# Documentation Technique
# Atelier Pro 1
# Groupe 1

Groupe 1

Novembre 2025

Tsiaroniaina-rianala RAMANANTSIALONINA : Co-responsable Linux
Gökhan YILMAZ : Co-responsable Linux
Enzo ROESCH : Co-responsable Windows
Sarah NIED: Co-responsable Windows

# Table des matières

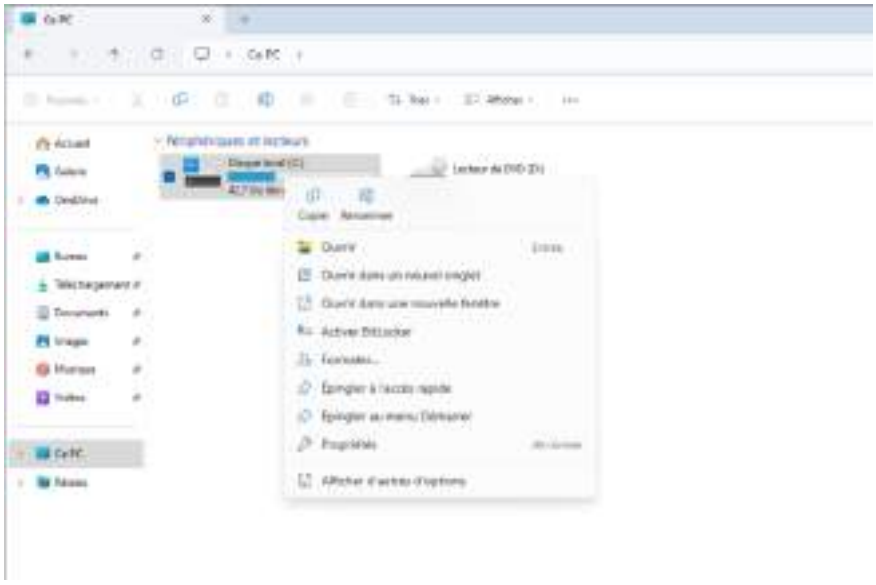
# Documentation Windows 11

## I. Chiffrer le disque dur Windows 11 (Sarah)

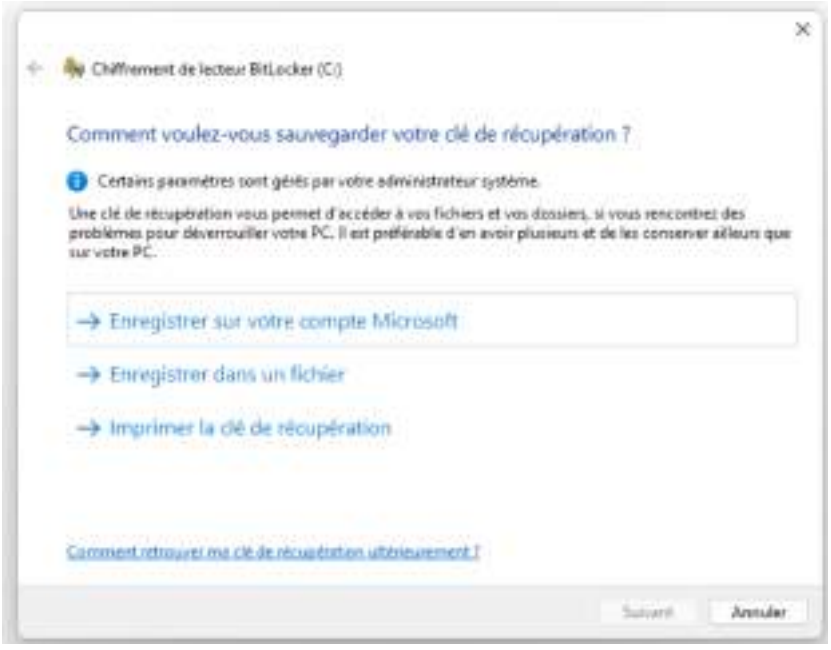
Le chiffrement du disque dur grâce à BitLocker permettra d'éviter le vol de données. Le disque ne sera plus accessible sans la clé de récupération. De plus, cela bloque aussi l'exploit où utilman.exe est remplacé par une invite de commande et permet l'accès en administrateur local au système.

### a. Procédure manuelle

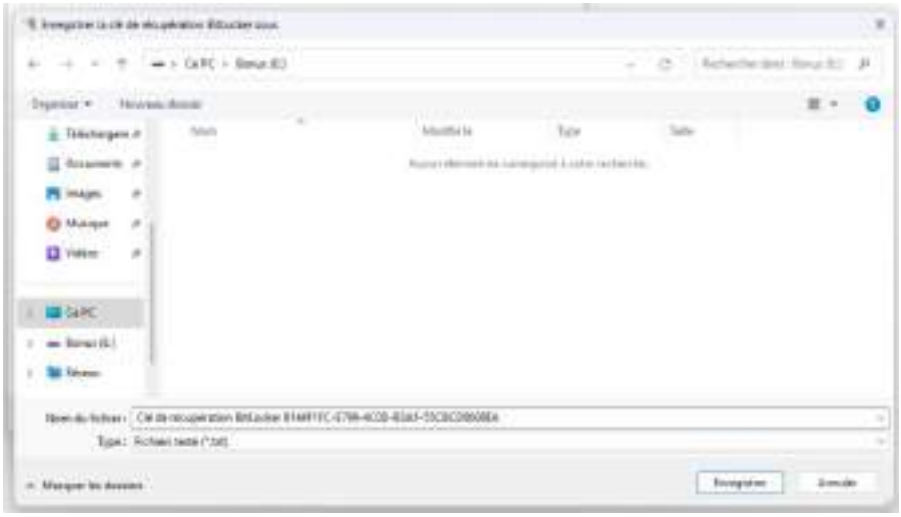
Aller dans l'explorateur de fichier du poste de travail, aller dans Ce PC, faire un clic droit sur le disque dur :



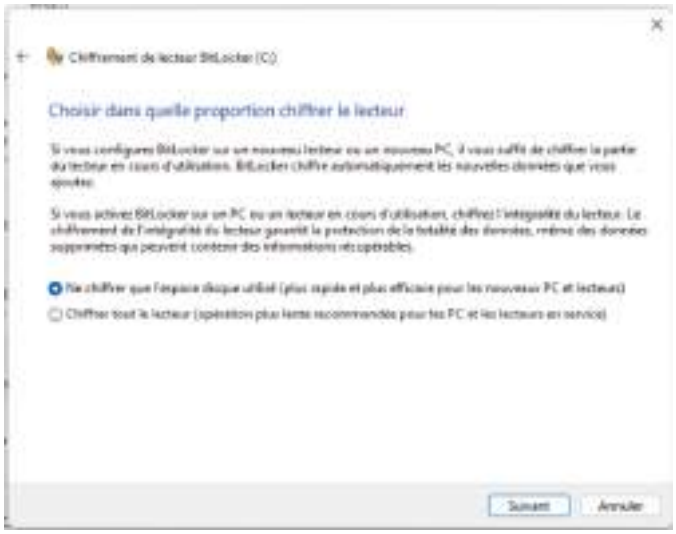
Cliquer sur Activer Bitlocker, l'assistant va se lancer, choisir où sauvegarder la clé de récupération qui permet de déchiffrer le disque :



Choisir enregistrer dans un fichier et la sauvegarder de préférence sur une clé USB :



Choisir de chiffrer l'espace disque utilisé comme les postes sont chiffrer avant déploiement (ils sont encore neufs) :

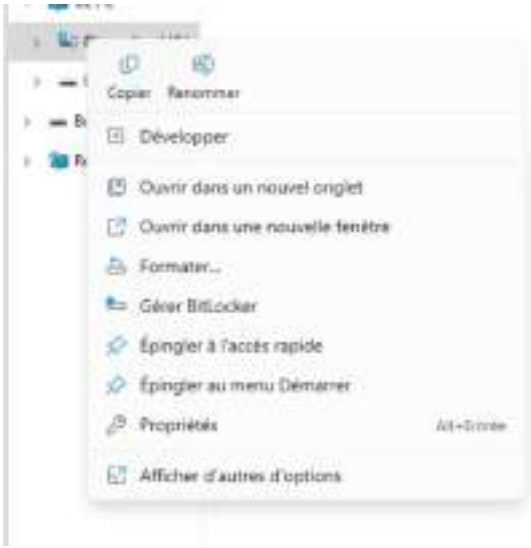



Choisir le mode chiffrement, ici nouveau mode de chiffrement car il s'agit du disque dur principal du poste de travail :

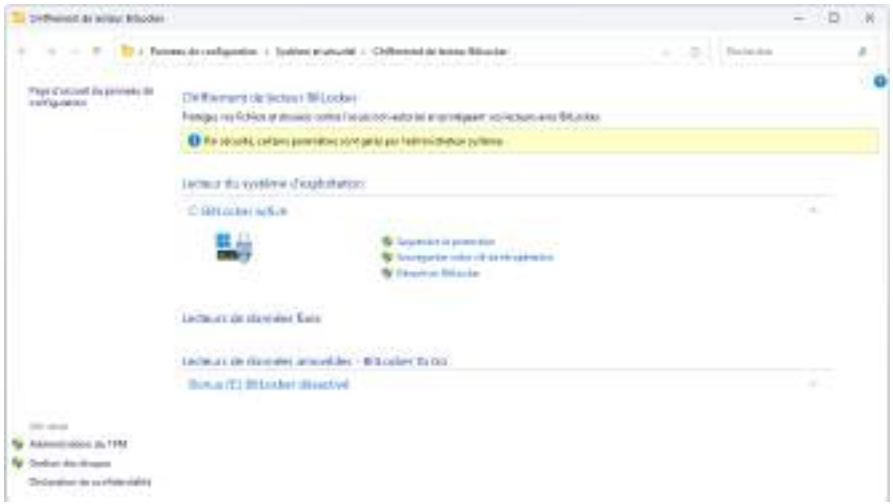

Cocher la vérification Bitlocker et lancer le chiffrement :


Le poste doit alors redémarrer :


Une fois le poste redémarré, aller dans Explorateur de fichier, Ce PC et faire un clic droit sur le lecteur C et aller sur Gérer BitLocker :




Une fois dans la gestion de BitLocker vérifier que Bitlocker est bien marqué comme activé :



Ici il est possible de sauvegarder à nouveau la clé de récupération si nécessaire.

## b. Procédure Powershell

```
# Exécuter en tant qu'administrateur

param(
    [string]$DriveLetter = "C:",
    [string]$EncryptionMethod = "Aes256"
)

# Vérifier les droits administrateur
if (-not
([Security.Principal.WindowsPrincipal][Security.Principal.WindowsIdentity]::GetCurrent()).IsIn
Role([Security.Principal.WindowsBuiltInRole]::Administrator)) {
    Write-Host "Ce script doit être exécuté en tant qu'administrateur"
    exit
```

```
}

# Vérifier les prérequis
Write-Host "Vérification des prérequis..."
$tpm = Get-WmiObject -Namespace "root\cimv2\security\microsofttpm" -Class Win32_Tpm -
ErrorAction SilentlyContinue

if (-not $tpm) {
   Write-Host "Avertissement : TPM non détecté. BitLocker peut nécessiter une clé USB de
secours."
}

# Vérifier l'état actuel
$volume = Get-BitLockerVolume -MountPoint $DriveLetter -ErrorAction SilentlyContinue
if ($volume.VolumeStatus -eq "FullyEncrypted") {
   Write-Host "Le disque $DriveLetter est déjà chiffré"
   exit
}

# Activer BitLocker
Write-Host "Activation de BitLocker sur $DriveLetter..."
try {
   Enable-BitLocker -MountPoint $DriveLetter -EncryptionMethod $EncryptionMethod -
RecoveryPasswordProtector -ErrorAction Stop
   Write-Host "BitLocker activé avec succès"

   # Afficher l'état
   Get-BitLockerVolume -MountPoint $DriveLetter | Select-Object VolumeStatus,
EncryptionPercentage
} catch {
   Write-Host "Erreur lors de l'activation : $_"
}
```

# II. Paramètres Biométriques et d'Écran de Verrouillage (Sarah)

## a. Amélioration de la protection anti-spoofing pour la reconnaissance faciale

Pour améliorer la reconnaissance faciale, comme pour tout logiciel, il faut s’assurer que le logiciel ainsi que les pilotes, notamment pour la caméra, soient à jour. De plus, un ordinateur équipé d’une caméra de bonne qualité pourra plus aisément faire de la reconnaissance faciale plus précise.

De plus, les paramètres de la reconnaissance faciale peuvent être modifiés. Aller dans Paramètres, Compte :


Puis dans Options de connexion :


Activer la coche pour Améliorer la protection de la reconnaissance faciale (cela demandera un redémarrage) et cliquer sur améliorer reconnaissance, suivre l'assistant :


Pour garantir la reconnaissance faciale, de bonnes pratiques peuvent être mises en place telles que :

- La recalibration régulière de Windows Hello en utilisant les fonctions d'amélioration de la reconnaissance.
- La numérisation multiple du visage : lunettes mises et retirées, coiffures différentes, expressions du visage, avec différents éclairages (par exemple, à différents moments de la journée).

Il est aussi possible d'utiliser d'autres méthodes d'authentification avec Windows Hello, tels que le code PIN (non recommandé) ou alors la reconnaissance d'empreintes. Pour cela aller de nouveau dans Paramètres, Compte, Options de connexion :

## b. Désactivation de l'utilisation de la caméra sur l'écran de verrouillage

Pour ne plus utiliser la caméra (et donc la reconnaissance faciale) pour déverrouiller l'écran de verrouillage, aller dans Paramètres, Comptes, Options de connexion et cliquer sur Supprimer :


## c. Empêchement de l'activation vocale des applications sur un appareil verrouillé

Aller dans Paramètres, Confidentialité et sécurité, Activation vocale. Désactiver Autoriser des applications à utiliser l'activation vocale quand un appareil est verrouillé :

# III. DNS et Sécurité Réseau (Enzo)

## a. Désactivation de la diffusion DNS Multicast et des requêtes parallèles A et AAAA

Multicast DNS est un protocole de découverte de machines qui s'exécute sur les systèmes Windows et aussi sur Linux au travers du service Avahi. En l'absence de serveur DNS, il permet, au même titre que le LLMNR, de résoudre les noms des machines sur les réseaux locaux.

