Table des matières

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.

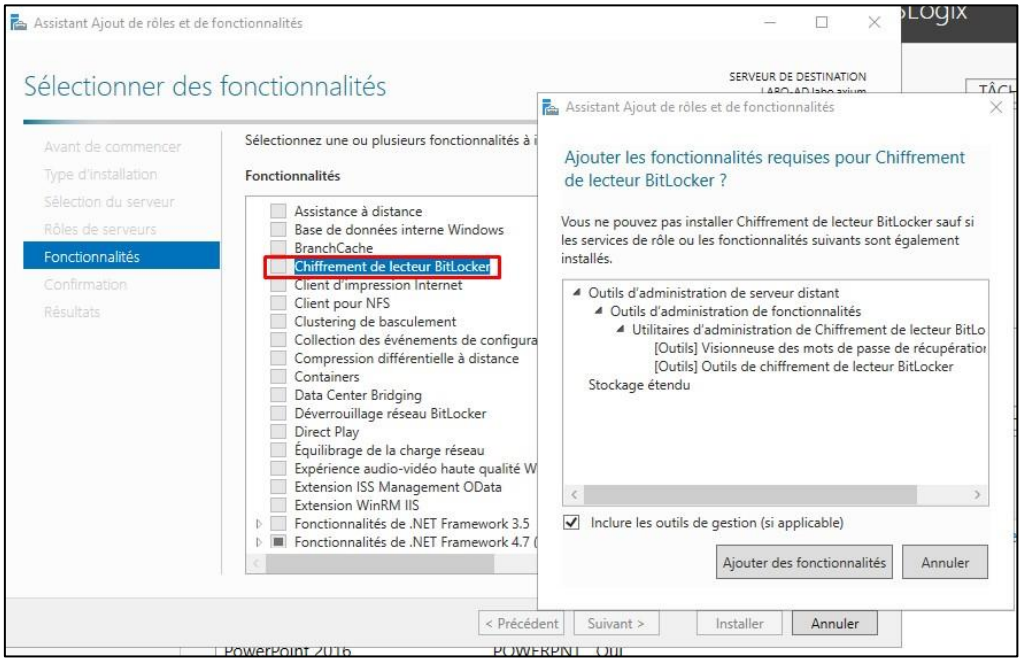
1. CONFIGURATION DE BITLOCKER

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

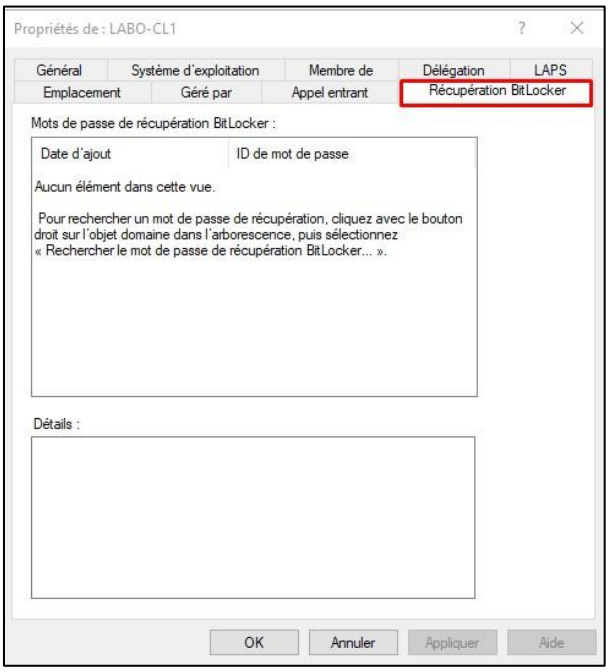
1 – Installation de la fonctionnalité BitLocker

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



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

Onglet « Récupération BitLocker » :



