN=C OU=D OU=E OU=E OU=E OU=E OU=I OU=I	robations Active Directory égies de groupe irectory SI tribution de noms par défaut [SCDN2 o2,DC=fr uilitin :computers Jormain Controllers mployés oreignSecurityPrincipals IIC				Autres actions
CN=L CN=N CN=N	ostAndFound Aanaged Service Accounts ITDS Quotas				
> 🛄 OU: 📑 CN: 📑 CN:	Déplacer Nouvelle connexion à partir d'ici	1			
CN:	Nouveau	>			
	Affichage Nouvelle fenêtre à partir d'ici	>			
	Nouvelle vue de la liste des tâches	i			
	Supprimer Renommer Actualiser Exporter la liste				
	Propriétés			Ac	tiver Windov
	Aide			Ac	édez aux paramèt

Cliquez sur l'onglet "**Sécurité**" puis sur le bouton "**Avancé**". Ensuite, si l'on souhaite retirer les droits, par exemple sur le groupe "**Utilisateurs authentifiés**" (même si ici ils n'ont pas les droits, c'est un exemple...), il suffit de sélectionner "**Utilisateurs authentifiés**" dans la liste et cliquer sur le bouton "**Modifier**". Il ne reste plus qu'à décocher les droits "**Tous les droits étendus**".

Fichier Action Affichage Paramètres de sécur	Autorisations	pour PC			×
Racine de la console Utilisateurs et ordinateur Propriétaire : Propriétaire : Propriétaire : Propriétaire : Autorisations Gestion des stratégies de Schéma Active Directory Modification ADSI	Principal : Type : S'applique à :	Utilisateurs authentifiés Sélectionnez un principal Autoriser · Cet objet uniquement ·			
Contexte d'attributio DC-titicsio2DC= C.N.=Builtin OU=Domain OU=Employé C.N.=Foreigno C.N.=Keys C.N.=Keys C.N.=NTOS Qu OU=PTC C.N.=NTOS Qu OU=PTC C.N.=Prorgram C.N.=TPM Dev C.N.=Users DESCRET C.N.=Users	Autorisations :	Contrôle total Lister le contenu Lire toutes les propriétés Écrire toutes les propriétés Supprimer Supprimer la sous-arborescence Autorisations de lecture Modifier les autorisations Modifier les propriétaire Toutes les écritures validées Toutes les écritures validées Tous les droits étendus Créer tous les objets enfants Supprimer tous les objets enfants Créer des objets account	Suppr. des objets msDS-App-Configuration Créer des objets msDS-AppData Suppr. des objets msDS-ApApData Gréer des objets msDS-ApAdminManager Gréer des objets msDS-ApAdminManagedServiceAccount Suppr. des objets msDS-GroupManagedServiceAccount Gréer des objets msDS-ManagedServiceAccount Gréer des objets msDS-ManagedServiceAccount Gréer des objets msDS-ShadowPrincipalContainer Gréer des objets msSexChOnfigurationContainer Gréer des objets msieee80211-Policy Suppr. des objets msieee80211-Policy		Δctis

D – Ajouter des autorisations de lire le mot de passe LAPS

Au sein de l'annuaire Active Directory, je dispose d'un groupe nommé "**laps**" qui contient **tous les utilisateurs qui doivent être en mesure de lire le mot de passe laps** de chaque ordinateur (correspondant au compte Administrateur local de la machine).

Pour ajouter l'autorisation de lire le mot de passe, nous allons utiliser le cmdlet "**Set-AdmPwdReadPasswordPermission**" avec deux paramètres qui vont permettre de préciser l'OU (*-Identity*) et le nom du groupe (ou l'utilisateur) à autoriser (*-AllowedPrincipals*). Ce qui donne :

PS C:\Users∖Administrateur≻ <mark>Set</mark>	-AdmPwdReadPasswordPermission -Identity "Ol	J=PC,DC=iticsio2,DC=fr" -AllowedPrinci	
Name Distinguis	hedName	Status	
PC OU=PC,DC=i	ticsio2,DC=fr	Delegated	
PS C:\Users\Administrateur> _			

On obtient un retour dans la console avec le statut "Delegated "

Le tour est joué, passons à la suite.

E – Ajouter des autorisations de réinitialisation du mot de passe LAPS

En fonction de l'organisation du service informatique de l'entreprise, peut-être que les administrateurs et les techniciens du support sont différents, et qu'ils ont des autorisations différentes. On peut imaginer avoir **deux groupes pour les autorisations LAPS** : un groupe qui permet de lire le mot de passe et un second groupe qui permet en plus la réinitialisation du mot de passe. Dans le cadre de ce TP, nous allons continuer d'utiliser le groupe "**laps**".

