Table des matières

Pr	ésentation	3
1.	Configuration de BitLocker	5
	1 – Installation de la fonctionnalité BitLocker	5
	2 – Configuration de la GPO	7
	3 – Création d'un filtre WMI pour cibler Windows 11	10
	4 – Activer BitLocker manuellement sur un poste	10
	5 – Scripts et GPO pour activer automatiquement BitLocker sur les postes	12
	6 – Récupérer la clé de récupération	15
	7 - Vérification du fonctionnement de la clé de récupération	17
	8- Conclusion	17
2.	TROUBLESHOOTING	18

PRESENTATION

Dans le cadre de la sécurisation des postes et des données, on m'a demandé de mettre en place BitLocker.

BitLocker est une fonctionnalité intégrée à Windows, qui permet de chiffrer le contenu d'un disque dur.

Avant sa mise en place, on doit comprendre comment fonctionne BitLocker et plus précisément le rôle de la puce TPM :

Avec une puce TPM (Trusted Platform Module), BitLocker stocke les clés de chiffrement dans le matériel, offrant ainsi une sécurité renforcée et permettant le déverrouillage automatique au démarrage du système, après une vérification de l'intégrité.

Sans puce TPM, BitLocker peut toujours chiffrer les disques, mais nécessite un mot de passe ou une clé USB pour déverrouiller le volume chiffré lors du démarrage, ce qui peut être moins transparent mais toujours sécurisé.

La première étape est de regarder du côté de nos postes et d'identifier les postes qui ont des puces TPM et ceux qui n'en ont pas. De notre côté on doit avoir **70%** de postes avec une puce TPM et **30%** sans puce TPM.

Ensuite il faut déterminer quelles solutions adopter :

- Solution 1 : Mise en place de BitLocker uniquement pour les postes avec des puces TPM
- Solution 2 : Mise en place de BitLocker avec puce TPM et PIN pour les postes sans puces

À savoir BitLocker avec puce TPM est transparent pour l'utilisateur (sauf configuration contraire), alors qu'a l'inverse sans puce TPM cela demande aux utilisateurs de rentrer un deuxième mot de passe (PIN) en plus de leurs sessions avant l'ouverture de celles-ci.

Mais il est également possible de mettre en place BitLocker avec TPM et un PIN pour sécuriser davantage le poste.

À la suite des discussions avec les responsables informatiques, il a été convenu de prioriser le chiffrement des PC portables des utilisateurs avec BitLocker. L'implémentation d'un code supplémentaire n'étant pas souhaitée, la solution avec puce TPM sera privilégiée.

La solution adoptée est de mettre en place d'abord BitLocker avec les puces TPM sur les postes portables Windows 11. Sachant que les puces TPM sont un prérequis pour l'installation de Windows 11. La grande majorité des PC Portables sont sur W11.

Sachant que les utilisateurs peuvent être amené à faire du télétravail donc le risque de compromission des PC Portables est plus élevé, donc cela explique pourquoi vouloir prioriser ces équipements.

1. CONFIGURATION DE BITLOCKER

La mise en place de BitLocker via GPO va nous permettre de :

- Stocker les clés de récupération BitLocker dans l'Active Directory pour chaque ordinateur protégé par BitLocker
- Déployer uniformément BitLocker sur les postes
- Activer automatiquement la protection BitLocker sur les postes via un script
- 1 Installation de la fonctionnalité BitLocker

Sur le contrôleur de domaine dans le gestionnaire de serveur, installer ces fonctionnalités :

électionner des fonctionnalités		SERVEUR DE DESTINATION LARO, AD Jaho, avium		
Avant de commencer Type d'installation Sélection du serveur	Sélectionnez une ou plusieurs fonctionnalités à i Fonctionnalités	à i Ajouter les fonctionnalités requises pour Chiffrement de lecteur BitLocker ?		
Rôles de serveurs Fonctionnalités	Base de données interne Windows BranchCache Chiffrement de lecteur BitLocker	Vous ne pouvez pas installer Chiffrement de lecteur BitLocker sauf si les services de rôle ou les fonctionnalités suivants sont également installés.		
	Client d'impression Internet Client pour NFS Clustering de basculement Collection des événements de configura Compression différentielle à distance Containers Data Center Bridging Déverrouillage réseau BitLocker Direct Play Équilibrage de la charge réseau Expérience audio-vidéo haute qualité W Extension ISS Management Onets	Outils d'administration de serveur distant Outils d'administration de fonctionnalités Utilitaires d'administration de Chiffrement de lecteur B [Outils] Visionneuse des mots de passe de récupér [Outils] Outils de chiffrement de lecteur BitLocker Stockage étendu		
	Extension WirRM IIS Fonctionnalités de .NET Framework 3.5 Fonctionnalités de .NET Framework 4.7 (Inclure les outils de gestion (si applicable) Ajouter des fonctionnalités Annuler 		