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

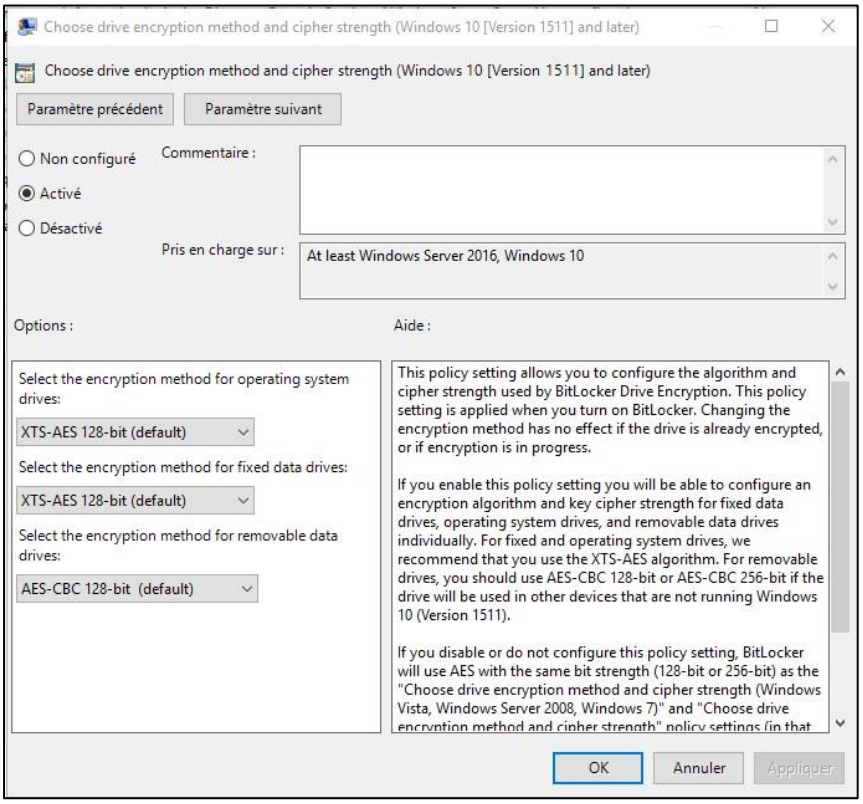
2 – Configuration de la GPO

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 :

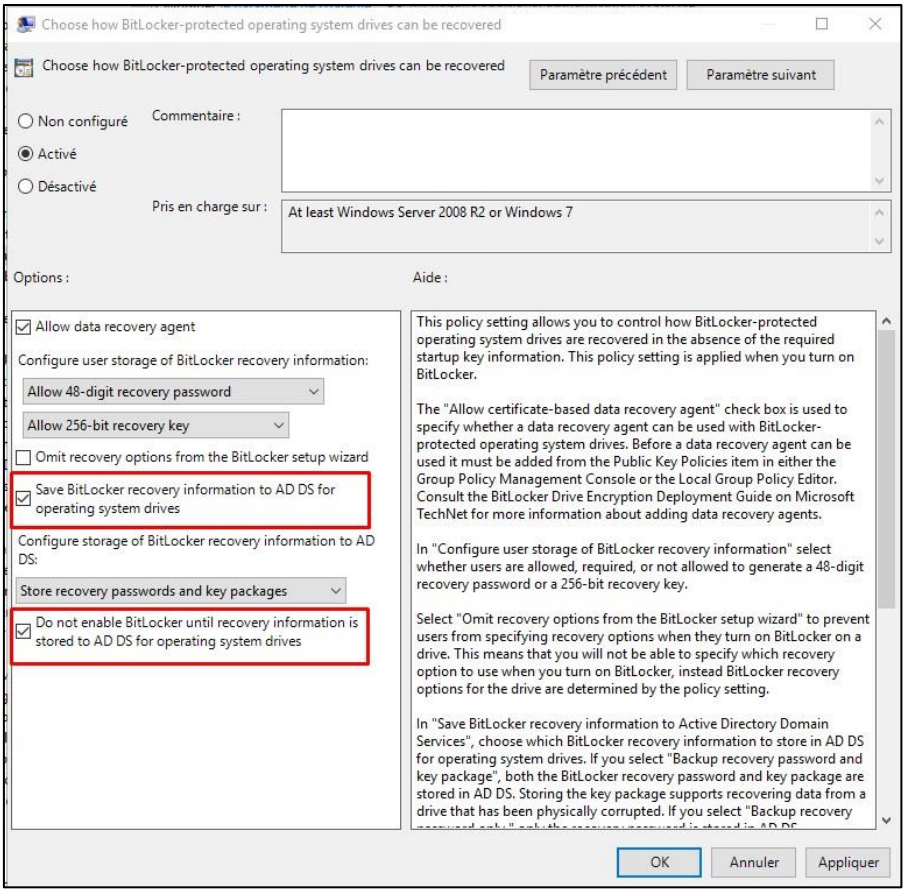
- **Choose drive encryption method and cipher strenght (Windows 10 and later) –** Activé**,** spécifie les méthodes de chiffrement à utiliser pour un lecteur, dans mon cas je choisis la méthode par défaut.



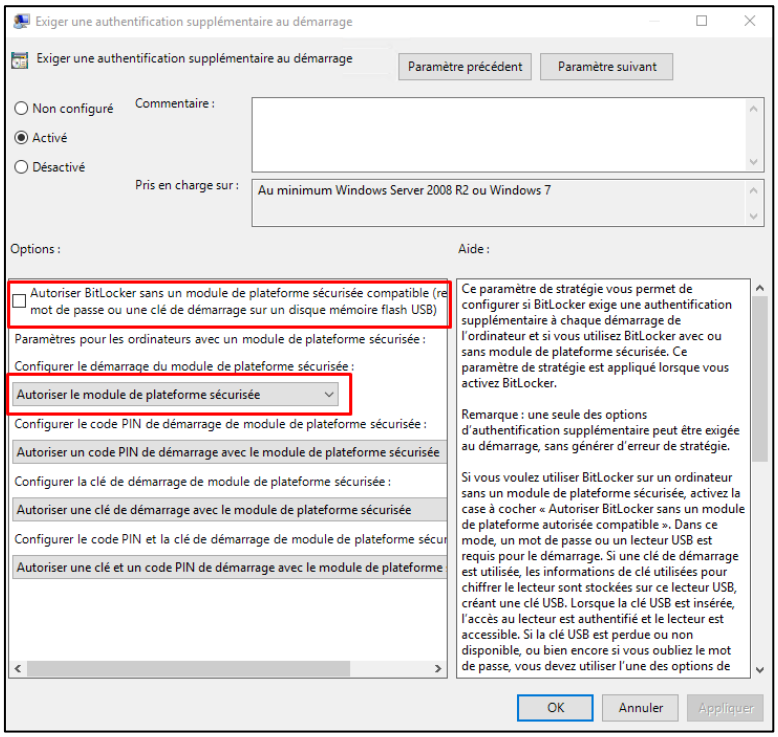
Dans **Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Chiffrement de lecteur BitLocker > Operating System Drives**

- **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 :



- **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).