**Pour le désactiver le DNS Multicast :**

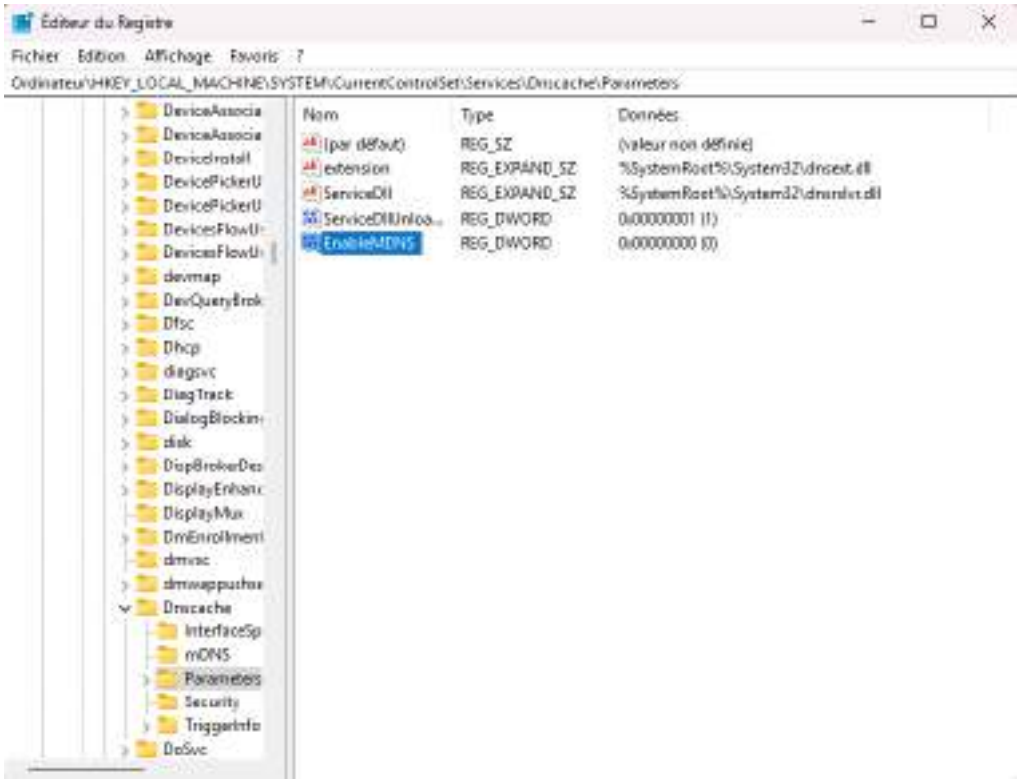
Win + R > regedit

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters

Créer la propriété DWORD (32 bits)

Nom : EnableMDNS

Valeur : 0 (0 = désactivé, 1 = activé par défaut)




Par défaut, Windows résout en parallèle les adresses IPv4 (A) et IPv6 (AAAA). Ça peut poser problème sur certains réseaux.

**Pour le désactiver les requêtes parallèles A et AAAA :**

Win + R > regedit

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters

Créer une valeur DWORD (32 bits)

Nom : DisableParallelAandAAAA

Valeur : 1 (1 = désactivé, 0 = activé par défaut)

## b. Désactivation de NTLMv1

L'authentification NTLM désigne un ensemble de protocoles d'authentification inclus dans la bibliothèque Windows Msv1_0.dll. Les protocoles d'authentification NTLM comprennent les versions 1 et 2 de LAN Manager et les versions 1 et 2 de NTLM.

Ils ont pour but d'authentifier des utilisateurs et des ordinateurs sur la base d'un mécanisme de stimulation/réponse destiné à prouver à un serveur ou un contrôleur de domaine qu'un utilisateur connaît le mot de passe associé à un compte. On désactive NTLMv1 car ancien.

Pour le désactiver :

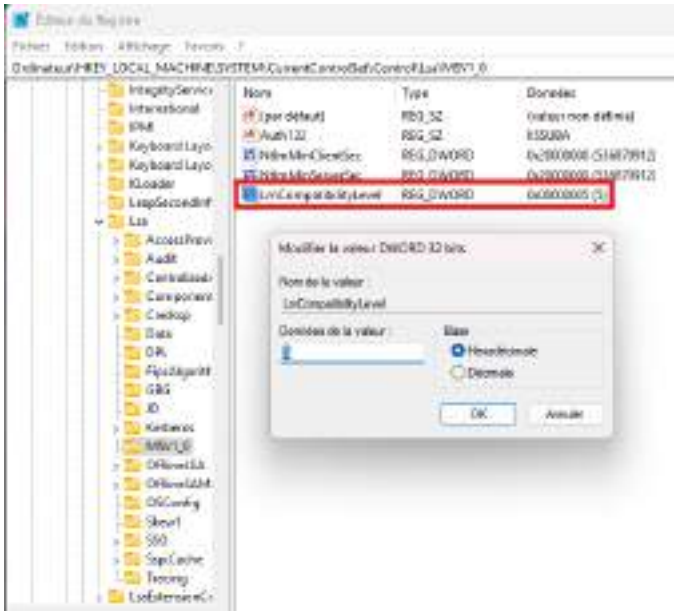
Win + R > regedit

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0

Créer ou modifier la clé DWORD (32 bits) LmCompatibilityLevel

Nom : LmCompatibilityLevel

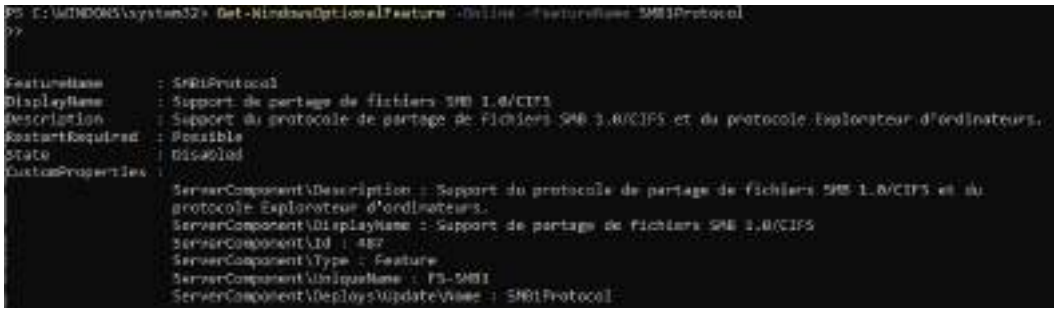
Valeur : 5 (Envoyer uniquement NTLMv2, refuser LM et NTLMv1)



## c. Désactivation de SMBv1

SMBv1 (Server Message Block version 1) est un protocole réseau inventé par Microsoft dans les années 80 pour le partage de fichiers et d'imprimantes entre ordinateurs Windows. Il est très vieux et non sécurisé, avec pas de chiffrement et une faible authentification.

On vérifie d'abord si SMBv1 est activé :




Dans PowerShell en admin :

Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

Si le 'State' est "Disabled" = Désactivé / Si le "State" est "Enabled" = Activé

Pour le désactiver avec PowerShell :

Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -NoRestart

/!\ Redémarrage nécessaire pour appliquer

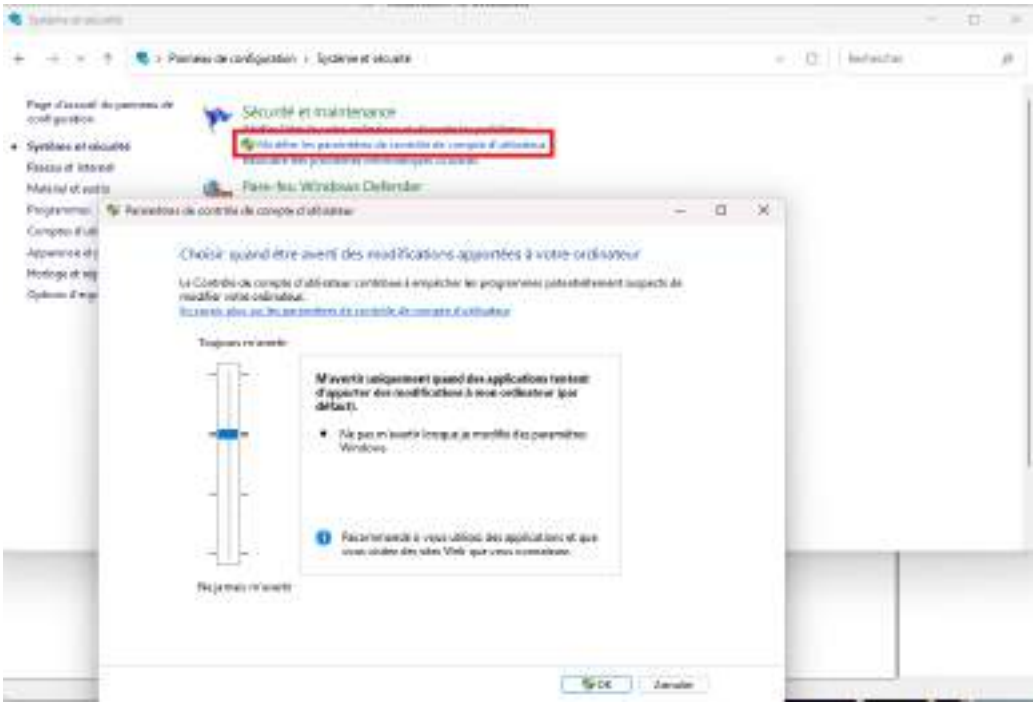
## d. Activation de l'UAC et configuration des paramètre associés

L'UAC (User Account Control) est une fonctionnalité de sécurité essentielle conçue pour empêcher les modifications non autorisées d'un système Windows. C'est entre autres comparable à l'action "sudo" sous Linux qui consiste à élever les privilèges à la demande.

Sans l'UAC, des logiciels malveillants et des utilisateurs non autorisés pourraient obtenir des privilèges d'administrateur, facilitant ainsi l'installation de logiciels malveillants, la modification des paramètres système ou la compromission de données sensibles.

Pour activer l'UAC :

Panneau de configuration > Système et sécurité > Modifier les paramètres de contrôle de compte utilisateur



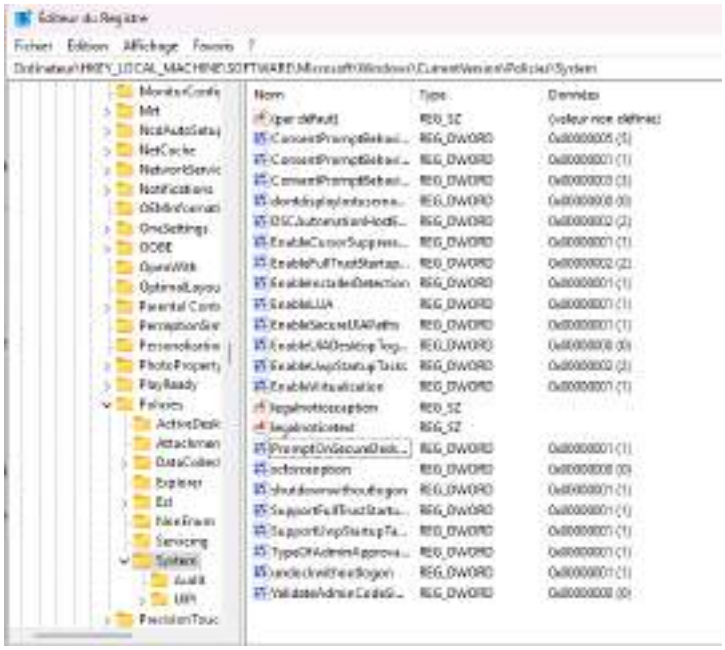

Par défaut, le curseur est réglé sur le niveau 3.

Si le curseur est tout en bas, l'UAC est désactivé. Plus il est élevé, plus la sécurité est renforcée.

Les paramètres associés sont nombreux, on les retrouve dans le registre :

Win + R > regedit

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System



Les plus importants :

| | |
|---|---|
| **EnableLUA** | Active ou désactive l'UAC.<br>1 = activé<br>0 = désactivé |
| **ConsentPromptBehaviorAdmin** | Détermine le comportement des invites pour les comptes administrateurs.<br>Valeurs possibles :<br>0 = Élever sans demander (dangereux)<br>1 = Demander mot de passe Admin (bureau sécurisé)<br>2 = Demander mot de passe Admin (bureau non sécurisé)<br>3 = Demander confirmation (bureau sécurisé)<br>4 = Demander confirmation (bureau non sécurisé)<br>5 = Demander consentement (valeur par défaut) |
| **ConsentPromptBehaviorUser** | Comportement pour les utilisateurs standards.<br>Valeurs :<br>0 = Échec automatique (aucune invite)<br>1 = Demander mot de passe Admin (bureau sécurisé)<br>2 = Demander mot de passe Admin (bureau non |

| | |
|---|---|
| | sécurisé)<br>3 = Demander confirmation (bureau sécurisé)<br>4 = Demander confirmation (bureau non sécurisé)<br>5 = Demander consentement (valeur par défaut) |
| **PromptOnSecureDesktop** | Définit si l'invite UAC se fait sur le bureau sécurisé (fond noir, tout bloqué).<br>1 = oui<br>0 = non |

# IV. Sécurité des Mots de Passe et de l'Authentification (Sarah)

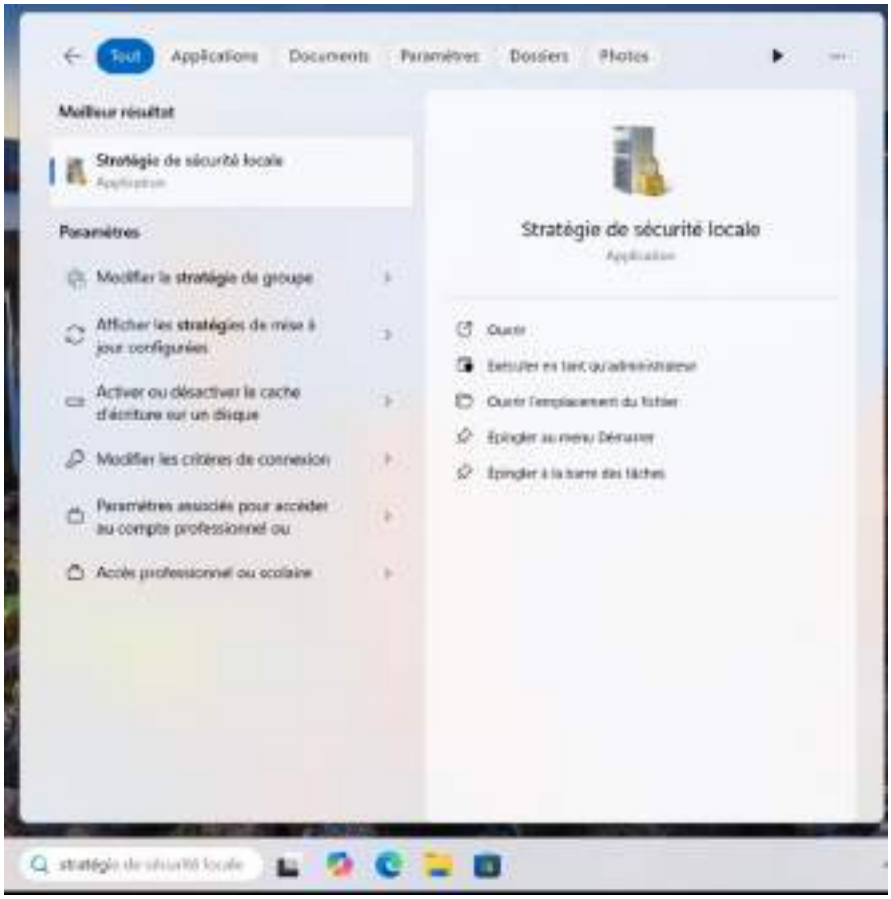
## a. Politique de mots de passe

L'application d'une politique de mots de passe est nécessaire. Une fois l'active directory déployé sur un contrôleur de domaine, une stratégie de groupe globale pourra être créée.