Le cmdlet pour cette autorisation se nomme "**Set-AdmPwdResetPasswordPermission**" et il fonctionne comme le cmdlet précédent. Ce qui donne :

ame	DistinguishedName	Status	
	OU=PC,DC=iticsio2,DC=fr	Delegated	

On obtient un retour dans la console avec le statut "Delegated "

Les autorisations sont effectives et s'appliquent au groupe " LAPS "

ame	DistinguishedName	Status
C	OU=PC,DC=1t1cs1o2,DC=tr	Delegated
S C:\Users\/	Administrateur> Set-AdmPwdResetPasswordPermission -Id	lentity "OU=PC,DC=iticsio2,DC=fr" -AllowedPrincipals "laps"
S C:\Users\/ ame	Administrateur> Set-AdmPwdResetPasswordPermission -Id DistinguishedName	lentity "OU=PC,DC=iticsio2,DC=fr" -AllowedPrincipals "laps" Status

IV – Configuration de la GPO LAPS

La dernière étape de la configuration, avant que l'on déploie le client LAPS sur les postes de travail à gérer, consiste à créer une GPO de configuration de LAPS. Cette GPO va contenir différents paramètres, notamment pour activer la gestion du compte Administrateur avec LAPS, ou encore pour définir la complexité du mot de passe généré aléatoirement par LAPS.

1 – ADMX de LAPS

Nous devons commencer par **importer les fichiers ADMX de LAPS** sur notre contrôleur de domaine, à l'intérieur du dossier "**PolicyDefinitions**" (magasin central) puisqu'il sert à ajouter des modèles d'administration supplémentaires.

Pour récupérer le fichier ADMX et son fichier de langue ADML, nous devons aller sur le serveur où l'on a installé les outils d'administration de LAPS. Il y a un fichier à copier et a coller dans le fichier SYSVOL

> Ce	PC \rightarrow Disque local (C:) \rightarrow Windows \rightarrow Po	licyDefinitions >			 V Rechercher dans: PolicyDefini ク
^	Nom	Modifié le	Туре	Taille	^
	📜 en-US	21/10/2024 12:46	Dossier de fichiers		
	📜 fr-FR	07/08/2021 02:36	Dossier de fichiers		
ne 🛪	ActiveXInstallService.admx	08/05/2021 10:15	Fichier ADMX	5 Ko	
*	AddRemovePrograms.admx	08/05/2021 10:15	Fichier ADMX	5 Ko	
*	AdmPwd.admx	28/04/2021 13:56	Fichier ADMX	4 Ko	
	AllowBuildPreview.admx	08/05/2021 10:15	Fichier ADMX	2 Ko	
	AppCompat.admx	08/05/2021 10:15	Fichier ADMX	6 Ko	

Ensuite, nous pouvons passer à la configuration de la GPO.

2 – GPO pour LAPS

Pour créer la GPO, nous devons ouvrir la console d'édition des stratégies de groupe et créer une nouvelle GPO. Nous allons nommer cette GPO "LAPS-Config" et l'appliquer sur mon OU "PC". C'est important de lier la GPO sur cette OU "PC" (à adapter selon votre configuration, bien $s\hat{u}r$) et non sur une autre OU, car jusqu'ici nous avons géré les autorisations de LAPS sur cette OU.

Ensuite, modifons la GPO via un clic droit "Modifier" et parcourons les paramètres comme ceci :



Ce modèle d'administration pour LAPS contient 4 paramètres.Voici la signification de ces différents paramètres :

- Password Settings : définir la complexité du mot de passe, sa longueur et sa durée de vie

- Name of administrator account to manage : définir un compte administrateur à configurer autre que le compte Administrateur intégré à Windows. En effet, le compte Administrateur BUILT-IN est automatiquement détecté, grâce au SID (Identifiant de sécurité unique) même s'il est renommé. Si l'on cible le compte Administrateur intégré à Windows, il ne sera pas utile de configurer ce paramètre.

- **Do not allow password expiration longer than required by policy** : ne pas autoriser une expiration du mot de passe plus longue que le permet la stratégie définie au sein du paramètre "*Password settings*".

- Enable local admin password management : activer ou désactiver la gestion du mot de passe administrateur avec LAPS pour l'ordinateur cible.