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:

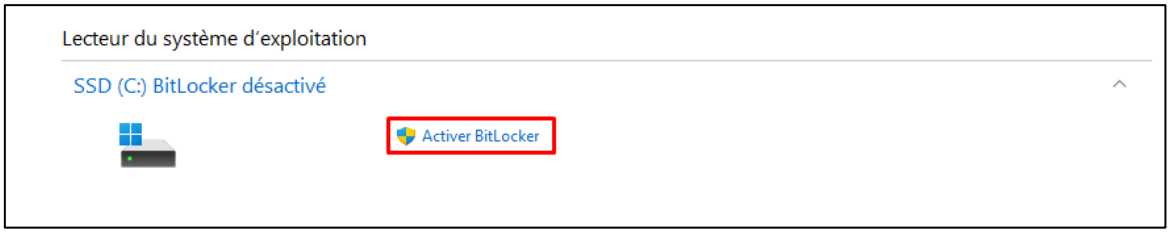
SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0.2%" AND ProductType = "1"

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.

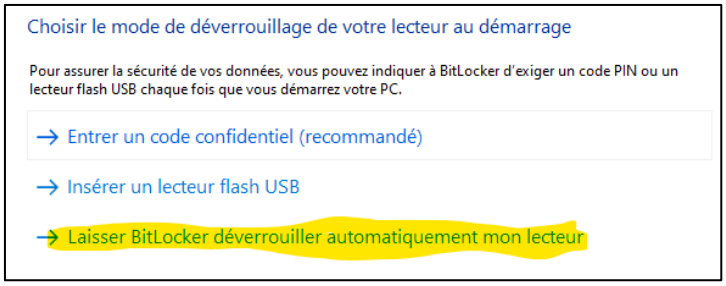
Pour configurer BitLocker il faut se rendre dans « Gérer BitLocker » depuis Windows, dans la partie du lecteur du système d'exploitation et cliquer sur « Activer BitLocker ».



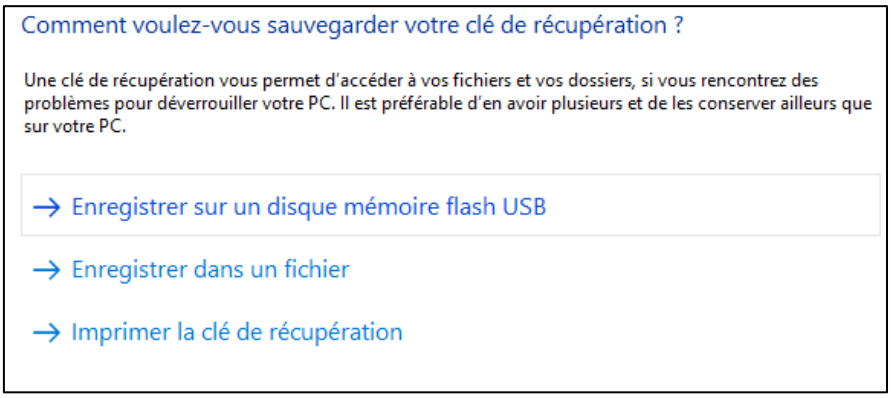
On demande ensuite de choisir le mode de déverrouillage du lecteur au démarrage, il y'a 3 propositions, celles que j'ai autorisé dans la GPO :

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

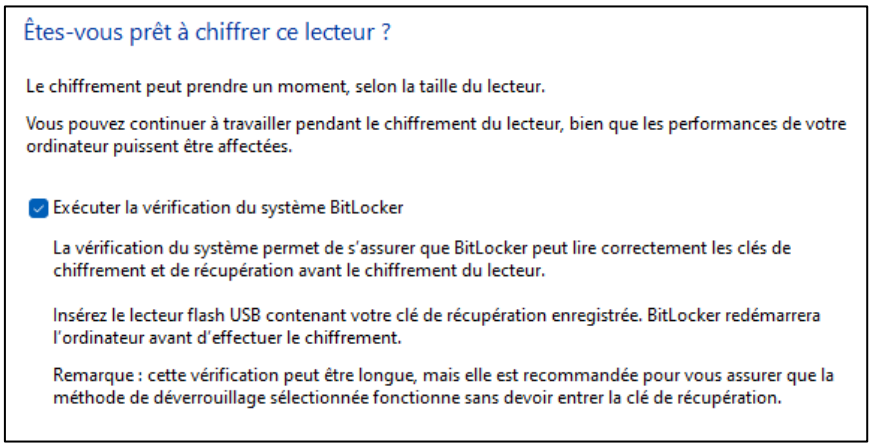
Dans mon cas je choisi la dernière option :



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 ».