Cependant, il est aussi possible de le faire localement sur chaque poste. Pour cela, la Stratégie de sécurité locale doit être modifiée sur chaque poste pour prendre en compte les paramètres suivants :

- Longueur minimale 12 caractères
- Durée de vie : 90 jours
- Verrouillage de compte à 3 tentatives
- Durée de verrouillage 30 minutes
- Complexité du mot de passe

Aller dans Stratégie de sécurité locale :




Puis dans Stratégies de comptes, Stratégie de mots de passe :

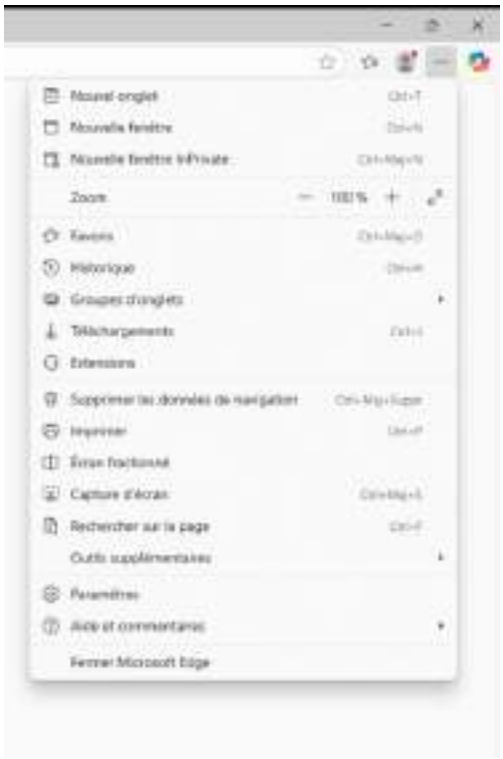
Ensuite changer les différents paramètres suivants : Longueur minimale du mot de passe, Durée de vie maximale du mot de passe et Le mot de passe doit respecter des exigences de complexité :

Ensuite aller dans Stratégie de verrouillage du compte et changer les paramètres suivants : Seuil de verrouillage du compte et Durée de verrouillage des comptes

## b. Désactivation de l'enregistrement des mots de passe en clair en mémoire

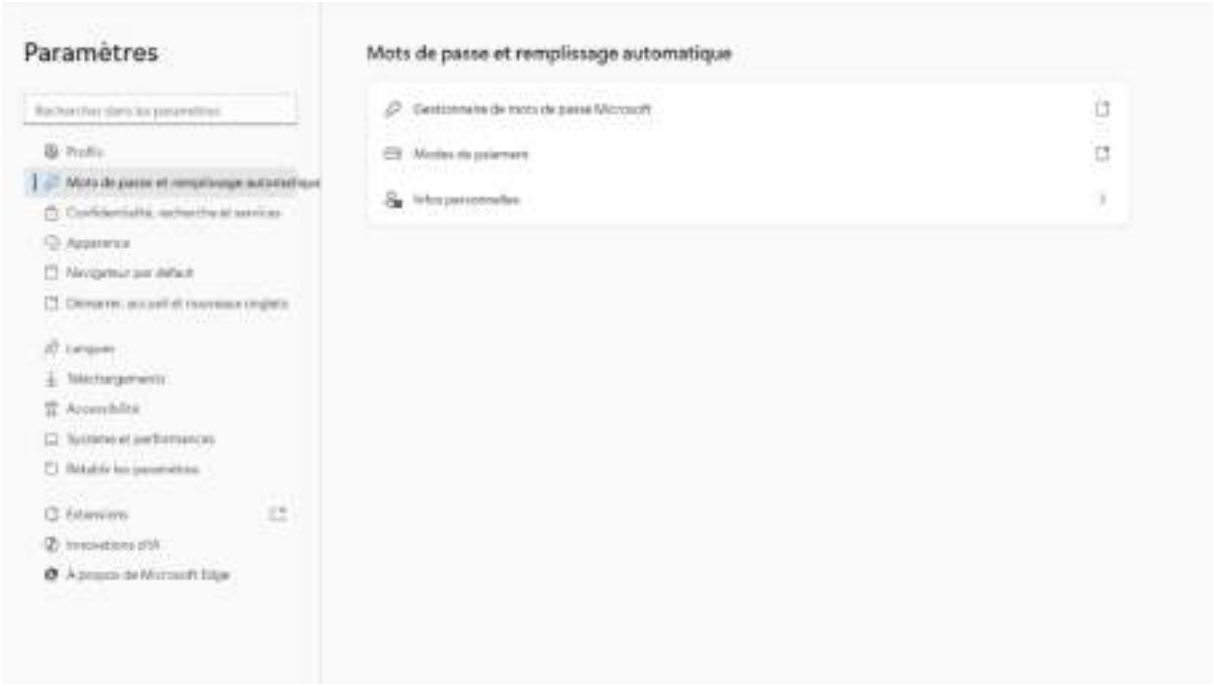
### *i. Sur Edge*

Aller sur Edge, à droite cliquer sur les trois points :



Cliquer sur Paramètres, aller dans Mots de passe et remplissage automatique, Infos Personnelles et désactiver l'option Enregistrer et remplir automatiquement les informations personnelles pour éviter que Edge puisse enregistrer les données remplies dans les formulaires :


Esnuite revenir sur Mots de passe et remplissage automatique et cliquer sur Gestionnaire de mots de passe Microsoft :

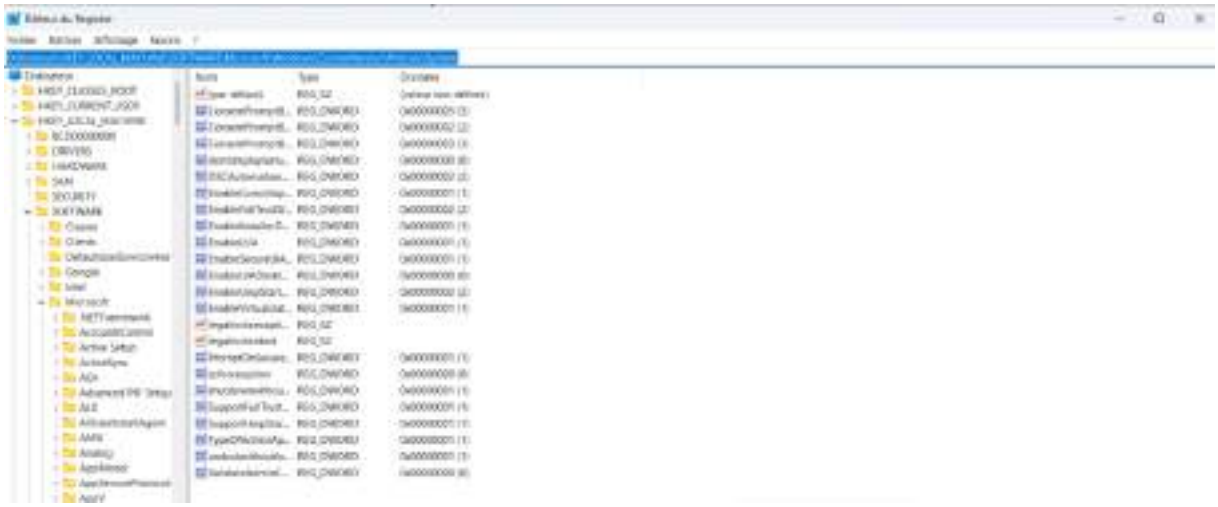



Une nouvelle page s'ouvre alors :

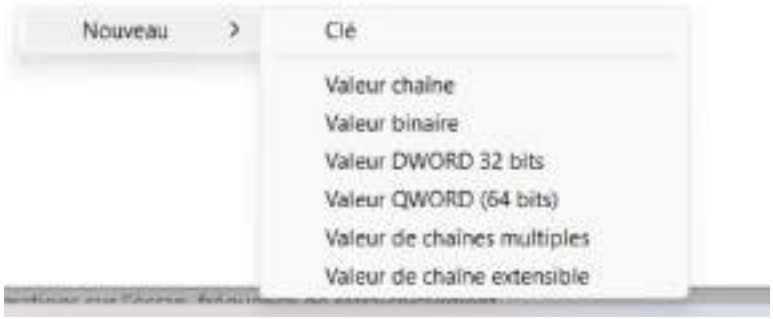

Aller sur Paramètres, puis désactiver Proposer l'enregistrement des mots de passe et Afficher et remplir automatiquement les mots de passe et les clés d'accès :

### *ii. Sur le poste de travail*

Aller dans l'Editeur de registre (win+R, regedit), mettre l'adresse HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System :



Faire un clic droit, aller sur Nouveau, cliquer sur Valeur DWORD 32 bits:




Nommer cette nouvelle valeur CacheLogonsCount et s'assurer que la valeur est bien à 0 :


Il est possible aussi créer cette valeur grâce à un script powershell :

```
# Créer la clé si elle n'existe pas
$path = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
if (-not (Test-Path $path)) {
   New-Item -Path $path -Force | Out-Null
}
# Créer la valeur CachedLogonsCount
New-ItemProperty -Path $path -Name "CachedLogonsCount" -Value 0 -PropertyType DWORD
-Force
```

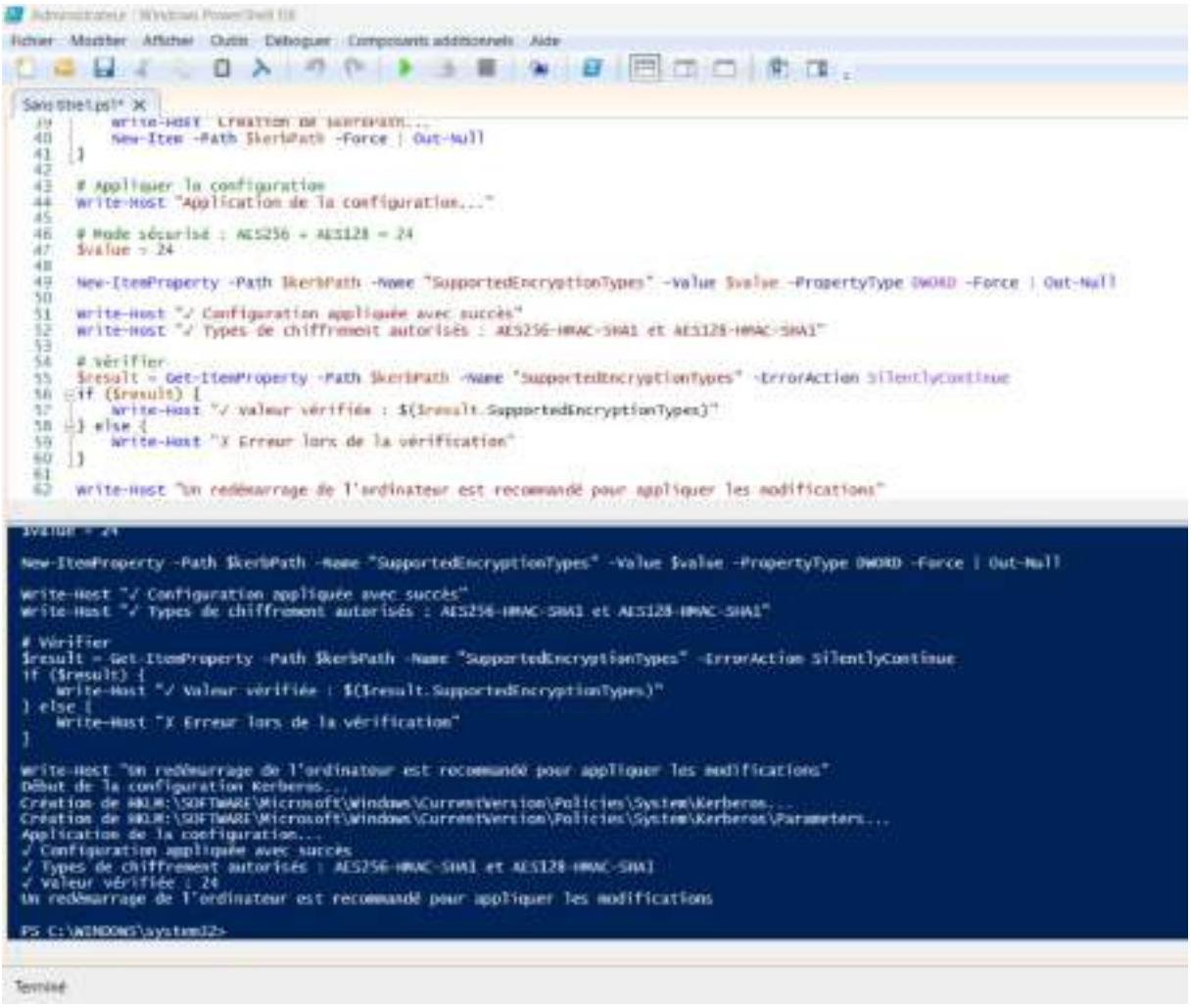
### c. Restriction des types de chiffrement Kerberos

Il est possible de changer les types de chiffrement Kerberos dans le Registre, voici le script pour le faire (à lancer en administrateur avec powershell):

```
# Exécuter en tant qu'administrateur

# Vérifier les droits administrateur
$isAdmin =
([Security.Principal.WindowsPrincipal][Security.Principal.WindowsIdentity]::GetCurrent()).IsIn
Role([Security.Principal.WindowsBuiltInRole]::Administrator)

if (-not $isAdmin) {
   Write-Host "ERREUR : Vous devez exécuter PowerShell en tant qu'administrateur"
   exit
}

Write-Host "Début de la configuration Kerberos..."

# Créer le chemin étape par étape
$basePath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies"
$systemPath = "$basePath\System"
$kerbPath = "$systemPath\Kerberos\Parameters"

# Créer Policies si n'existe pas
if (-not (Test-Path $basePath)) {
   Write-Host "Création de $basePath..."
   New-Item -Path $basePath -Force | Out-Null
}

# Créer System si n'existe pas
if (-not (Test-Path $systemPath)) {
   Write-Host "Création de $systemPath..."
   New-Item -Path $systemPath -Force | Out-Null
}

# Créer Kerberos si n'existe pas
$kerbParent = "$systemPath\Kerberos"
if (-not (Test-Path $kerbParent)) {
   Write-Host "Création de $kerbParent..."
   New-Item -Path $kerbParent -Force | Out-Null
}

# Créer Parameters
if (-not (Test-Path $kerbPath)) {
```

```
    Write-Host "Création de $kerbPath..."
    New-Item -Path $kerbPath -Force | Out-Null
}

# Appliquer la configuration
Write-Host "Application de la configuration..."

# Mode sécurisé : AES256 + AES128 = 24
$value = 24

New-ItemProperty -Path $kerbPath -Name "SupportedEncryptionTypes" -Value $value -
PropertyType DWORD -Force | Out-Null

Write-Host "✓ Configuration appliquée avec succès"
Write-Host "✓ Types de chiffrement autorisés : AES256-HMAC-SHA1 et AES128-HMAC-SHA1"

# Vérifier
$result = Get-ItemProperty -Path $kerbPath -Name "SupportedEncryptionTypes" -ErrorAction
SilentlyContinue
if ($result) {
    Write-Host "✓ Valeur vérifiée : $($result.SupportedEncryptionTypes)"
} else {
    Write-Host "✗ Erreur lors de la vérification"
}

Write-Host "Un redémarrage de l'ordinateur est recommandé pour appliquer les
modifications"
```