Normalement après ça on a un nouvel onglet « Récupération BitLocker » dans les propriétés des postes

Onglet « Récupération BitLocker » :

General	Système d'exploi	tation	Membre de	Délégation	n LAPS
Emplacemen	t Géré pa	r /	Appel entrant	Récupér	ation BitLocker
Mots de passe	de récupération Bit	Locker :			
Date d'ajout		ID de mot	de passe		
Aucun élémen	t dans cette vue.				
Pour recherch	per un mot de passe	de récunér	ation cliques av	ec le houton	
droit sur l'objet	domaine dans l'arb	orescence,	puis sélectionne	z	
« Rechercher	le mot de passe de	récupératio	n BitLocker ».		
Détails :					
Détails :					
Détails :					
 Détails :					
Détails :					
Détails :					

C'est ici que la clé de récupération va apparaître.

2 – Configuration de la GPO

Sur le contrôleur de domaine je crée une nouvelle stratégie de groupe « BitLocker – TPM », celle-ci se situe à cet emplacement :

Dans Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Chiffrement de lecteur BitLocker

Configurer les paramètres suivants :

• Choose drive encryption method and cipher strenght (Windows 10 and later) – Activé, spécifie les méthodes de chiffrement à utiliser pour un lecteur, dans mon cas je choisis la méthode par défaut.

Paramètre précédent Paramètre suiva	ant
 Non configuré Commentaire : Activé Désactivé Pris en charge sur : 	At least Windows Server 2016 Windows 10
Options :	Aide :
Select the encryption method for operating drives: XTS-AES 128-bit (default) Select the encryption method for fixed data XTS-AES 128-bit (default) Select the encryption method for removable drives: AES-CBC 128-bit (default)	system This policy setting allows you to configure the algorithm and cipher strength used by BitLocker Drive Encryption. This policy setting is applied when you turn on BitLocker. Changing the encryption method has no effect if the drive is already encrypted, or if encryption is in progress. drives: If you enable this policy setting you will be able to configure an encryption algorithm and key cipher strength for fixed data drives, operating system drives, and removable data drives individually. For fixed and operating system drives, we recommend that you use the XTS-AES algorithm. For removable drives, you should use AES-CBC 128-bit or AES-CBC 256-bit if the drive will be used in other devices that are not running Windows 10 (Version 1511). If you disable or do not configure this policy setting, BitLocker will use AES with the same bit strength (128-bit or 256-bit) as the "Choose drive encryption method and cipher strength (Windows Vista, Windows Strere 2008, Windows 7)" and "Choose drive encryption method and cipher strength in that

Dans Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Chiffrement de lecteur BitLocker > Operating System Drives

- Enforce drive encryption type on operating system drives Activé, permet d'indiquer à BitLocker comment il doit chiffrer le disque, dans mon cas je le mets en « full encryption ».
- Choose how BitLocker protected operating system drives can be recovered Activé, permet d'indiquer aux postes qu'ils doivent stocker leurs clés de récupération dans l'AD et aussi de vérifier que la clé est bien stocké avant de commencer à chiffrer le disque. Choisir ces paramètres :