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.



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 :

BitLocker - TPM.ps1*

```
#Si le disque systÃ¨me est "FullyDecrypted" alors la suite du programme s'Ã©xÃ©cute
if((Get-BitLockerVolume -MountPoint $env:SystemDrive).VolumeStatus -eq "FullyDecrypted"){

#Ajouter mÃ©thode de protection BitLocker dans ce cas TPM
   Add-BitLockerKeyProtector -MountPoint $env:SystemDrive -TpmProtector

#Activation BitLocker sur la partition systÃ¨me et verification avant chiffrement
   Enable-BitLocker -MountPoint $env:SystemDrive -RecoveryPasswordProtector

}
```

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.

```
@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.
```

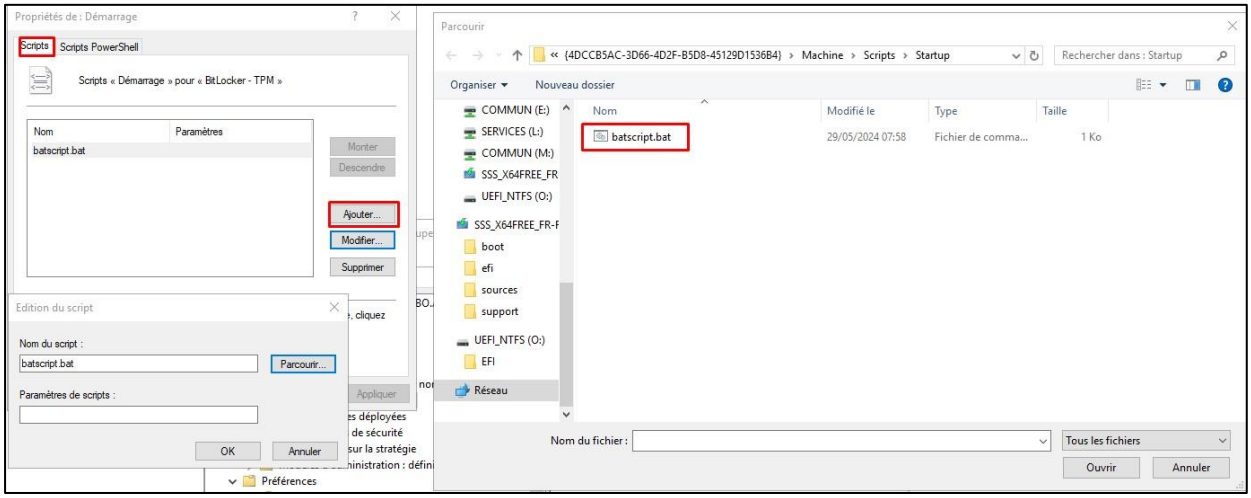
Explication globale : Ce script batch défini la politique d'éxécution de script powershell en « Bypass » pour cette session et exécute le script precedemment crée puis termine par remettre la politique d'éxécution de base.

Ensuite dans la GPO précédemment créée, on doit mettre en place un script qui s'exécutera à chaque démarrage des postes.

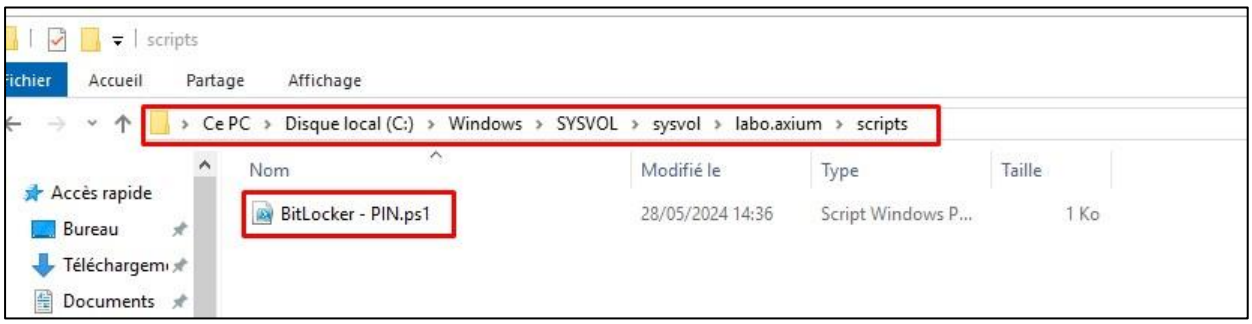
Pour cela suivre le chemin suivant :