Résultat :



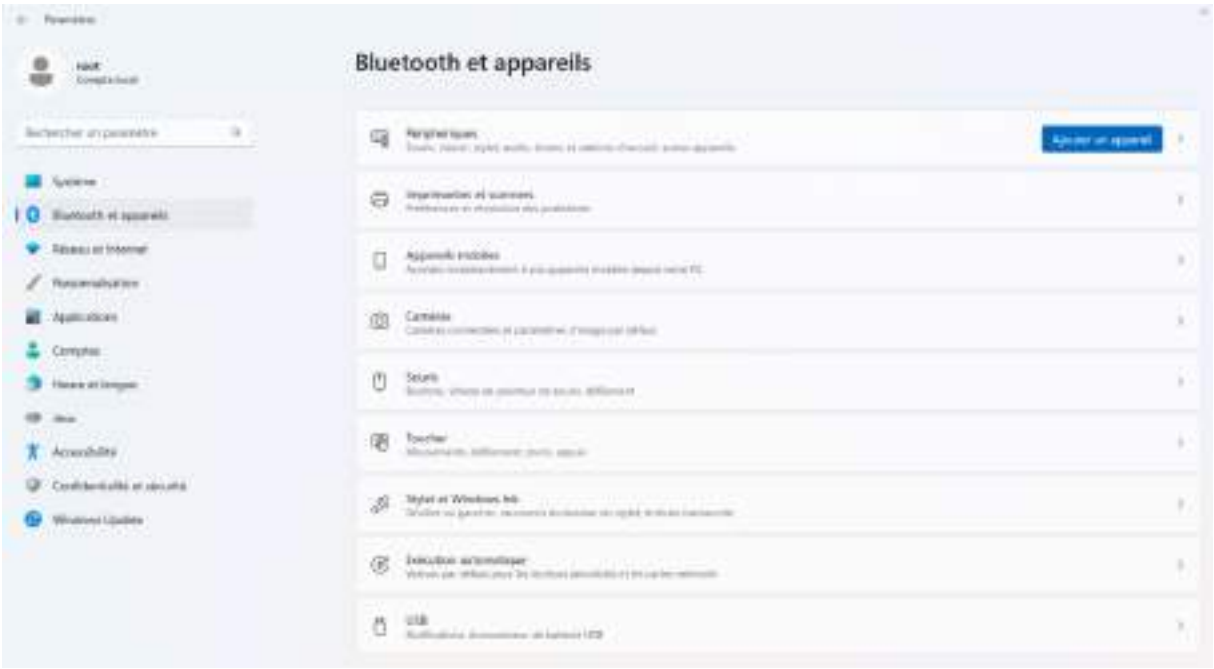

## d. Désactivation de PowerShell V2

Faire ce script powershell (en administrateur) qui permet de vérifier si la V2 est active et si oui, désactiver cette fonctionnalité :

```
#Vérifier si PowerShellV2 existe
$powershellv2 = Get-WindowsOptionalFeature -online -featurename
MicrosoftWindowsPowershellV2

#Si oui le désactiver
if ($powershellv2.State -eq 'Enabled') {
   write-host "PowershellV2 détecté - Suppression en cours"
   Disable-WindowsOptionalFeature -FeatureName MicrosoftWindowsPowershellV2 -Online -
NoRestart
}
```

## e. Désactivation d'AutoRun

Aller dans Paramètres, Bluetooth et Appareils :




Cliquer sur Exécution automatique et décocher Utiliser l'exécution automatique pour tous les médias et tous les périphériques :


# V. Protection réseau (Enzo)

## a. Activation de la signature SMB/LDAP

La signature SMB (Server Message Block) permet d'ajouter une signature cryptographique (un hachage) à chaque paquet SMB échangé entre un client et un serveur. Cette signature garantit que :

- L'intégrité des données est assurée (personne n'a modifié les paquets en cours de route).
- L'authenticité est vérifiée (les paquets viennent bien du bon client/serveur et pas d'un attaquant qui s'intercale – attaque man-in-the-middle).

La signature LDAP (Lightweight Directory Access Protocol) est un protocole de communication qui permet aux clients (applications, ordinateurs, utilisateurs) de dialoguer avec un service d'annuaire (comme Active Directory ou OpenLDAP).

Il sert à :

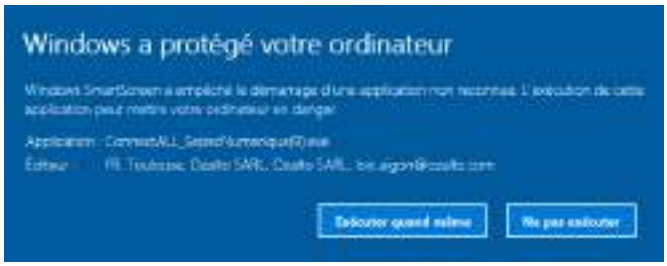
- Rechercher des informations (ex. trouver un utilisateur, un groupe, une imprimante).
- Lire/mettre à jour des données stockées dans l'annuaire (ex. modifier un mot de passe).
- Authentifier les utilisateurs et applications via l'annuaire.

## b. Configuration des paramètres de sécurité des membres de domaine.

La sécurité des membres de domaine protège l'intégrité et la confidentialité des communications entre un poste et son contrôleur de domaine, en imposant signature, chiffrement et refus des connexions non sécurisées.

## c. Activation de SmartScreen :

Microsoft Defender SmartScreen protège des sites web et applications de hameçonnage et de programmes malveillants, et le téléchargement de fichiers potentiellement malveillants. Cette sécurité affiche un avertissement informant l'utilisateur que le site pourrait être malveillant ou pour les fichiers, un avertissement demandant l'attention




Paramètre > Confidentialité et sécurité > Sécurité Windows > Contrôle des applications et du navigateur > Protection fondée sur la réputation

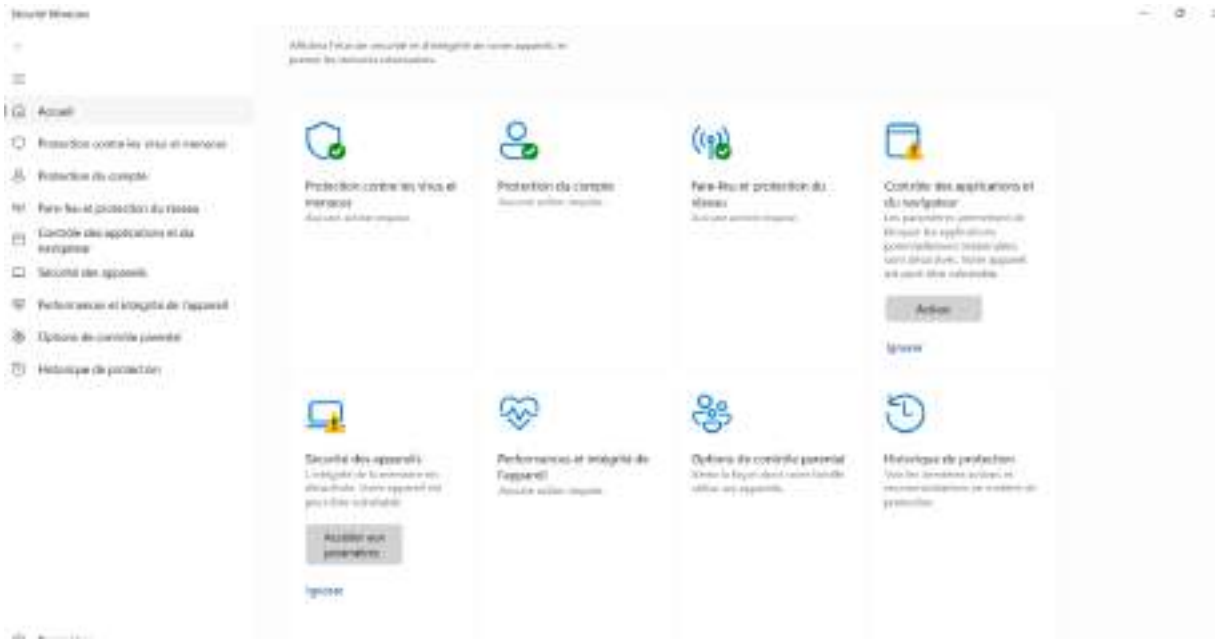

Ce paramètre doit être activé

Dans Paramètres de protection fondée sur la réputation, on peut choisir différents paramètres à activer individuellement que propose SmartScreen

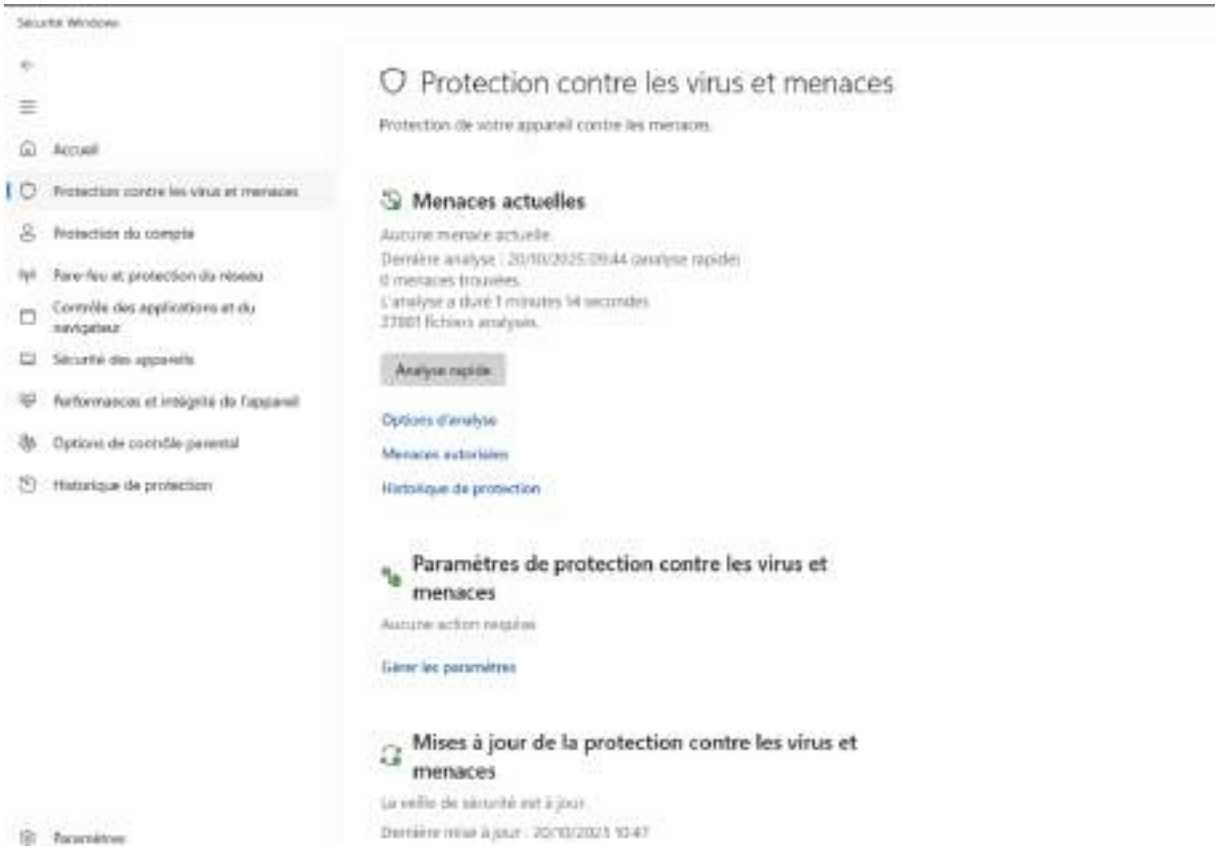

# VI. Paramètres de Windows Defender (Sarah)

## a. Activation de diverses protections dans Windows Defender

Aller dans Sécurité Windows :



Aller dans Protection contre les virus et menaces et sous Paramètres de protection contre les virus et menaces cliquer sur Gérer les paramètres :




Défiler jusqu'à Dispositif d'accès contrôlé aux dossiers et cliquer sur Gérer l'accès contrôlé aux dossiers :


Activer Dispositif d'accès contrôlé aux dossiers et valider le message :

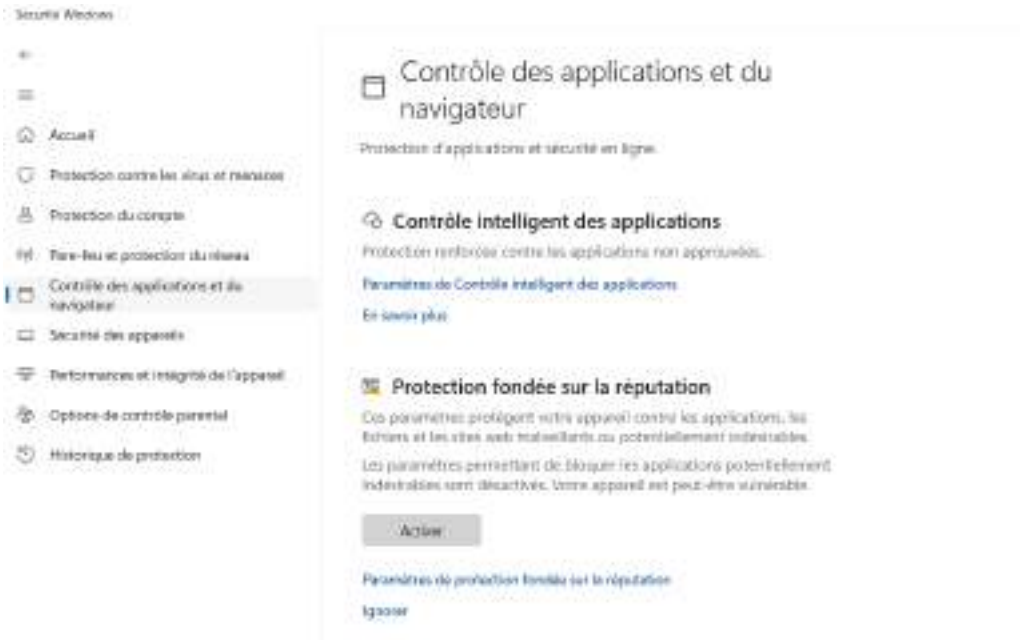

Il est aussi possible de configurer OneDrive pour récupérer des fichiers lors d'une attaque de ransomware, mais pour cela GSB doit avoir choisi Onedrive comme solution de stockage de données.

Une fois le paramètre de contrôle d'accès activé, il est possible de définir quels dossiers doivent être protégé et de voir l'historique de blocage :

Ceci est très utile notamment pour les dossiers contenant des données sensibles (notamment données de santé).