LAPS			
Sélectionnez un élément pour obtenir	Paramètre	État	Commentaire
une description.	E Password Settings	Non configuré	Non
	E Name of administrator account to manage	Non configuré	Non
	E Do not allow password expiration time longer than required	Non configuré	Non
	Enable local admin password management	Non configuré	Non

Nous allons commencer par définir une stratégie de complexité des mots de passe via le paramètre "**Password Settings**". Avec la stratégie indiquée sur la copie d'écran ci-dessous, on obtient des mots de passe très complexes et qu'il sera très difficile de mémoriser. Par exemple, on peut obtenir « 6F5g@FRlb)1KE. »

	Password Setting	gs					_		×
	Password Setting	gs			Paramètre	précédent	Paramètre su	ivant	
	O Non configuré	Commentaire :							^
	Activé								
	O Désactivé								\sim
l		Pris en charge sur :	At least Mic	rosoft Windo	ws Vista or V	/indows Serve	er 2003 family		^
									\vee
	Options :			Aide :					
	Password Complexit	у		Configures	nassword pa	arameters			\neg
	Large letters + smal	l letters + numbers + s	pecials 🗸	Descuerde	omplovite	which charact	are are used when		
	Password Length	14		generating	a new passw	ord	ers are used when	.,	
	Password Age (Days	i) 30	•	characters	arge letters +	small letters	+ numbers + spe	ecial	
				Password l	ength				
				Minimum Maximum	: 8 character n: 64 characte	s ers			
				Default: 14	4 characters				
				Password a Minimum	ge in days : 1 day				
				Maximum Default: 3	n: 365 days) days				
					2.		Activer	Win	dov
	<		>				Accédez a	aux par	amjè
							activer W	indows	5.
ł						OK	Annuler	Appliq	uer

Ensuite, nous allons activer deux autres paramètres donc il suffit de les basculer sur l'état "Activé" : •

Enable local admin password management (indispensable pour activer LAPS)

Do not allow password expiration longer than required by policy

Do not allow pas	ssword expiration time	longer than	required by policy				\times
Do not allow pas	ssword expiration time	longer than	required by policy				
Paramètre précéder	nt Paramètre suiv	/ant					
○ Non configuré	Commentaire :						~
 Activé 							
○ Désactivé							\sim
	Pris en charge sur :	At least Mid	rosoft Windows Vista or W	indows Server 2003	family		~
							\sim
Options :			Aide :				
			When you enable this se longer than password ag is NOT allowed. When su changed immediately an to policy. When you disable or not expiration time may be I Settings" policy.	tting, planned pass e dictated by 'Pass ich expiration is det d password expirat configure this setti onger than required	word expi word Setti ected, pas ion is set i ng, passw ł by "Pass	ration ings" pol ssword is according vord word	icy g
			l	UK A	nnuier	Atpbi	quern

Le dernier paramètre ne sera pas configuré, car le compte "Administrateur" d'origine est utilisé sur mes postes de tests. Il conviendra de l'activer et le configurer en fonction de vos besoins. Vous pouvez fermer la GPO puisqu'elle est prête. Nous obtenons la configuration suivante :

📋 LAPS		
Sélectionnez un élément pour obtenir	Paramètre	État
une description.	E Password Settings	Activé
	Name of administrator account to manage	Non configuré
	🖹 Do not allow password expiration time longer than required	Activé
	Enable local admin password management	Activé

Pour finir, profitons d'être sur la configuration de la GPO pour désactiver le traitement des paramètres utilisateurs puisque cette GPO contient uniquement des paramètres ordinateurs. Effectuez un clic droit sur la GPO, puis sous "**Etat GPO**" cliquez sur "**Paramètres de configuration utilisateurs désactivés**".

APS-CONFIG	Interdit le Panne	au de Activé	Aucun(e)	10/ 11/	10/2024 03.43	Admins du domaine
Filtres WMI	LAPS-CONTRA	Modifier		06/	01/2025 17:33	Admins du domaine Admins du domaine
Objets GPO Starter	Lecteur Ré	État GPO			Activé	
lélisation de stratégie de groupe	Lecteur Re	Sauvegarder		~	Paramètres de	configuration utilisateurs désactivés
Iltats de stratégie de groupe ive Directory	Raccouci E	Restaurer à partir d' Importer des param	'une sauvegarde nètres		Paramètres de Tous les param	configuration ordinateurs désactivés tères désactivés

3 - Créer la GPO pour déployer le MSI de LAPS

Avant de commencer à créer la GPO, nous devons héberger le package MSI sur un partage, accessible au travers du réseau, depuis les postes clients qui doivent pouvoir installer ce package. La solution de faciliter consiste à utiliser le dossier "DC" du partage Script lié à l'Active Directory. De notre côté, nous déposerons le package MSI à l'endroit ci-dessous : notre chemin : <u>\\SCDN2\Docs\MSI</u>.