💭 Choose how BitLocker-protected operating system drives	can be recovered — — — — — — — — — — — — — — — — — — —
Choose how BitLocker-protected operating system drives	can be recovered Paramètre précédent Paramètre suivant
O Non configuré Commentaire : Activé O Désactivé	∧
Pris en charge sur : At least Windows	Server 2008 R2 or Windows 7
Options :	Aide :
Allow data recovery agent Configure user storage of BitLocker recovery information: Allow 48-digit recovery password Allow 256-bit recovery key Omit recovery options from the BitLocker setup wizard Save BitLocker recovery information to AD DS for operating system drives Configure storage of BitLocker recovery information to AD DS: Store recovery passwords and key packages D on ot enable BitLocker until recovery information is	This policy setting allows you to control how BitLocker-protected operating system drives are recovered in the absence of the required startup key information. This policy setting is applied when you turn on BitLocker. The "Allow certificate-based data recovery agent" check box is used to specify whether a data recovery agent can be used with BitLocker- protected operating system drives. Before a data recovery agent can be used it must be added from the Public Key Policies item in either the Group Policy Management Console or the Local Group Policy Editor. Consult the BitLocker Drive Encryption Deployment Guide on Microsoft TechNet for more information about adding data recovery agents. In "Configure user storage of BitLocker recovery information" select whether users are allowed, required, or not allowed to generate a 48-digit recovery password or a 256-bit recovery key. Select "Omit recovery options from the BitLocker setup wizard" to prevent
stored to AD DS for operating system drives	Users from specifying recovery options when they turn on BitLocker on a drive. This means that you will not be able to specify which recovery option to use when you turn on BitLocker, instead BitLocker recovery options for the drive are determined by the policy setting. In "Save BitLocker recovery information to Active Directory Domain Services", choose which BitLocker recovery information to store in AD DS for operating system drives. If you select "Backup recovery password and key package", both the BitLocker recovery information to store in AD DS drive that has been physically corrupted. If you select "Backup recovery More than the second of the sec

Exiger une authentification supplémentaire au démarrage – Activé, permet de configurer si BitLocker exige une authentification supplémentaire à chaque démarrage de l'ordinateur et si on utilise BitLocker avec ou sans module de plateforme sécurisée. Dans mon cas je décoche l'option « Autoriser BitLocker sans module de plateforme sécurisée... » et j'autorise l'utilisation du TPM (voir image).

💭 Exiger une authentification supplémentaire au démarrage — 🛛 🛛 🗙							
📷 Exiger une authe	entification supplémen	re précédent Paramètre suivant					
O Non configuré	Commentaire :			^			
Activé							
○ Désactivé				~			
	Pris en charge sur :	Au minimum Windows	s Server 2008	R2 ou Windows 7			
Options :				Aide :			
Autoriser BitLocker mot de passe ou	er sans un module de une clé de démarrage	plateforme sécurisée cor sur un disque mémoire f	mpatible (re flash USB)	Ce paramètre de stratégie vous permet de configurer si BitLocker exige une authentification supplémentaire à chaque démarrage de			
Paramètres pour les	ordinateurs avec un m	iodule de plateforme séc	curisée :	l'ordinateur et si vous utilisez BitLocker avec ou sans module de plateforme sécurisée. Ce paramètre de stratégie est appliqué lorsque vous activez BitLocker. Remarque : une seule des options d'authentification supplémentaire peut être exigée au démargne cans chéner d'ereur de textérnie			
Configurer le déman	rage du module de pla	teforme sécurisée :					
Autoriser le module	de plateforme sécurise	ée 🗸					
Configurer le code P	PIN de démarrage de n	nodule de plateforme sé	curisée :				
Autoriser un code P	IN de démarrage avec	le module de plateforme	e sécurisée	au démarrage, sans générer d'erreur de stratégie.			
Configurer la clé de	démarrage de module	de plateforme sécurisée	11	Si vous voulez utiliser BitLocker sur un ordinateur sans un module de plateforme sécurisée, activez la			
Autoriser une clé de	démarrage avec le mo	dule de plateforme sécu	ırisée	case à cocher « Autoriser BitLocker sans un module			
Configurer le code P	PIN et la clé de démarr	age de module de plate	forme sécur	mode, un mot de passe ou un lecteur USB est			
Autoriser une clé et	un code PIN de démar	rage avec le module de j	plateforme	est utilisée, les informations de clé utilisées pour			
chiffrer le lecteur sont stockées sur ce lecteur créant une clé USB, Lorsque la clé USB est ins							
			l'accès au lecteur est authentifié et le lecteur est accessible. Si la clé USB est perdue ou non				
			disponible, ou bien encore si vous oubliez le mot				
<			>	de passe, vous devez uniser i une des options de			
OK Annuler Appliquer							

Ce paramétrage laisse libre à l'administrateur de configurer BitLocker avec puce TPM et d'y ajouter une clé de démarrage et/ou un code PIN. En revanche la mise en place de BitLocker sans puce TPM ne sera pas autorisé car la GPO autorise uniquement le TPM.