S'assurer que le pare-feu est bien actif dans Pare-feu et protection du réseau :


Dans Contrôle des applications et navigateur, cliquer sur Activer en dessous de Protection fondée sur la réputation :




## b. Configuration des fonctionnalités cloud et des protections contre les exploits système.

Dans Sécurité Windows, aller dans Protection contre les virus et menaces et s'assurer que Protection dans le cloud est bien activé :


Dans Sécurité Windows, aller dans Contrôle des applications et cliquer sur Paramètres d'Exploit Protection sous Exploit Protection :


Dans Paramètres d'Exploit Protection, tout mettre en Activé :

# VII. Sécurité MS Office (Enzo)

Sécuriser les applications Microsoft Office (Word, Excel, PowerPoint, Outlook) contre les attaques de malspam — c'est-à-dire les courriels malveillants contenant des fichiers piégés (macros, scripts, liens ou fichiers infectés).

Ces attaques visent souvent à exécuter du code sur la machine de l'utilisateur via des macros VBA, contenu externe, ou liens suspects.

## a. Désactivation des macros non signées :

Les macros VBA sont souvent utilisées pour exécuter du code malveillant.

Pour les bloquer :

Ouvrir Word (ou Excel, PowerPoint)

Aller dans Fichier > Options > Centre de gestion de la confidentialité > Paramètres du Centre de gestion de la confidentialité

Sélectionner Paramètres des macros

Cocher Désactiver toutes les macros avec notification

(Option recommandée : l'utilisateur doit explicitement les activer s'il a confiance)

ou Désactiver toutes les macros sauf celles signées numériquement

## b. Blocage des fichiers téléchargés depuis Internet

Les fichiers Office téléchargés (email, navigateur, clé USB) peuvent être dangereux.

Pour les protéger :

Toujours enregistrer les fichiers reçus dans un dossier sécurisé.

Ouvrir Word > Options > Centre de gestion de la confidentialité > Paramètres du Centre de gestion de la confidentialité

Aller dans Paramètres du mode protégé

Cocher Activer le mode protégé pour les fichiers provenant d'Internet

Cocher aussi :

Activer le mode protégé pour les fichiers situés dans des emplacements potentiellement dangereux

Activer le mode protégé pour les pièces jointes Outlook

## c. Désactivation du contenu externe (liens et données web)

Les pirates utilisent souvent des liens distants ou images externes pour exécuter du code à distance.

Pour bloquer ces contenus :

Dans Word/Excel > Options > Centre de gestion de la confidentialité > Paramètres du Centre de gestion de la confidentialité

Cliquer sur Paramètres du contenu externe

Cocher :

Ne pas autoriser les connexions automatiques à des données

Ne pas télécharger automatiquement les images dans les documents

## d. Sécurisation d'Outlook (filtrage anti-malspam et pièces jointes)

Activer le filtrage automatique du courrier indésirable :

Dans Outlook > Accueil > Courrier indésirable > Options du courrier indésirable

Sélectionner Haute

Cocher Ne pas télécharger les images dans les messages HTML

Bloquer les extensions de fichiers dangereuses :

Outlook bloque par défaut les fichiers .exe, .js, .vbs, etc.

Pour vérifier :

Regedit > HKEY_CURRENT_USER\Software\Microsoft\Office\<version>\Outlook\Security

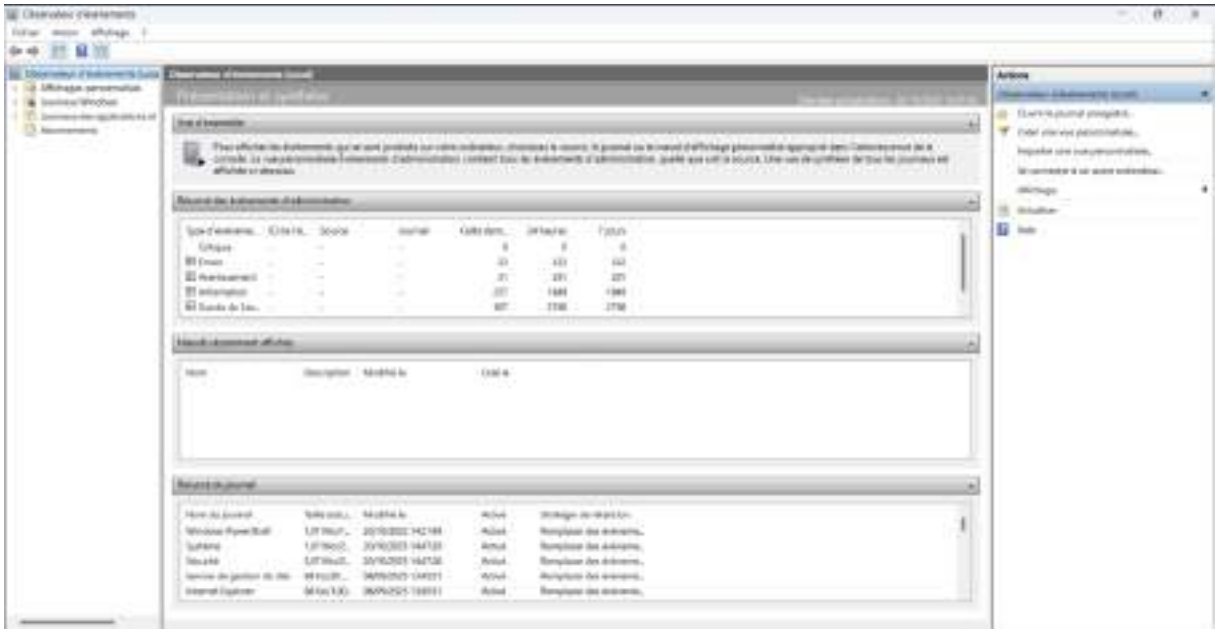
Créer ou modifier la clé Level1Remove si besoin (laisser vide pour bloquer tous les fichiers à risque).

# VIII. Journalisation des Événements Windows (Sarah)

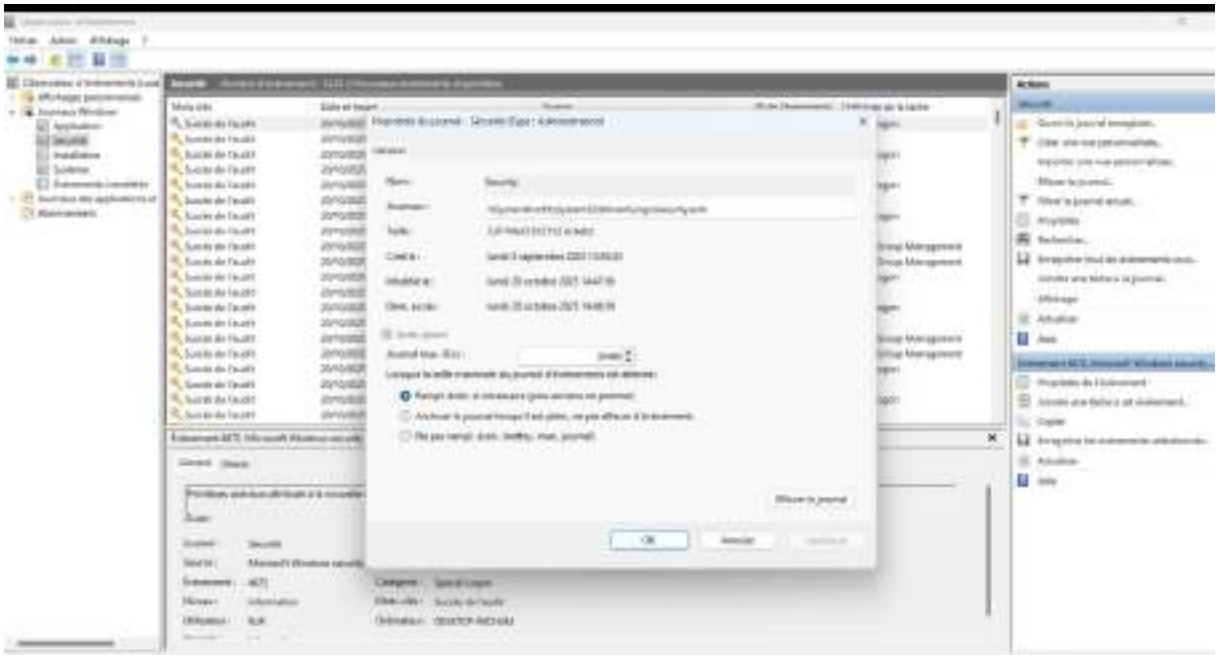
## a. Augmentation de la taille des journaux d'événements de sécurité

### *i. Procédure manuelle*

Aller dans Observateur d'Evenements :



Aller dans Journaux Windows, Sécurité et cliquer sur Propriétés dans le volet à droite :



Changer la taille du Journal max (ko), par exemple ici à 28 800, et cliquer sur Ok :

#### *ii. Procédure powershell*

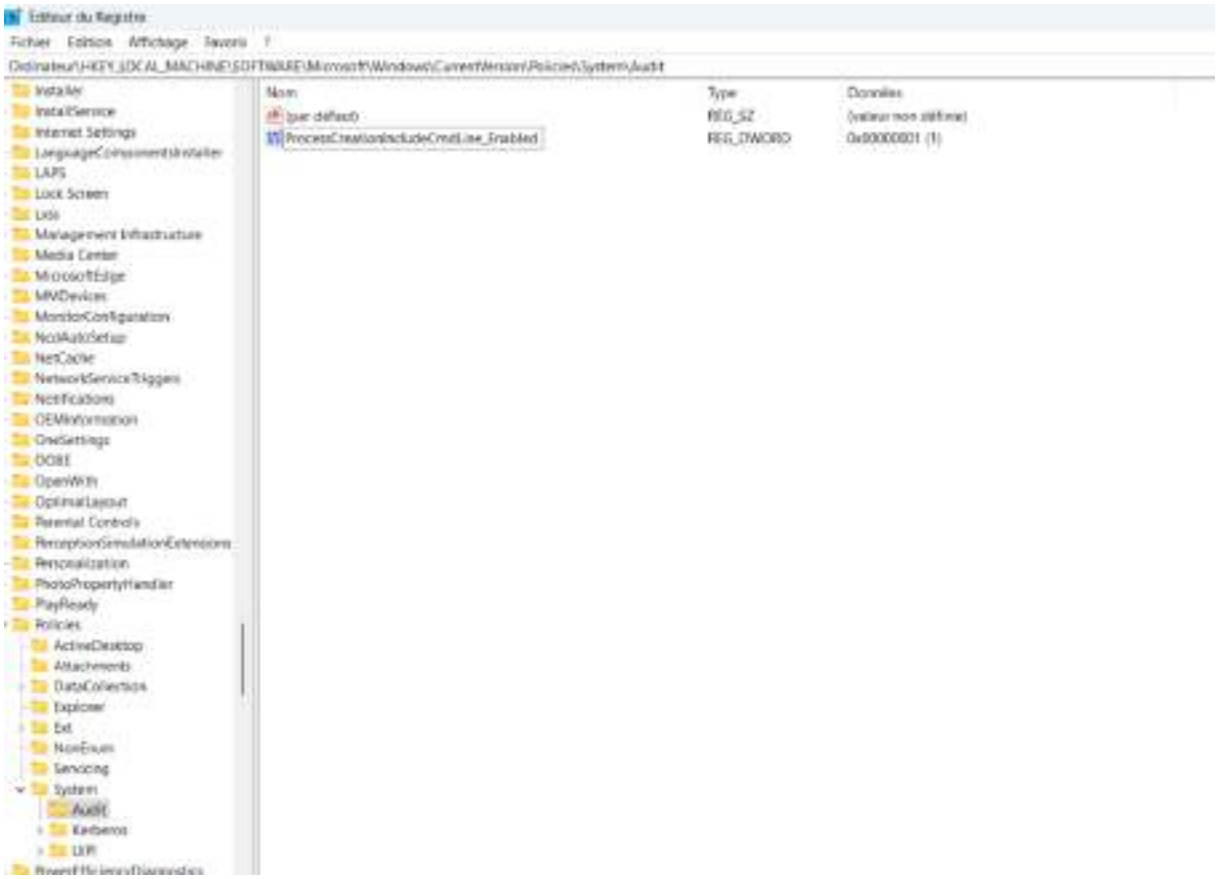
Lancer un powershell en administrateur et faire cette commande : Limit-EventLog -LogName Security -MaximumSize 28KB

### b. Activation de la journalisation des données de ligne de commande pour la création de processus

Pour activer la journalisation, il est possible de changer les paramètres de stratégie de groupe ou de créer une clé de registre.

Pour créer la clé de registre, faire la commande suivante dans powershell en administrateur :

reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit" /v ProcessCreationIncludeCmdLine_Enabled /t REG_DWORD /d 1 /f



## IX. Mesures de sécurité avancées (Enzo)

Ces mesures permettent de détecter et tracer toute activité suspecte ou malveillante, même si elle provient d'un utilisateur interne ou d'un script.

Elles facilitent les analyses post-incident, renforcent la conformité au RGPD et aux bonnes pratiques ANSSI, et réduisent considérablement la surface d'attaque.

## a. Activation des paramètres de sécurité avancés

Les “paramètres de sécurité avancés” regroupent différentes stratégies locales renforçant les contrôles sur les comptes, les connexions et les services système.

Ouvrir secpol.msc → Stratégies locales > Options de sécurité

Vérifier / activer les paramètres suivants :

| Paramètre | Valeur recommandée | Description |
|---|---|---|
| Comptes : verrouiller les comptes après 3 tentatives | Activé | Empêche les attaques par force brute. |
| Comptes : durée du verrouillage = 30 minutes | Activé | Définit la durée du blocage du compte. |
| Comptes : longueur minimale du mot de passe = 12 caractères | Activé | Conformité RGPD / ANSSI. |
| Contrôle d’accès réseau : autoriser les connexions anonymes | Désactivé | Empêche l’accès réseau non authentifié. |
| Réseau : autoriser le stockage de mots de passe en clair | Désactivé | Évite le stockage d’identifiants en texte clair. |
| Utilisateur : élévation UAC requise | Activé | Garantit que toute action admin demande une confirmation. |

## b. Activation de la journalisation des modules PowerShell et des blocs de scripts

La journalisation PowerShell permet de conserver une trace complète de chaque commande, module ou script exécuté sur la machine.

Win + R → gpedit.msc

Naviguer vers :
Configuration ordinateur → Modèles d'administration → Composants Windows → Windows PowerShell

Activer les paramètres suivants :

- Activer la journalisation des modules
- Activer la journalisation des blocs de scripts
- Activer la transcription PowerShell

Pour la transcription, définir un dossier sécurisé où seront enregistrés les journaux :
Exemple : C:\Logs\PowerShell

## c. Configuration des politiques d'audit

L'audit Windows permet de surveiller les événements critiques (connexions, accès fichiers, changements de stratégie, etc.). Ces journaux sont indispensables pour détecter les intrusions, comportements anormaux ou actions administratives suspectes.