Dans **Configuration Ordinateur > Paramètres Windows > Scripts > Démarrage**

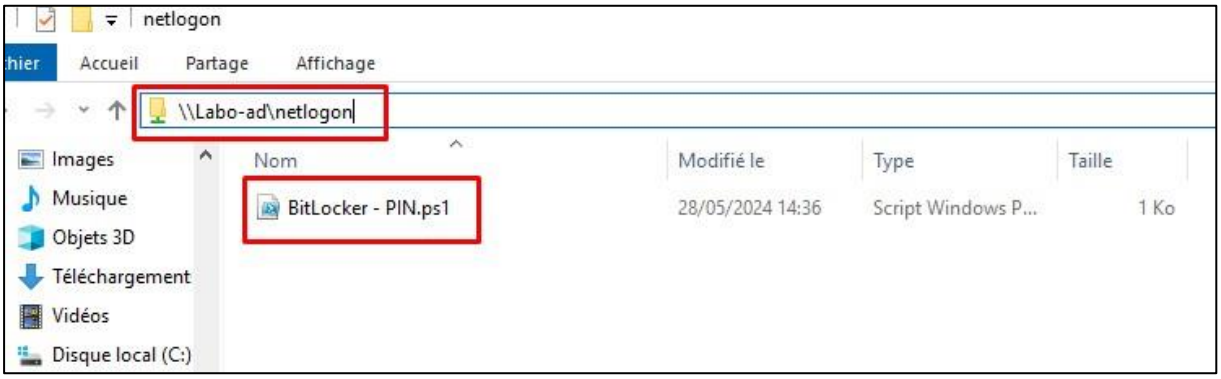
Il faut copier le script batch et le coller dans le dossier par défaut de la GPO et l'ajouter.