La GPO est désormais en place mais celle-ci nécessite la mise en place de script et d'une GPO pour la déployer « automatiquement » sur les postes. En revanche la mise en place manuel de BitLocker est possible et c'est ce que l'on va voir désormais.

3 – Création d'un filtre WMI pour cibler Windows 11

Avant de continuer la mise en place il faut dans notre cas créer un filtre WMI ciblant Windows 11 sur des PC Portables (le filtre récupère l'état de la batterie) qui viendra s'appliquer sur notre GPO. Le voici:

SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0.2%" AND ProductType = "1"

Select * from Win32_Battery where BatteryStatus<>0

4 – Activer BitLocker manuellement sur un poste

À ce stade il est possible de configurer manuellement BitLocker sur un poste, certains paramètres seront « autoconfigurés » par la GPO, comme le fait de choisir si on chiffre la totalité du disque ou seulement l'espace utilisé.

Pour configurer BitLocker il faut se rendre dans « Gérer BitLocker » depuis Windows, dans la partie du lecteur du système d'exploitation et cliquer sur « Activer BitLocker ».

xploitation		
activé		/
	Activer BitLocker	

On demande ensuite de choisir le mode de déverrouillage du lecteur au démarrage, il y'a 3 propositions, celles que j'ai autorisé dans la GPO :

- Entrer un code confidentiel (PIN)
- Insérer un lecteur flash USB
- Laisser BitLocker déverrouiller automatiquement mon lecteur (TPM uniquement)

Dans mon cas je choisi la dernière option :

Ensuite on nous demande de choisir comment sera sauvegardé la clé de récupération (en plus de la sauvegarde dans l'AD), dans mon cas je choisis « Enregistrer sur un disque mémoire flash USB ».

Comment voulez-vous sauvegarder votre clé de récupération ?
Une clé de récupération vous permet d'accéder à vos fichiers et vos dossiers, si vous rencontrez des problèmes pour déverrouiller votre PC. Il est préférable d'en avoir plusieurs et de les conserver ailleurs que sur votre PC.
→ Enregistrer sur un disque mémoire flash USB
\rightarrow Enregistrer dans un fichier
→ Imprimer la clé de récupération

La dernière étape est la vérification du système BitLocker pour vérifier que les clés de chiffrement et de récupération sont accessibles avant de commencer à chiffrer.

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 chiffrement et de récupération avant le chiffrement du lecteur.
Insérez le lecteur flash USB contenant votre clé de récupération enregistrée. BitLocker redémarrera l'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.

Le système nous demande ensuite de redémarrer pour débuter le chiffrement du lecteur.

Au redémarrage un message apparaît pour indiquer que le chiffrement a commencé :



BitLocker est désormais en place sur ce poste, la clé de récupération est bien sauvegardée dans l'AD. (Voir suite)

5 – Scripts et GPO pour activer automatiquement BitLocker sur les postes

Cette manipulation permet d'activer BitLocker sans devoir l'activer manuellement sur chacun des postes.

Pour faire cela on va utiliser le module « BitLocker » de Powershell qui est intégré à Windows.

Voici le script Powershell à utiliser avec les explications de celui-ci :



Explication globale : Ce script récupère le disque système et détermine si il est chiffré avec BitLocker, si le disque est « FullyDecrypted » alors la suite du programme s'exécutera. Cette ligne est là pour éviter que le BitLocker rechiffre à chaque fois un disque déjà chiffré.

Ensuite la deuxième ligne ajoute une méthode de protection dans ce cas TPM uniquement.

La dernière ligne active BitLocker sur la partition système et verifie que la clé de récupération est bien remontée dans l'AD pour éviter de chiffrer un lecteur sans clé de récupération.