diteur de gestion des stratégies de groupe		$ \Box$ \times
🛃 📜 🗢 🛛 MSI		$ \Box$ \times
ier Accueil Partage Affichage		~ 😮
→ ~ 🛧 📜 > Réseau > SCDN2 > Docs > MSI	~ ご R	echercher dans : MSI 🔎
Photo ^ Nom ^	Modifié le	Туре
LAPS.x64	31/10/2024 13:15	Package Windows
System32		
Ce PC		
Bureau		
🖻 Documents		
🛋 Images		
Musique		
🧊 Objets 3D		
🕹 Téléchargement:		
📕 Vidéos		
Serlin (\\SCDN2)		
😓 Disque local (C:)		
🖆 Lecteur de DVD (
Londres (\\SCD)		
Paris (\\SCDN2\I		
Lecteur de DVD (C		
Réseau		
✓ <		>

A partir de la console de gestion des stratégies de groupe, nous allons créer une GPO nommée "**LAPS-Installation**" qui sera là en complément de la GPO "**LAPS-Config**" créée précédemment. Elle sera liée également à l'OU "Computer" puisque cette OU contient tous les PC que je souhaite gérer avec LAPS.

D'un point de vue technique, rien n'empêche d'utiliser la même GPO pour l'installation et la configuration. Pour utilisation d'une solution pour déployer les postes Windows, il faut penser à inclure l'installation de LAPS en ce moment afin de se passer de cette GPO d'installation.

Une fois la GPO créée, nous devons la modifiée comme suit :

Configuration ordinateur > Stratégies > Paramètres du logiciel > Installation de logiciel



Nous devons indiquer quel est le package MSI à déployer, alors accédons à notre partage et sélectionnez le MSI de LAPS. Validons... La fenêtre ci-dessous va apparaître. Sélectionnons "**Attribué**" et cliquez sur "**OK**".

Éditeur de gestion des stratégies de	Iroupe		_	×
Fichier Action Affichage ?				
Þ 🔿 🚈 📰 🗐 🚇 📔 E				
 Stratégie LAPS-Installation [SCDN2.1' Configuration ordinateur Stratégies Paramètres du logiciel Installation de logiciel Paramètres Windows Modèles d'administration Modèles d'administration Configuration utilisateur Stratégies Préférences Préférences 	Id Nom Version État du dég Aucun élément à a Déploiement du logiciel Sélectionnez le type de déploiement : Publié Attribué Attribué Sélectionnez cette option pour assigner l'application san modification.	ploie Source fficher dans cet aperçu. X Is Annuler		

Voilà, le package MSI est inclus à la GPO et prêt à être installé sur les postes ! Le mode "Attribué" permet d'utiliser les options par défaut, ce qui est satisfaisant pour l'installation de LAPS.

3 - Tester l'installation de LAPS sur une machine

Nous allons utiliser la machine "CLIENT", sous Windows 10, et qui appartient à l'OU "PC". Après avoir ouvert une session, nous devons faire une mise à jour des GPO à partir d'une console : nous allons utiliser cette commande **gpupdate** /**force** dans l'Invite de commande



Un avertissement s'affiche pour me dire que l'installation du logiciel s'effectue au redémarrage et il m'est proposé de redémarrer. Il suffit d'indiquer "**O**" et de **valider pour que la machine redémarre**.



Suite au redémarrage, si l'on regarde au sein des applications et fonctionnalités, on constate quelque chose d'intéressant : "**Local Administrator Password Solution**" apparaît dans la liste ! LAPS est installé sur cette machine et cela va suivre sur les autres machines de mon parc...



Puisque le client LAPS est déployé sur au moins une machine de notre parc et que la GPO de configuration de l'outil est en place, normalement il doit y avoir du changement du côté de l'Active Directory. Autrement dit, les attributs "ms-Mcs-AdmPwd" et "ms-Mcs-AdmPwdExpirationTime" ne doivent plus être vide.

4 - Afficher le mot de passe avec LAPS UI

A partir du menu Démarrer de votre serveur, vous pouvez trouver l'application "LAPS UI" à l'intérieur d'un dossier nommé "LAPS". Ce petit utilitaire est très pratique et va éviter d'utiliser la console Active Directory. Il va permettre d'afficher le mot de passe et la date d'expiration d'un ordinateur.

Faisons un essai avec notre PC client :

haps ui	×
Computer name: CLIENT	Search
Password:	
5JZdwzX7kK\$-CF	
Password expires: 06/02/2025 20:54:45]
New expiration time (leave as is for immediate expiration):	
vendredi 10 janvier 2025 14:04:45	Set
	Exit
	.:

Le mot de passe apparaît bien, et la date d'expiration est lisible du premier coup.

Merci là nous arrivons à la fin du TP, à bientôt pour un nouveau.