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



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



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

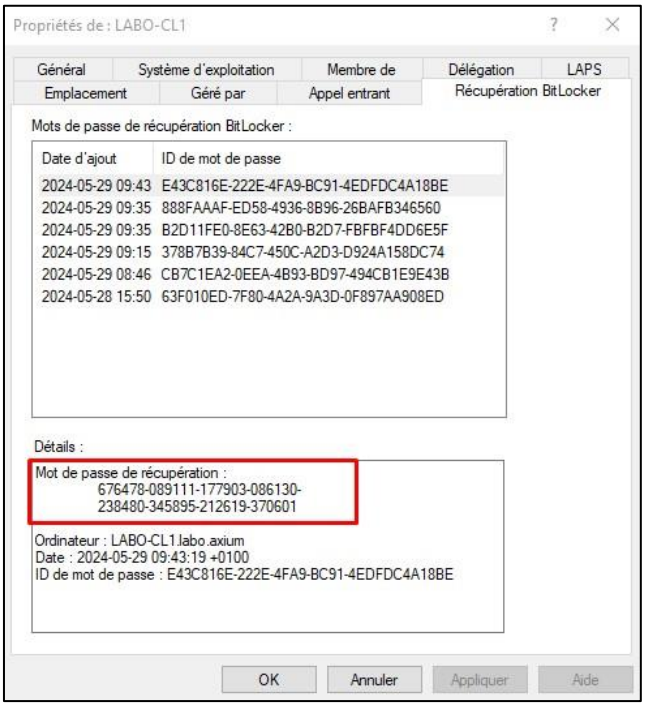
```
@echo off
REM Définir la politique d'exécution sur Bypass pour cette session et exécuter le script PowerShell
powershell -NoProfile -ExecutionPolicy Bypass -Command "& {Set-ExecutionPolicy Bypass -Scope Process -Force; . '\\Labo-ad\netlogon\BitLocker - PIN.ps1'; Set-ExecutionPolicy Restricted -Scope 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).

6 – Récupérer la clé de récupération

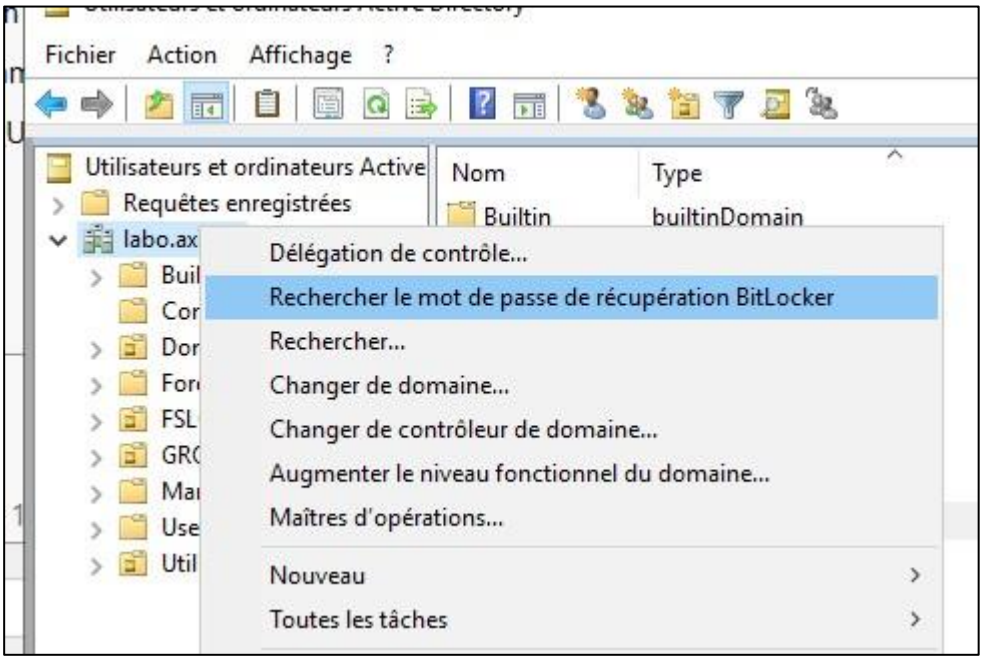
Afin de pouvoir contrer un éventuel problème avec la puce TPM, il est possible de récupérer la clé de récupération depuis l'AD, pour cela il faut se rendre dans les propriétés du poste concerné puis dans l'onglet « Récupération BitLocker ».