On va aussi utiliser un script batch pour contourner la politique d'exécution des scripts Powershell qui peut parfois poser un problème, pour contrer cela j'ai créé ce script batch.

```
gecho off
REM Définir la politique d'exécution sun Bypass pour cette session et exécuter le script PowerShell
powerShell -NoProfile -ExecutionPolicy Bypass -Command "& {Set-ExecutionPolicy Bypass -Scope Process -Force; . '\\Labo-ad\netlogon\BitLocker - PIN.ps1'; Set-ExecutionPolicy Restricted -Scope Process -Force}"
REM Optionnel : Afficher un message de confirmation
echo Le script PowerShell a été exécuté et la politique d'exécution a été réinitialisée.
```

Explication globale : Ce script batch défini la politique d'éxécution de script powershell en « Bypass » pour cette session et exécute le script precedemment crée puis termine par remettre la politique d'éxécution de base. Ensuite dans la GPO précédemment créée, on doit mettre en place un script qui s'exécutera à chaque démarrage des postes.

Pour cela suivre le chemin suivant :

Dans Configuration Ordinateur > Paramètres Windows > Scripts > Démarrage

Il faut copier le script batch et le coller dans le dossier par défaut de la GPO et l'ajouter.



Pour terminer il ne faut pas oublier d'ajouter le script Powershell dans cet emplacement (dans SYSVOL à l'emplacement dédié pour les scripts)

er Accueil Partage → → ↑ 🚺 → Ce P	Affichage C > Disque local (C:) > Windows >	SYSVOL > sysvol > labo.axi	um > scripts	
^	Nom	Modifié le	Туре	Taille
Acces rapide	📓 BitLocker - PIN.ps1	28/05/2024 14:36	Script Windows P	1 Ko

Le chemin UNC du script PS dans mon cas est le suivant : « <u>\\labo-data\netlogon\BitLocker</u> - PIN.ps1 ».

│ 🛃 🚽 ╤ │ netlogon :hier Accueil Parta	ge Affichage			
· -> · 🛧 🖵 \\Labo	o-ad\netlogon			
📰 Images 🔷 ^	Nom	Modifié le	Туре	Taille
Musique	BitLocker - PIN.ps1	28/05/2024 14:36	Script Windows P	1 Ko
🗊 Objets 3D				
🖶 Téléchargement				
Vidéos				
🏪 Disque local (C:)				

C'est ce chemin qu'il faut renseigner dans le script batch :

@echo off		
REM Définir la politique d'exécution sur Bypass pour cette session et exécuter le script PowerShell		
powershell -NoProfile -ExecutionPolicy Bypass -Command "& {Set-ExecutionPolicy Bypass -Scope Process -Force; .	'\\Labo-ad\netlogon\BitLocker - PIN.ps1'	Set-ExecutionPolicy Restricted -Scope Process -Force}"
REM Optionnel : Afficher un message de confirmation		
echo Le script PowerShell a été exécuté et la politique d'exécution a été réinitialisée.		

Normalement si la configuration est bonne et que la GPO s'applique correctement, aux redémarrages des postes les PC demanderont aux l'utilisateurs de redémarrer (après 1 à 2 minutes) une nouvelle fois leurs postes pour terminer la mise en place de BitLocker.

Après la mise en place de BitLocker et le chiffrement du disque système terminé, nous devons apercevoir un « cadenas » sur le disque concerné (voir image).

- OneDrive	videos	
Ce PC		
E Bureau	✓ Périphériques et lecteurs (2)	
Documents	Windows 10 (C:)	Lecteur DVD RW (D:)
📰 Images	142 Go libres sur 231 Go	DVD
👌 Musique	✓ Emplacements réseau (2)	
Objets 3D	COMMUN (E:)	SERVICES (F:)
🕂 Téléchargement:	120 Go libros sur 455 Go	120 Co libror our 465 Co
Vidéos	459 00 libres sur 405 00	
🚔 Windows 10 (C:)		

6 – Récupérer la clé de récupération

Afin de pouvoir contrer un éventuel problème avec la puce TPM, il est possible de récupérer la clé de récupération depuis l'AD, pour cela il faut se rendre dans les propriétés du poste concerné puis dans l'onglet « Récupération BitLocker ».