Ces journaux permettent de retracer toute action suspecte ou non autorisée sur le système, pour les configurer :

Win + R → Ouvrir secpol.msc
Aller dans Stratégies locales → Stratégie d'audit
Activer les options suivantes :

| Catégorie d'audit | Paramètre | État recommandé |
|---|---|---|
| Audit des événements d'ouverture de session | Succès et échecs | Journalise toutes les connexions locales et réseau. |
| Audit des événements d'accès aux objets | Succès et échecs | Suit l'accès aux fichiers, dossiers ou clés sensibles. |
| Audit des événements d'utilisation de privilèges | Succès | Enregistre les actions des comptes administrateurs. |

| | | |
|---|---|---|
| Audit des modifications de stratégie | Succès | Permet de suivre les changements de sécurité. |
| Audit des événements système | Succès et échecs | Surveille les arrêts anormaux, redémarrages ou erreurs critiques. |

Pour plus de détails, ouvrir Observateur d'événements → Journaux Windows → Sécurité

## X. Sécurité lsass (Sarah)

Ici il s'agit de renforcer LSASS, qui permet de valider les utilisateurs pour les connexions locales et distantes et appliquer des stratégies de sécurité locales, contre le vol d'informations d'identification.

Il faut pour cela aller dans l'éditeur de registre, aller à la HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LSASS.exe.


S'assurer ici que la valeur est bien à 8.

En script powershell :

```
# Crée la clé LSASS.exe si elle n'existe pas déjà
New-Item -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LSASS.exe" -Force | Out-Null

# Crée ou met à jour la valeur DWORD AuditLevel à 0x00000008
New-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LSASS.exe" `
  -Name "AuditLevel" -PropertyType DWord -Value 0x00000008 -Force
```

```
# Vérification
Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LSASS.exe" | Select-Object AuditLevel
```

# XI. Désinstallation des Applications Indésirables (Enzo)

Windows 11 installe automatiquement de nombreuses applications grand public (ex. Xbox, Spotify, Candy Crush, News, 3D Viewer…).

Ces applications ne sont pas nécessaires dans un environnement professionnel et peuvent :

- être sources de failles potentielles
- générer du trafic réseau inutile
- collecter des données d'utilisation.

Le but est donc de les supprimer via PowerShell ou via les paramètres Windows, en conservant uniquement les outils essentiels (Office, Edge, utilitaires système, etc.).

Manuellement :

Paramètres > Applications > Applications et fonctionnalités

Trier la liste par "Date d'installation" ou "Nom"

Sélectionner les applications inutiles (par exemple : 3D Viewer, Xbox, News, OneNote, Groove Music, Cortana, etc.)

Cliquer sur Désinstaller

Via Powershell :

Exemple pour Xbox :

*Get-AppxPackage *xbox* | Remove-AppxPackage*

# XII. Pare-feu et Blocage des Connexions (Sarah)

## a. Activation du Pare-feu Windows

Le pare-feu Windows est déjà activé par défaut, mais cela peut être vérifié dans Sécurité Windows, Pare-feu et protection du réseau :


## b. Blocage des connexions à partir de binaires spécifiques (LOLBins)

Les attaques LOLBins ciblent certains exe. Pour pouvoir bloquer les connexions, il faut analyser quels exe sont activement utilisés. Cela permettra de bloquer les connexions nécessaires sans impacter la production.

Un script peut être utilisé pour ce faire :

```
#Rajouter à la liste ou enlever à la liste les binaires
$binaries = @(
  "C:\Windows\System32\rundll32.exe",
  "C:\Windows\System32\regsvr32.exe",
  "C:\Windows\System32\certutil.exe"
)

foreach ($bin in $binaries) {
  $name = "Block - " + (Split-Path $bin -Leaf)
  # si la règle existe déjà, on la remplace
  if (Get-NetFirewallRule -DisplayName $name -ErrorAction SilentlyContinue) {
    Remove-NetFirewallRule -DisplayName $name
  }
  New-NetFirewallRule -DisplayName $name `
    -Direction Outbound -Program $bin -Action Block -Profile Any -Enabled True
}
```

## XIII. Mises à jour Windows et AutoRun (Enzo)

Ici, on veut garantir que le système Windows reste à jour face aux failles de sécurité connues et empêcher l'exécution automatique de programmes potentiellement dangereux depuis des périphériques externes (clés USB, disques externes, CD/DVD).

Ces deux actions permettent de limiter les attaques de type malware, ransomware ou exploitation de vulnérabilités connues.

Pour l'activation des mises à jour automatiques de Windows avec l'interface graphique :

Ouvrir Paramètres > Windows Update

Cliquer sur Options avancées

Vérifier que les options suivantes sont activées :

- Télécharger automatiquement les mises à jour
- Installer automatiquement les mises à jour de sécurité
- Recevoir les mises à jour pour d'autres produits Microsoft

Redémarrer le poste si nécessaire.

L'AutoRun permet à Windows d'exécuter automatiquement un fichier (souvent autorun.inf) lorsqu'un

Cette fonctionnalité est pratique, mais dangereuse : elle est souvent utilisée pour propager des malwares via des clés USB ou disques externes.

Pour la désactivation de l'AutoRun avec l'interface graphique :

Ouvrir Panneau de configuration > Matériel et audio > Exécution automatique

Décocher Utiliser l'exécution automatique pour tous les médias et périphériques

Cliquer sur Enregistrer

# Documentation Linux Mint

## I. Mise à jour du système (Tsiaro)

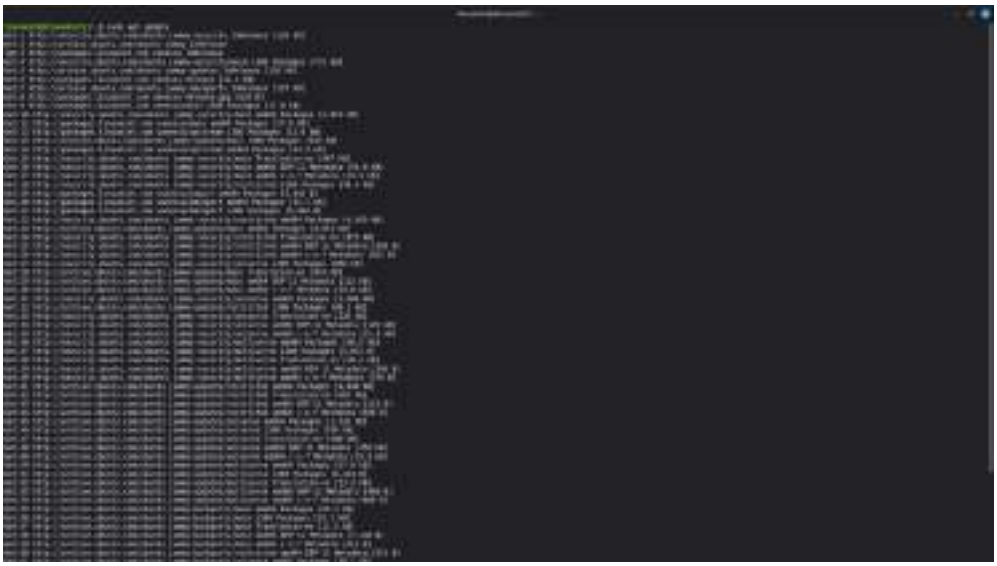
### 1. Objectif de sécurité

Les mises à jour incluent des correctifs de sécurité critiques qui corrigent les vulnérabilités découvertes. En maintenant le système à jour, vous réduisez le risque d'exploitation de failles de sécurité connues.

#### 1.1 Procédure

**Étape 1** : Mise à jour de la liste des paquets

Commande : Sudo apt update



**Étape 2 :** Mise à niveau des paquets installés

Commande : sudo apt upgrade –y


Tsiaroniaina-rianala RAMANANTSIALONINA, Gokhan YILMAZ
Enzo ROESCH et Sarah NIED

**Étape 3 :** Nettoyage des paquets obsolète

Commandes : sudo apt autoremove –y /

```
linuxmint@linuxmint21:~$ sudo apt autoremove
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 10 not upgraded.
linuxmint@linuxmint21:~$
```

sudo apt autoclean

```
linuxmint@linuxmint21:~$ sudo apt autoclean
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
linuxmint@linuxmint21:~$
```

## 1.2 Automatisation des mises à jour

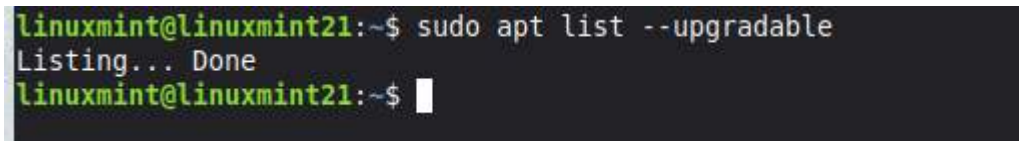
Pour assurer une sécurité continue, on va configurer les mises à jour automatiques :

Commandes : sudo apt install unattended-upgrades –y

Et ensuite faire cette commande : sudo dpkg-reconfigure --priority=low unattended-upgrades et choisir “YES”

### 1.3 Vérification

Commande : apt list –upgradable




On peut voir que tous les paquets ont été installés

# I. Configuration du pare-feu UFW

## 1. Objectif de sécurité

Un pare-feu bien configuré limite les connexions non autorisées à votre système. UFW (Uncomplicated Firewall) est un outil convivial pour configurer le pare-feu sur Linux, aidant à bloquer ou autoriser le trafic réseau de manière contrôlée.

## 2. Installation de UFW

Commande : sudo apt install ufw –y

```
linuxmint@linuxmint21:~$ sudo apt install ufw -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.1-4ubuntu0.1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
linuxmint@linuxmint21:~$
```

## 3. Configuration initiale

Étape 1 : Bloquer tout le trafic entrant par défaut

Commande : sudo ufw default deny incoming

```
linuxmint@linuxmint21:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
linuxmint@linuxmint21:~$
```

Étape 2 : Autoriser tout le trafic sortant par défaut

Commande : sudo ufw default allow outgoing

```
linuxmint@linuxmint21:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
linuxmint@linuxmint21:~$
```

**Étape 3 :** Autoriser SSH dans ufw

Commande : sudo ufw allow ssh ou sudo ufw allow 22/tcp

```
linuxmint@linuxmint21:~$  sudo ufw allow ssh
Rules updated
Rules updated (v6)
linuxmint@linuxmint21:~$
```

**Étape 4 :** Autoriser d'autres services si nécessaire

Dans notre cas on va autoriser le port 80(HTTP), 443(HTTPS), 53(DNS)

Commandes : sudo ufw allow 80/tcp , sudo ufw allow 443/tcp, sudo ufw allow 53

```
linuxmint@linuxmint21:~$ sudo ufw allow 80/tcp
Rules updated
Rules updated (v6)
linuxmint@linuxmint21:~$ sudo ufw allow 443/tcp
Rules updated
Rules updated (v6)
linuxmint@linuxmint21:~$ sudo ufw allow 53
Rules updated
Rules updated (v6)
linuxmint@linuxmint21:~$
```

**Étape 5:** Activer le Pare-feu

Commande : sudo ufw enable et ensuite taper "y"

```
linuxmint@linuxmint21:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
linuxmint@linuxmint21:~$
```

4. Vérification

   Commande : sudo ufw status verbose

   On peut voir que le pare-feu est actif et on peut également voir les règles actives

```
linuxmint@linuxmint21:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
80/tcp                     ALLOW IN    Anywhere
443/tcp                    ALLOW IN    Anywhere
53                         ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
80/tcp (v6)                ALLOW IN    Anywhere (v6)
443/tcp (v6)               ALLOW IN    Anywhere (v6)
53 (v6)                    ALLOW IN    Anywhere (v6)

linuxmint@linuxmint21:~$
```

II. Désactivation des services non nécessaires

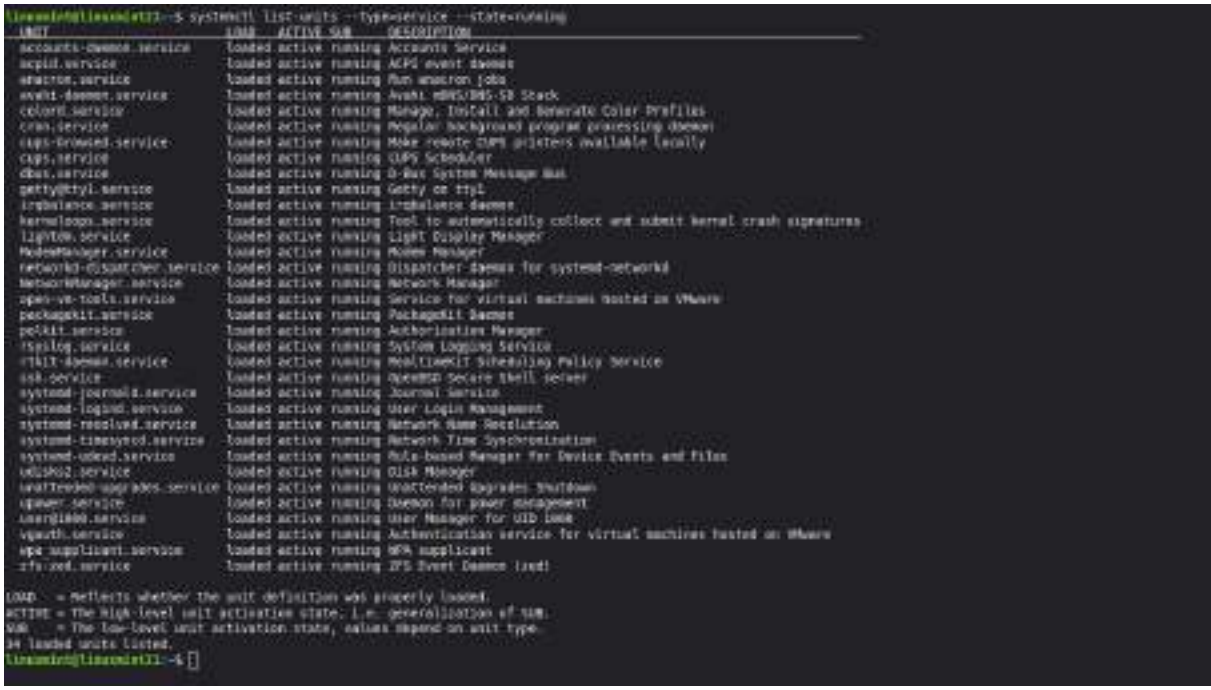
1. Objectif de sécurité

   La désactivation de services non nécessaires réduit la surface d'attaque potentielle. Chaque service actif peut être une porte d'entrée pour les attaquants. En désactivant les services inutiles, vous minimisez les risques de sécurité.