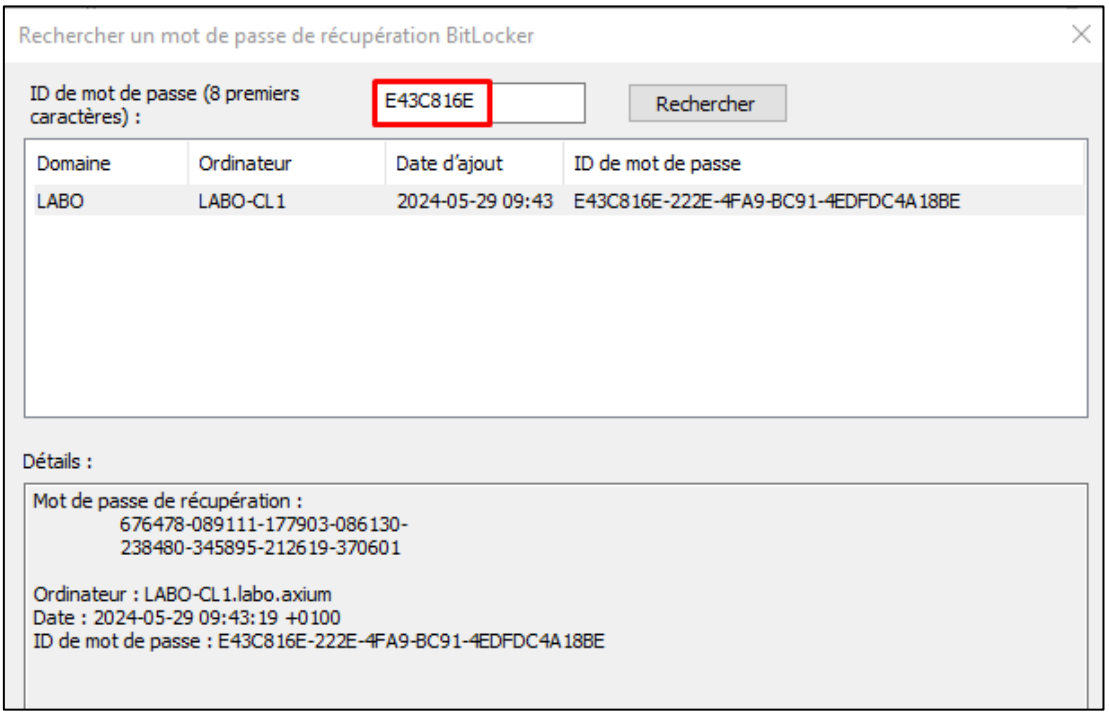


Petit Tips : Il est possible depuis l'AD avec les 8 premiers caractères de l'ID de mot de passe d'effectuer une recherche pour identifier rapidement le poste concerné.

Récupération des 8 caractères depuis le poste :

Récupération de la clé de récupération depuis l'AD :

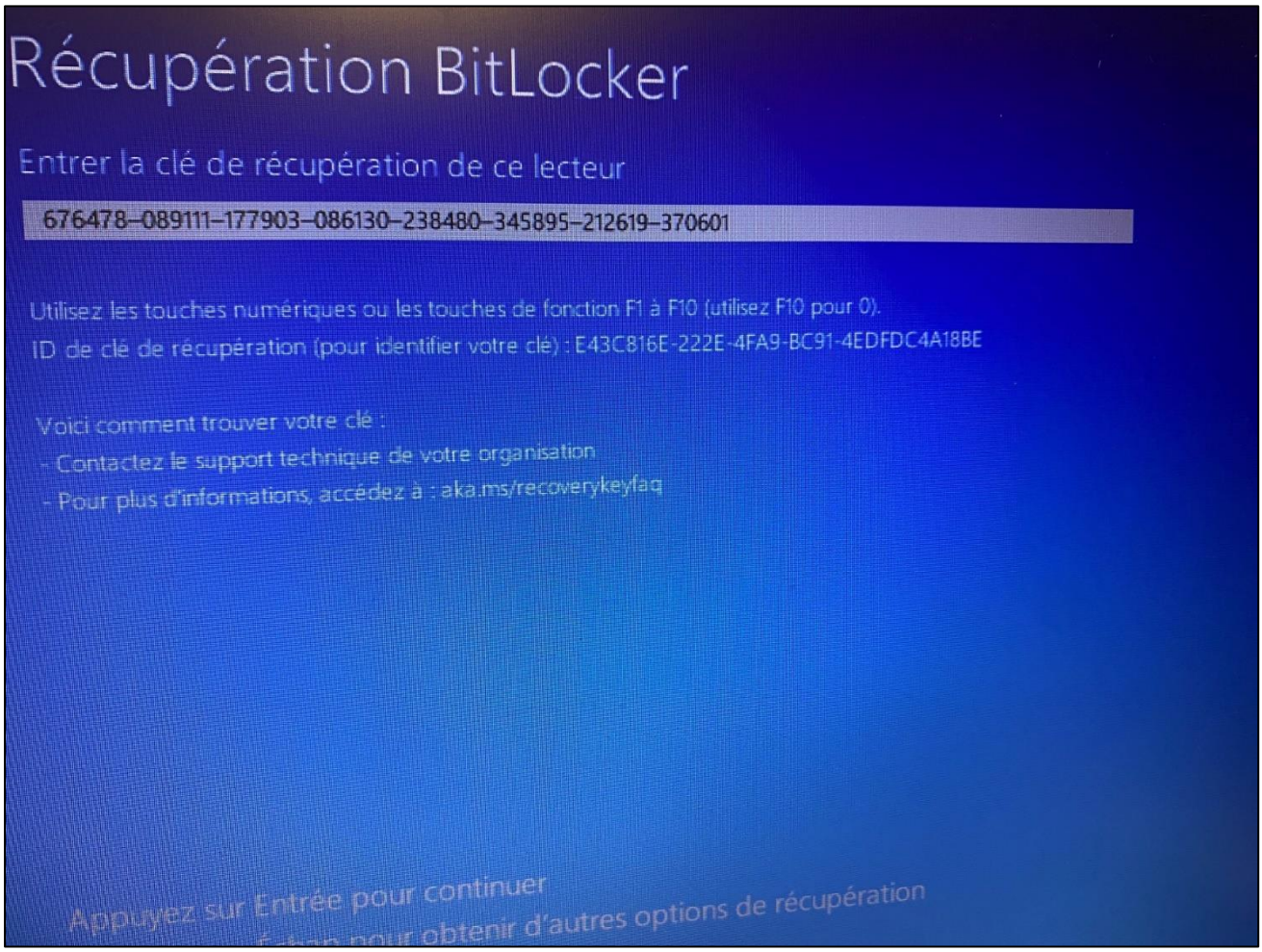




Lorsque qu'on rentre les 8 premiers caractères de l'ID du mot de passe à l'endroit indiqué en rouge, on retrouve facilement les informations de BitLocker pour le poste.

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 :

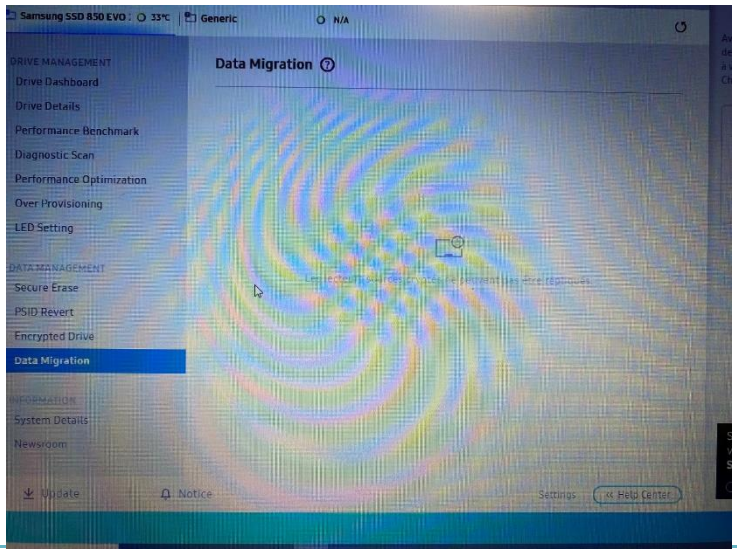
- Déplacement du lecteur protégé par BitLocker vers un nouvel ordinateur
- Installation d'une nouvelle carte mère avec un nouveau module de plateforme sécurisée