	Sys	stème d'exploitation	Membre de	Délégation	LAPS
Emplacem	ent	Géré par	Appel entrant	Récupération BitLocke	
Nots de pass	se de ré	cupération BitLocker :			
Date d'ajou	ut	ID de mot de passe			
2024-05-29	9 09:43	E43C816E-222E-4FA	9-BC91-4EDFDC4A1	I8BE	
2024-05-29	9 09:35	888FAAAF-ED58-493	36-8B96-26BAFB346	560	
2024-05-29	9 09:35	B2D11FE0-8E63-42E	30-B2D7-FBFBF4DD	SE5F	
2024-05-29	9 09:15	378B7B39-84C7-450	C-A2D3-D924A158D	C74	
2024-05-29	9 08:46	CB7C1EA2-0EEA-4B	93-BD97-494CB1E98	E43B	
2024-05-28	15.50	COE010ED 7000 440			
	5 10:50	63F010ED-7F00-4A2	A-9A3D-0F897AA90	8ED	
Détails : Mot de pass 67	se de réi 76478-0	cupération : 83111-177903-08613	A-9A3D-0F897AA90	3ED	
Détails : Not de pass 6 2	se de ré 76478-0 38480-3	cupération : 89111-177903-08613 45895-212619-37060	0- 1	3ED	

Petit Tips : Il est possible depuis l'AD avec les 8 premiers caractères de l'ID de mot de passe d'effectuer une recherche pour identifier rapidement le poste concerné.

Récupération des 8 caractères depuis le poste :

Recupération BitLocker
Entrer la clé de récupération de ce lecteur
Utilisez les touches numériques ou les touches de fonction F1 à F10 (utilisez F10 pour 0). ID de clé de récupération (pour identifier votre clé) E43C816E 222E-4FA9-BC91-4EDFDC4A18BE
Voici comment trouver votre clé :
- Contactez le support technique de votre organisation
 Pour plus d'informations, accédez à : aka.ms/recoverykeyfaq

	🔿 🖄 📷	🗐 🖬 🖬 🖬	🥐 📷 🦉	8 18 7 2 8	
>	Utilisateurs et 📋 Requêtes e	ordinateurs Active nregistrées	Nom	Type builtinDomain	^
~	abo.ax	Délégation de co	ontrôle	220002000	
	Cor	Rechercher le m	ot de passe de	récupération BitLocker	
	> 📑 Dor	Rechercher			
	> 🧮 For	Changer de don	naine		
	> FSL	Changer de con	trôleur de dom	aine	
	S GRU	Augmenter le ni	veau fonctionn	iel du domaine	
	> 📫 Use	Maîtres d'opérat	ions		
	> 💼 Util	Nouveau			>
		Toutes les tâche	s		>

Récupération de la clé de récupération depuis l'AD :

Ordinateur	Date d'ajout	ID de mot de passe	
LABO-CL1	2024-05-29 09:43	E43C816E-222E-4FA9-BC91-4EDFDC4A18BE	
e récupération : 78-089111-177903-0	86130-		
30-345895-212619-3	70601		
	e récupération : 78-089111-177903-0 30-345895-212619-3	LABO-CL1 2024-05-29 09:43	LABO-CL1 2024-05-29 09:43 E43C816E-222E-4FA9-BC91-4EDFDC4A18BE e récupération : 78-089111-177903-086130-300-345895-212619-370601 6

Lorsque qu'on rentre les 8 premiers caractères de l'ID du mot de passe à l'endroit indiqué en rouge, on retrouve facilement les informations de BitLocker pour le poste.

7 - Vérification du fonctionnement de la clé de récupération

Afin de garantir un déploiement serein de BitLocker en production, il est indispensable de valider le bon fonctionnement des clés de récupération. Un test a déjà été réalisé et les clés de récupération semblent fonctionner comme prévu.



8- Conclusion

Voilà BitLocker est en place et le chiffrement du disque système peut être configuré manuellement ou automatiquement, les informations sont sauvegardées dans l'AD et le déploiement peut être contrôlé via le filtre WMI notamment.