2. Lister les services actifs

   Commande : systemctl list-units --type=service --state=running

   On aura la liste complète des services actifs




3. Services à désactiver pour un poste nomade

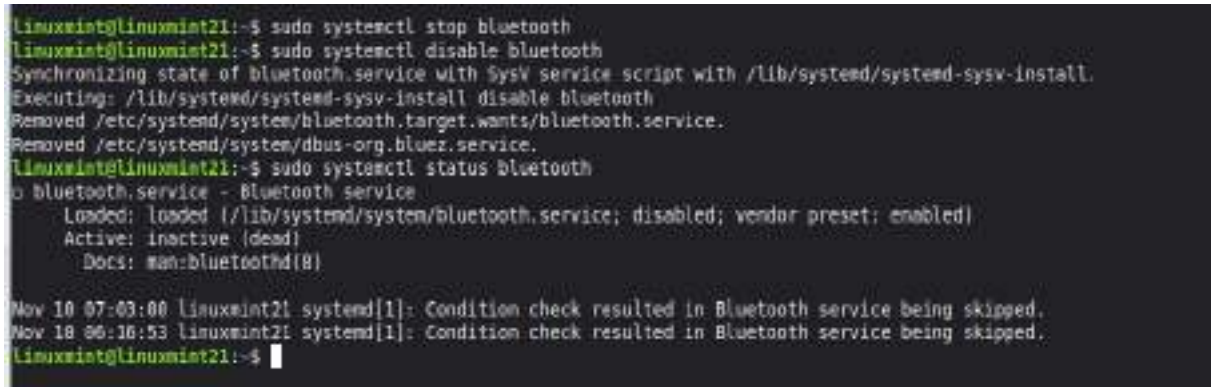
**Étape 1 :** Identifier les services non nécessaires

Pour un poste de visiteur médical, voici les services généralement inutiles :

- systemctl status bluetooth
- systemctl status cups
- systemctl status avahi-daemon
- systemctl status apache2
- systemctl status mysql

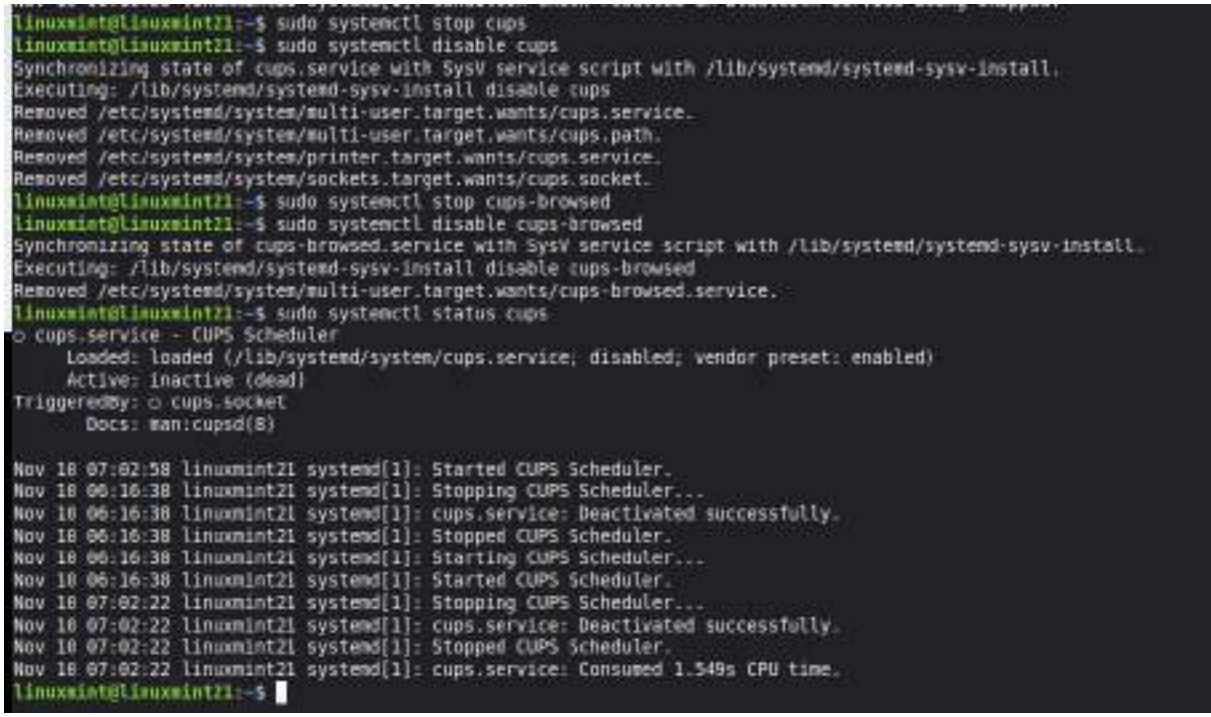
**Étape 2 :** Désactiver les services Bluetooth

Commande : sudo systemctl stop bluetooth / sudo systemctl disable bluetooth



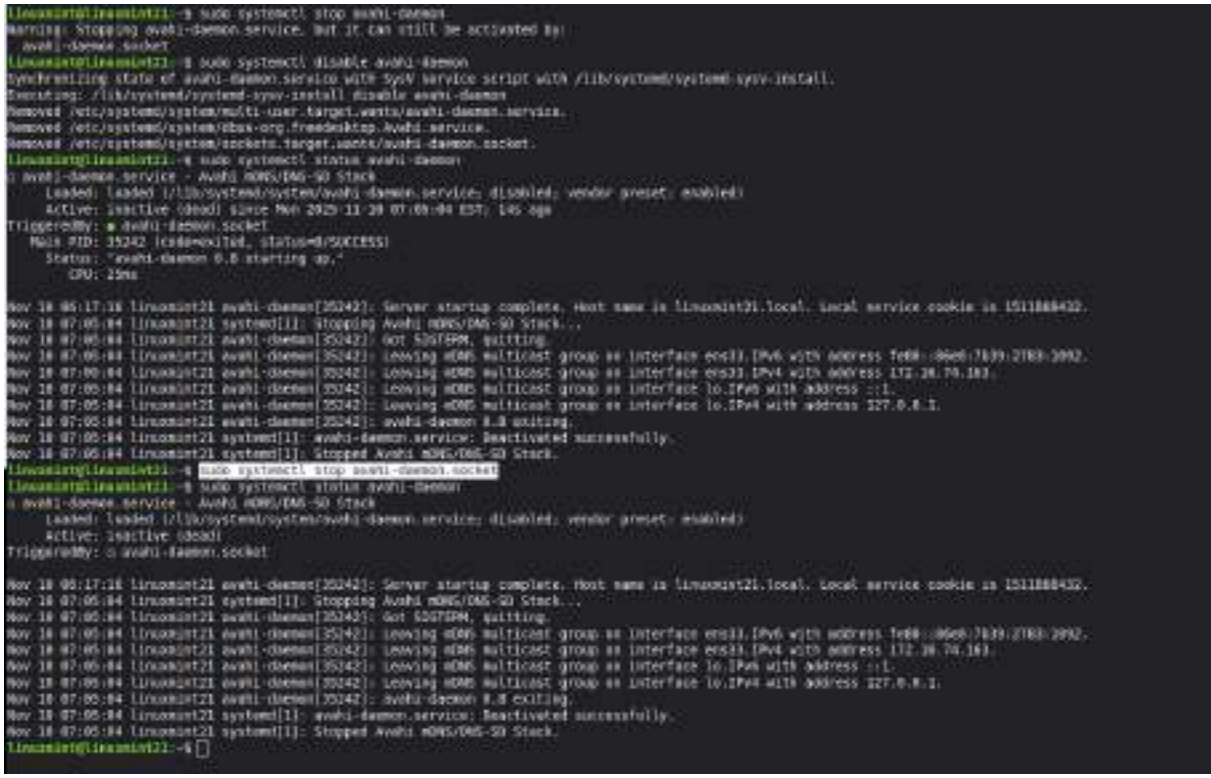

**Étape 3 :** Désactiver le service d'impression CUPS

Commandes : sudo systemctl stop cups / sudo systemctl disable cups / sudo systemctl stop cups-browsed / sudo systemctl disable cups-browsed




**Étape 4 :** Désactiver Avahi

Commandes : sudo systemctl stop avahi-daemon / sudo systemctl disable avahi-daemon / sudo systemctl stop avahi-daemon.socket



## III. Sécurisation de SSH

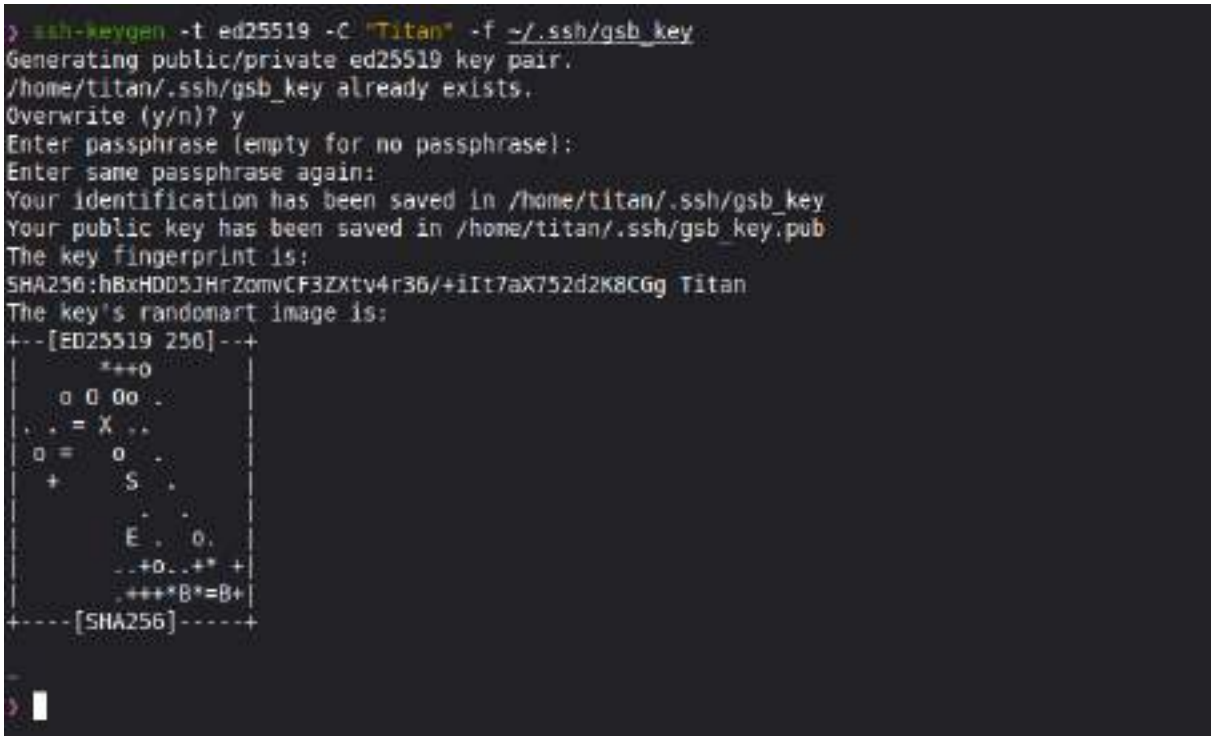
1. Désactivation de l'accès root via SSH

   Commande : sudo nano /etc/ssh/sshd_config et ensuite modifier “PermitRootLogin no”


2. Authentification par clé uniquement

   Étape 1: Sur le PC Hôte on va générer une clé SSH

   Commande : ssh-keygen -t ed25519 -C "Titan" -f ~/.ssh/gsb_key




La paraphrase ici c'est Asakura123.

Étape 2: Copier la clé publique vers le Pc LinuxMint

Commande : ssh-copy-id -i ~/.ssh/gsb_key.pub linuxmint@172.16.74.163


Maintenant on peut se connecter en SSH par clé :

Étape 3: Sécurisation du serveur SSH

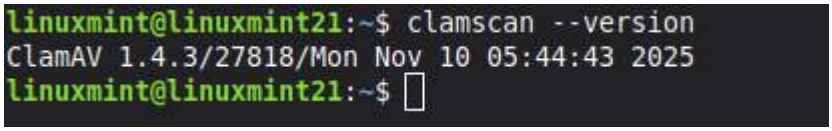
Pour sécuriser le serveur ssh on va modifier la configuration de SSH

Commande : sudo nano /etc/ssh/sshd_config

IV. Installation et Configuration de ClamAV et Lynis

1. Installation de ClamAV (Antivirus)

Commandes : sudo apt update / sudo apt install clamav clamav-daemon –y / clamscan –version

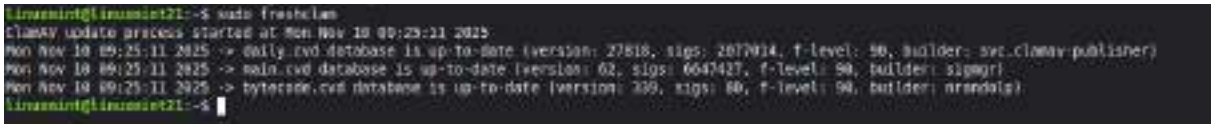



Étape 1 : Arrêter le service de mise à jour automatique

Commande : sudo systemctl stop clamav-freshclam

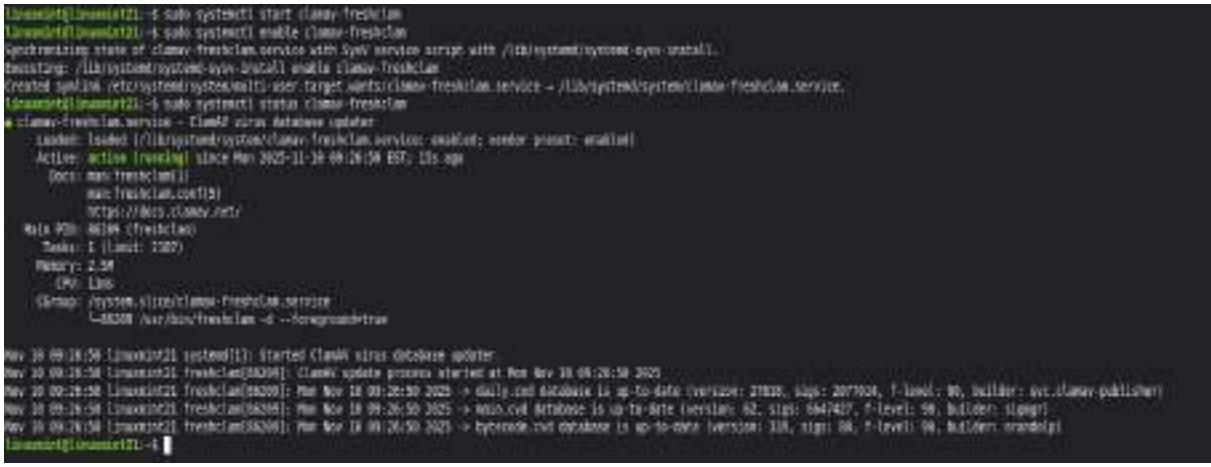
Étape 2 : Mettre à jour manuellement la base de données

Commande : sudo freshclam



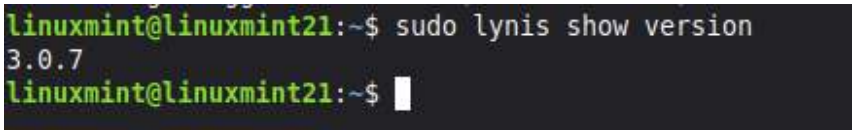
Étape 3 : Redémarrer le service

sudo systemctl start clamav-freshclam / sudo systemctl enable clamav-freshclam



V. Installation et Configuration de Lynis

Commandes : sudo apt install lynis –y / lynis show version


Premier audit de sécurité :

Lancer un audit complet

Commande : sudo lynis audit system

## VI. Configuration des Règles iptables (Gökhan)

Iptables est un outil puissant pour configurer les règles de pare-feu sur Linux. La configuration appropriée des règles iptables contribue à contrôler le trafic réseau entrant et sortant, renforçant ainsi la sécurité.