- Modification, désactivation ou effacement du module de plateforme sécurisée
- Modification des paramètres de configuration de démarrage
- 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

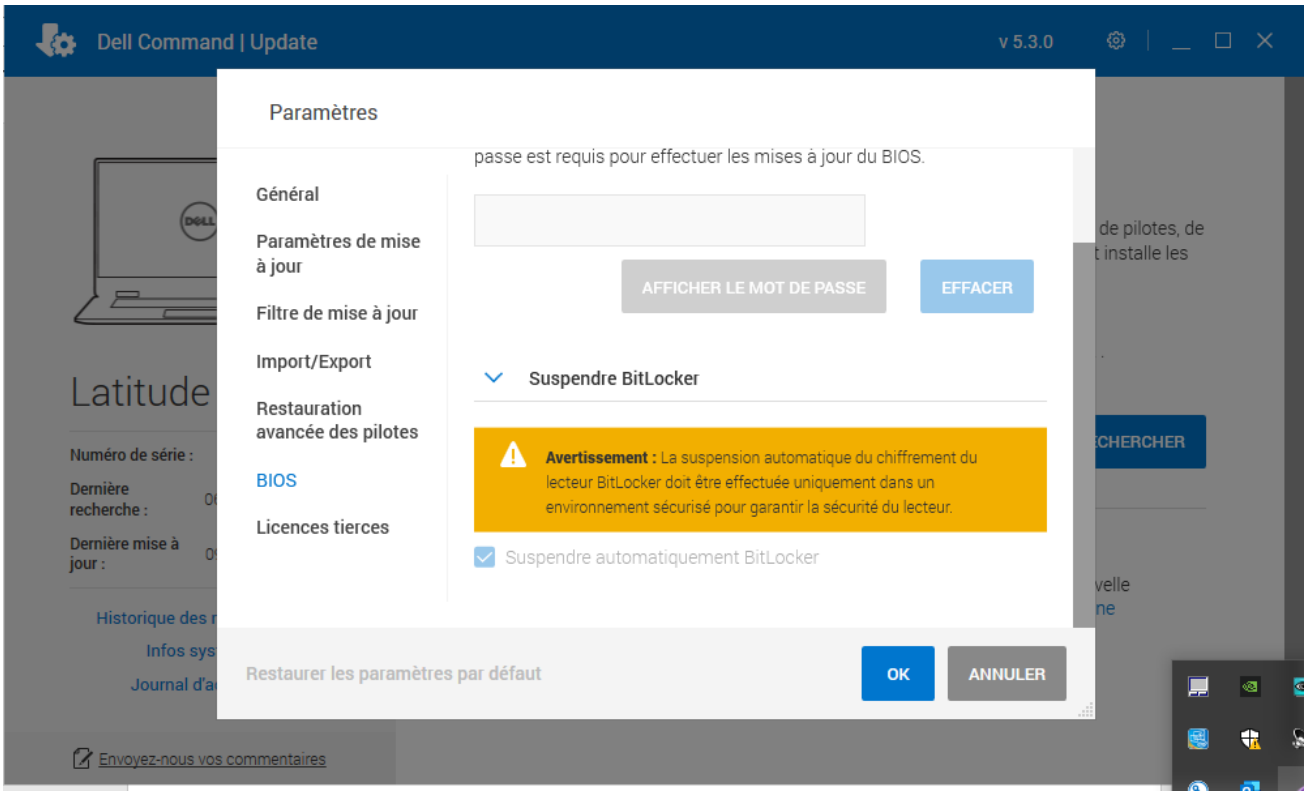
La Migration du disque système via l'outil Samsung Magician est impossible car l'outil ne peut pas migrer un disque chiffré, voir image.



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.

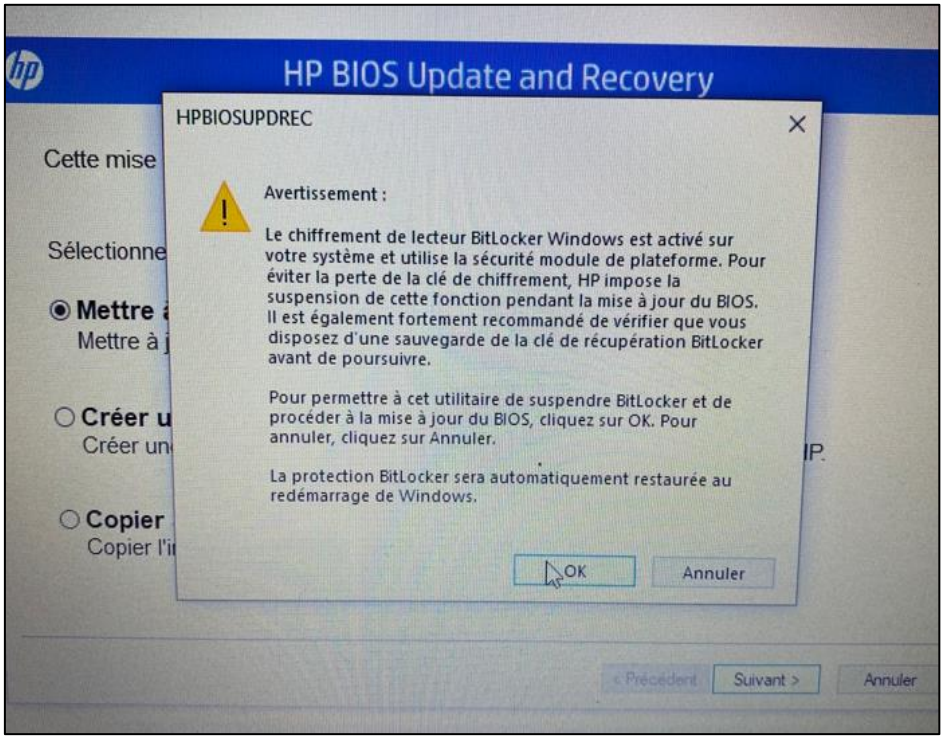


Toujours selon DELL, lorsqu'une mise à jour du BIOS est disponible et sélectionnée, et que l'option **Suspendre automatiquement BitLocker** est cochée, l'option **Redémarrer automatiquement le système** (le cas échéant) est cochée, par défaut, elle est désactivée. Lors de l'installation de la mise à 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.