2. TROUBLESHOOTING

Selon Microsoft, les types de modification du système qui peuvent provoquer un échec de la vérification de l'intégrité et empêcher le module TPM de libérer la clé BitLocker pour déchiffrer le lecteur du système d'exploitation protégé sont les cas suivants :

- Déplacement du lecteur protégé par BitLocker vers un nouvel ordinateur
- Installation d'une nouvelle carte mère avec un nouveau module de plateforme sécurisée
- Modification, désactivation ou effacement du module de plateforme sécurisée
- Modification des paramètres de configuration de démarrage
- Modification du BIOS, du microprogramme UEFI, de l'enregistrement de démarrage master, du secteur de démarrage, du gestionnaire de démarrage, de l'option ROM ou d'autres composants de démarrage précoces ou des données de configuration de démarrage
- Retrait, insertion ou épuisement complet de la charge sur une batterie intelligente sur un ordinateur portable

Pour « tester » BitLocker avant mise en production, on a imaginé différents scénarios comme : enlever / ajouter de la RAM, MàJ Windows, MàJ firmware, Migration du disque système via l'outil Samsung Magician..

Le fait d'ajouter ou d'enlever de la RAM ne modifie pas le comportement de BitLocker.

Les MàJ Windows n'affecte pas le comportement de BitLocker

La Migration du disque système via l'outil Samsung Magician est impossible car l'outil ne peut pas migrer un disque chiffré, voir image.



Pour les mises à jour du firmware du BIOS, nous utilisons en grande majorité des postes DELL, et ceux-ci on l'outil « Dell Command Update » d'installé.

Selon DELL, Dell Command | Update prend en charge la possibilité d'installer les mises à jour du BIOS même si le chiffrement BitLocker est activé sur le disque de démarrage du système. Cela permet de suspendre BitLocker lors de la mise à jour du BIOS et de reprendre le chiffrement BitLocker une fois le BIOS mis à niveau.

DELL précise ensuite que « Dell Command Update » ajoute dans l'écran des paramètres du BIOS une case à cocher intitulée **Suspendre automatiquement BitLocker.** Celle-ci est cochée par défaut.

bell Command	I Update	v 5.3.0	© .			
Latitude Numéro de série : Dernière ise à o jour : Historique des r Infos sys Journal d'a	Paramètres Général Paramètres de mise à jour Filtre de mise à jour Import/Export Restauration avancée des pilotes BIOS Licences tierces	passe est requis pour effectuer les mises à jour du BIOS. ▲FFICHER LE MOT DE PASSE ▲FFICHER LE MOT DE PASSE ▲ Suspendre BitLocker ▲ ▲ Aretissement : La suspension automatique du chiffrement du lecteur BitLocker doit être effectuée uniquement dans un environnement sécurisé pour garantir la sécurité du lecteur. ■ Suspendre automatiquement BitLocker ■ Suspendre automatiquement BitLocker	de pilotes t installe le CHERCHEI velle ne	, de is R	•	
🛛 Envoyez-nous vos c	commentaires					

Toujours selon DELL, lorsqu'une mise à jour du BIOS est disponible et sélectionnée, et que l'option **Suspendre automatiquement BitLocker** est cochée, l'option **Redémarrer automatiquement le système** (le cas échéant) est cochée, par défaut, elle est désactivée. Lors de l'installation de la mise à jour du BIOS, BitLocker est suspendu temporairement pour appliquer les mises à jour du BIOS. Une fois que le BIOS a été mis à jour et que les autres mises à jour ont été appliquées, le système redémarre automatiquement pour effectuer la mise à jour du BIOS, après quoi BitLocker est réactivé.

Pour vérifier le comportement d'une update du BIOS, j'ai utilisé un PC Portable HP disponible dans mon LAB avec BitLocker activé via le TPM, j'ai installé « HP Support Assistant » qui est l'équivalent de l'outil « Dell Command Update ». L'outil d'HP agit sensiblement de la même manière que celui de Dell.

Lors de la recherche de mise à jour via l'outil d'HP, celui à trouvé une mise à jour pour le BIOS, idéal pour tester le comportement de BitLocker.

Avant de mettre à niveau le BIOS, l'outil nous demande manuellement de permettre à l'utilitaire HP de suspendre temporairement BitLocker pendant la mise à jour du BIOS. (Voir image)



Après ça un petit message apparaît pour signifier que BitLocker est suspendu.