**Je vous montre comment procéder à son installation, taper les commandes dans l'ordre ci-dessous :**

sudo apt update

Sudo apt install iptables-persistent -y

**Les 2 commandes ci-dessous permettent d'enlever toutes les règles par défauts existantes.**

Sudo iptables -F

Sudo iptables -X

Politique par défaut de iptables :

sudo iptables -P INPUT DROP

sudo iptables -P FORWARD DROP

sudo iptables -P OUTPUT ACCEPT

**Pour Autoriser le trafic entrant sur localhost :**

sudo iptables -A INPUT -i lo -j ACCEPT.

**Autoriser les connexions déjà établies :**

sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

**Autoriser SSH, HTTP, HTTPS :**

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

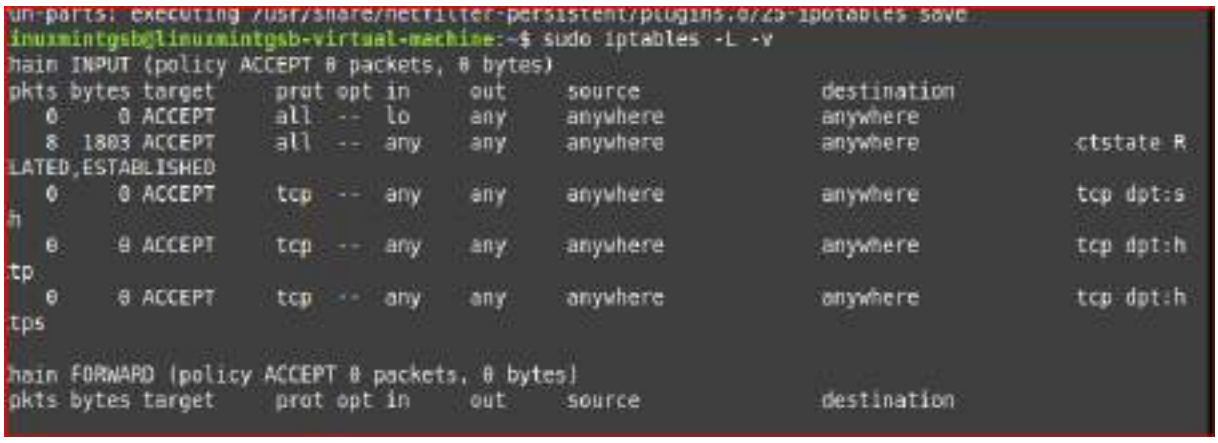
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

**Sauvegarder la configuration :**

sudo netfilter-persistent save.

Sudo iptables -L -v.




## VII. Désactivation de l'Exécution de Scripts dans /tmp (Gökhan)

Désactiver l'exécution de scripts dans le répertoire /tmp limite les risques d'exécution de scripts malveillants, renforçant ainsi la sécurité du système.

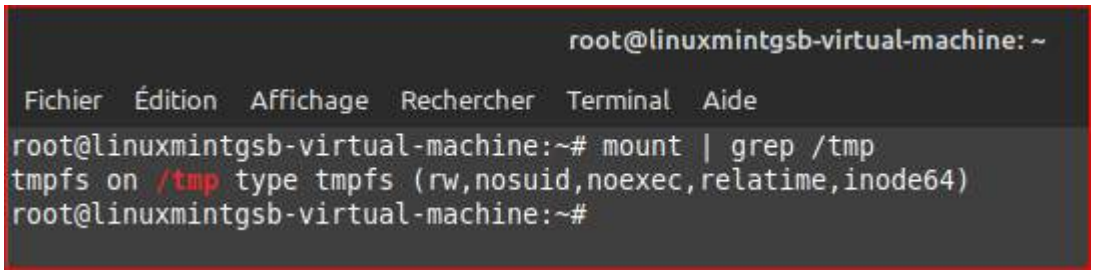
Pour cela, il faut tout d'abord éditer le fichier : sudo nano /etc/fstab

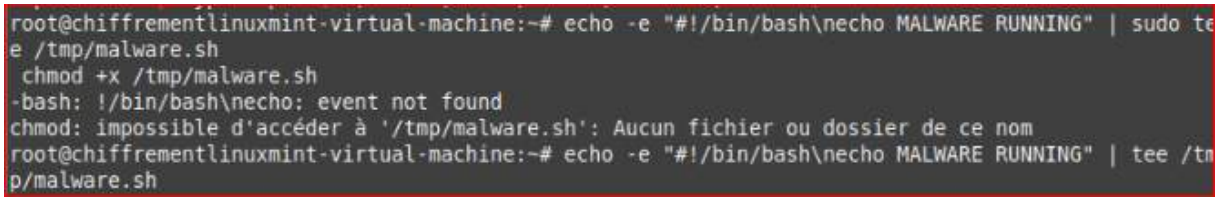
Ajouter cette ligne ; tmpfs /tmp tmpfs defaults,noexec,nosuid 0 0

Redémarrer et/ou remonter /tmp : sudo mount -o remount,noexec,nosuid /tmp

Puis, vérifier à l'aide de la commande ci-dessous et comme indiqué « noexec,nosuid »

Mount | grep /tmp




## VIII. Restriction des droits sur les fichiers sensibles (Gökhan)

**Objectif :**

Nous devons empêcher l'accès à certains fichiers, qui devrons être accessibles uniquement par les utilisateurs autorisés pour garantir l'intégrité et la confidentialité des données.

Limiter l'accès aux fichiers critiques (passwd, shadow, sudoers...).

**Effectuer les commandes suivantes :**

sudo chmod 640 /etc/shadow

sudo chmod 644 /etc/passwd

sudo chmod 440 /etc/sudoers

sudo chown root:root /etc/{shadow,passwd,sudoers}

Pour les journaux :

sudo chmod -R go-rwx /var/log.

```
root@linuxmintgsb-virtual-machine:~# chmod 640 /etc/shadow
root@linuxmintgsb-virtual-machine:~# chmod 644 /etc/passwd
root@linuxmintgsb-virtual-machine:~# chmod 440 /etc/sudoers
root@linuxmintgsb-virtual-machine:~# chown root:root /etc/{shadow,passwd,sudoers}
root@linuxmintgsb-virtual-machine:~# sudo chmod -R go-rwx /var/log
root@linuxmintgsb-virtual-machine:~#
```

## IX. Installation de fail2ban (Gökhan)

Fail2ban est un outil de prévention des intrusions qui protège le système en détectant et en bloquant les adresses IP suspectes. Son installation renforce la sécurité du système contre les attaques par force brute.

Veuillez effectuer les commandes suivantes pour procéder à son installation :

Sudo apt update

sudo apt install fail2ban -y

sudo systemctl enable fail2ban

sudo systemctl start fail2ban

```
hiffrementlinuxmint@chiffrementlinuxmint-virtual-machine:~$ apt update
sudo] Mot de passe de chiffrementlinuxmint :
tteint :1 http://archive.ubuntu.com/ubuntu jammy InRelease
tteint :2 http://security.ubuntu.com/ubuntu jammy-security InRelease
tteint :3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease
tteint :4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease
gn :5 http://packages.linuxmint.com virginia InRelease
tteint :6 http://packages.linuxmint.com virginia Release
ecture des listes de paquets... Fait
onstruction de l'arbre des dépendances... Fait
ecture des informations d'état... Fait
59 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.
hiffrementlinuxmint@chiffrementlinuxmint-virtual-machine:~$ apt install fail2ban -y
```

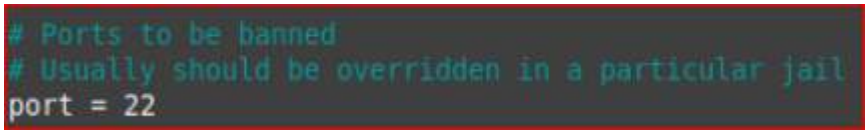
```
root@chiffrementlinuxmint-virtual-machine: ~
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
oot@chiffrementlinuxmint-virtual-machine:~# systemctl enable fail2ban
ynchronizing state of fail2ban.service with SysV service script with /lib/systemd/systemd-sysv-in
tall.
xecuting: /lib/systemd/systemd-sysv-install enable fail2ban
oot@chiffrementlinuxmint-virtual-machine:~# systemctl start fail2ban
oot@chiffrementlinuxmint-virtual-machine:~#
```

Une fois effectué, entrez cette commande pour rentrer dans les fichiers de configuration ; sudo nano /etc/fail2ban/jail.local

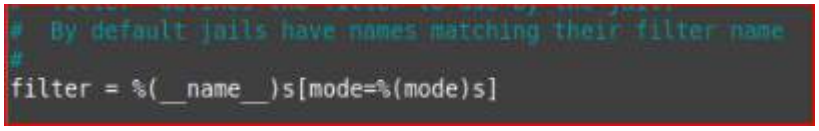
```
# [sshd]
enabled = true
```

modifier la ligne « enabled » et décocher ou modifier la ligne pour activer « enabled=true » ATTENTION, veillez à bien modifier la bonne ligne car il y a plusieurs ligne « enabled= » il doit y avoir pour celle-ci [sshd]comme ci-dessus.

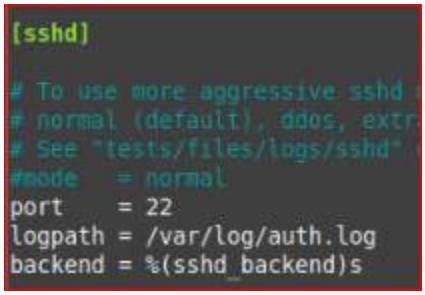
Ensuite modifier la ligne «port» , ajouter « 22 » après le « = ».



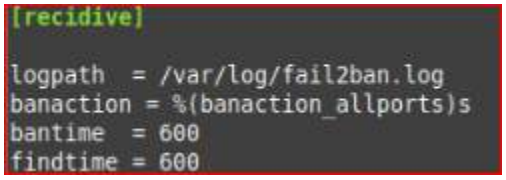

Poursuivons avec la ligne « filter » remplacez le texte dedans par « sshd ».




Même chose, ici nous modifions la ligne logpath = /var/log/auth.log

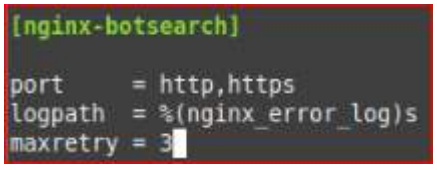



Pour la suite, cherchez la ligne suivante :

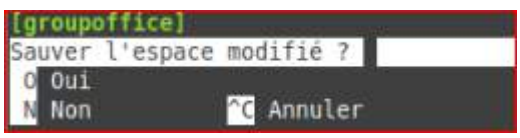



Remplacer le « bantime » et le « findtime » par 600 chacun.

Et enfin : la ligne « maxretry = 3 ».




Quitter le fichier config avec la touche CTRL du clavier et X, puis appuyer sur O, ou Y et appuyer sur la touche entrer.




Ou bien, pour faire plus simple, vous pouvez tout simplement inscrire cette ligne ci-dessous, en dessous de « [sshd] » :

```
[sshd]
enabled = true
port = 22
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 600
findtime = 600
```

enabled = true

port = 22

filter = sshd

logpath = /var/log/auth.log

maxretry = 3

bantime = 600

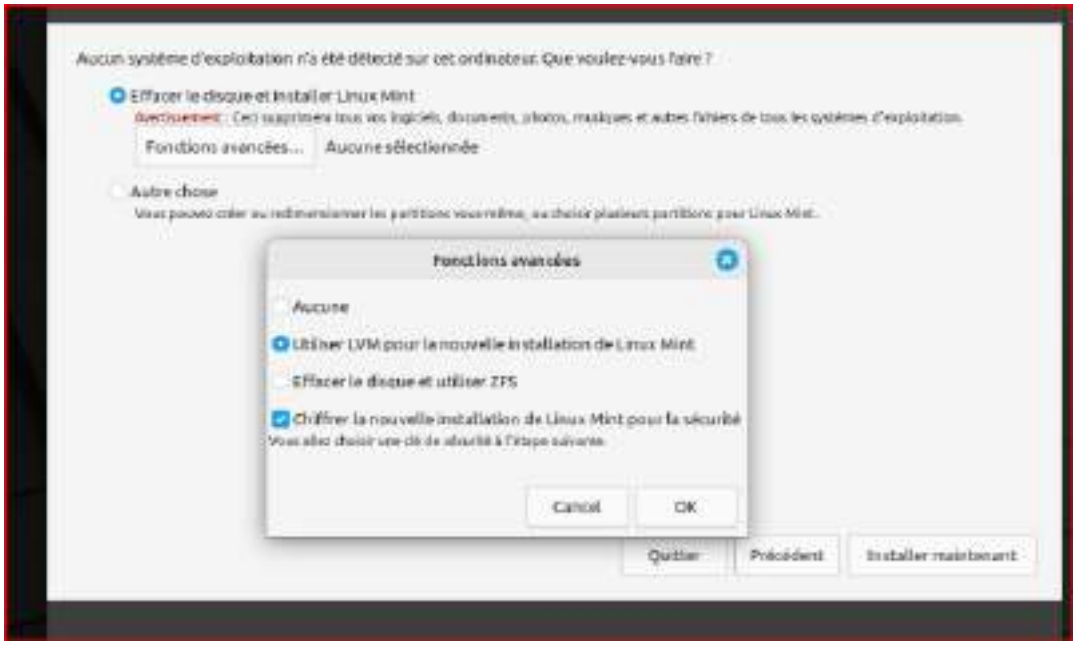
findtime = 600

```
    C:\Users\Gokha/.ssh/known_hosts:3: 10.0.0.7
Are you sure you want to continue connecting (yes/no/[fingerprin
Warning: Permanently added '192.168.133.128' (ED25519) to the li
test@192.168.133.128's password:
Permission denied, please try again.
test@192.168.133.128's password:
Permission denied, please try again.
test@192.168.133.128's password:
test@192.168.133.128: Permission denied (publickey,password).

C:\Users\Gokha>
```

## X. Chiffrement (Gökhan)

**Sélectionner Français en langue clavier**

pour le stockage sélectionner fonctions avancées→cocher « utiliser LVM pour la nouvelle installation de linux mint » et « Chiffrer la nouvelle installation de linux mint pour la sécurité » Il faudra par ailleurs entrer un mot de passe pour la clé de sécurité, qui vous sera demandé à chaque démarrage.




Pour la clé de sécurité, j'ai mis : **Sasori-67**

Activer la clé de récupération, cela génèrera automatiquement une clé de récupération stocké dans l'emplacement suivant : **/home/mint/recovery.key**