AP1

LIVRABLE 3

GROUPE N°3

DOCUMENTATION DU PROJET

Durée du projet : 27.10.24 / 21.01.25

Fourniture d'une solution informatique nomade sécurisée

Date limite de remise : 21 /01/2025

SYNAPSE IT

Chef de Projet :

ALBISSER Samy – Chef de projet IT (Linux)

Membre :

ABGARYAN Arman – Administrateur Système (Windows)

SOMMAIRE

Table des matières

SOMMAIRE

SOMMAIRE

SOMMAIRE

SOMMAIRE

SOMMAIRE

SOMMAIRE

SOMMAIRE

SOMMAIRE

SOMMAIRE

SOMMAIRE

SOMMAIRE

SOMMAIRE

SOMMAIRE

SOMMAIRE

SOMMAIRE

1. Documentation d'installation Windows

0. Création d'une machine virtuelle (VM) dans VMware

1. Introduction :

- Voici un guide détaillé pour créer une machine virtuelle (VM) dans **VMware Workstation** ou **VMware Player**.

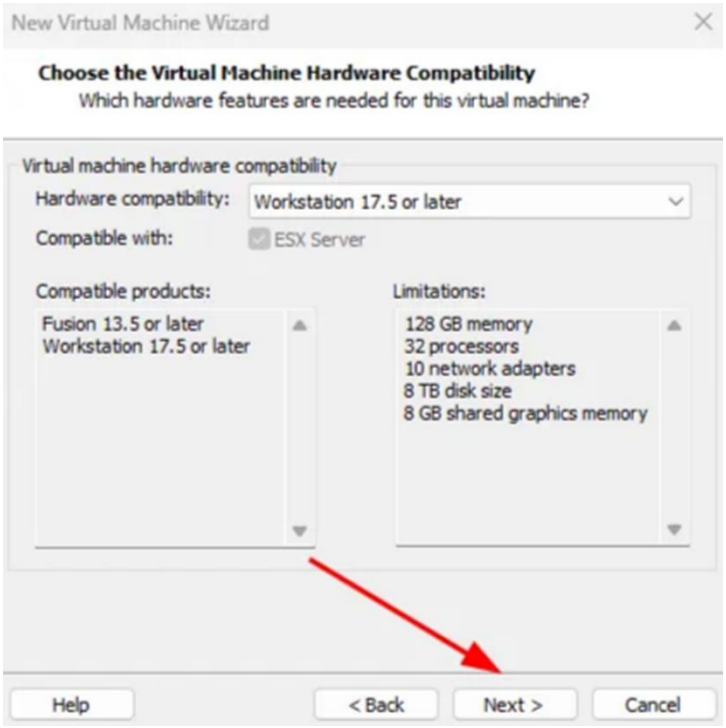
2. Ouvrir VMware Workstation/Player

- Lancez VMware Workstation ou VMware Player sur votre poste.
- Sur l'écran principal, cliquez sur **Create a New Virtual Machine** (Créer une nouvelle machine virtuelle).

3. Sélection du type de configuration

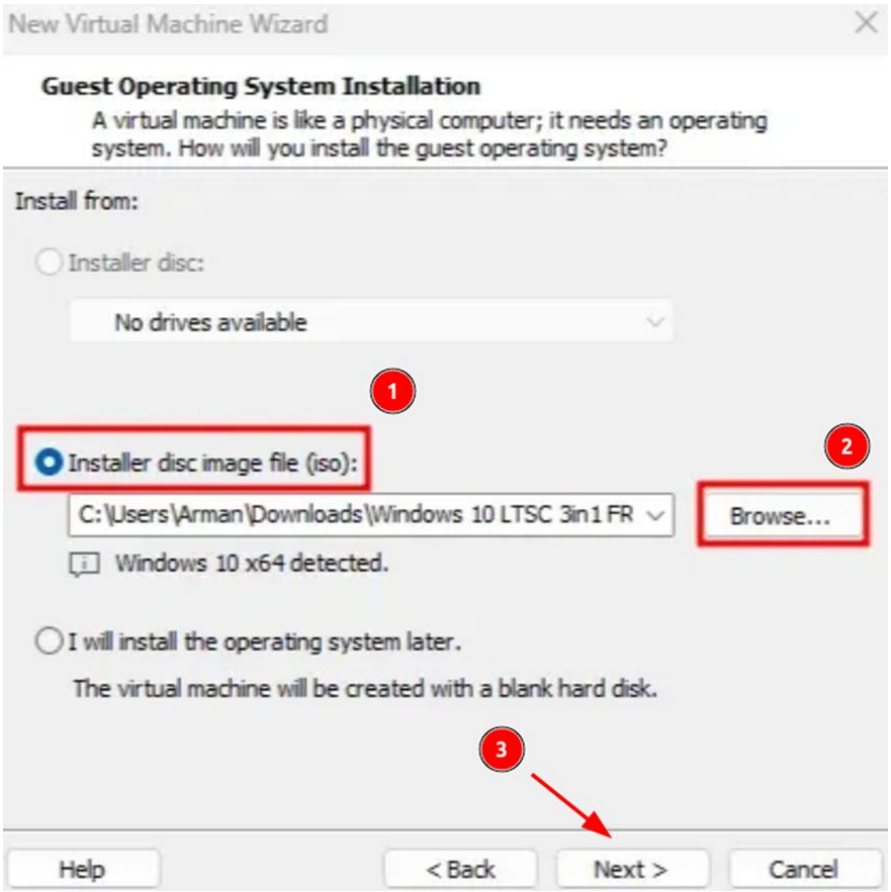
- Une fenêtre s'ouvre vous demandant de choisir entre deux choix, sélectionnez **Custom** puis cliquez sur **Next**.

- Cliquez à nouveau sur **Next**.



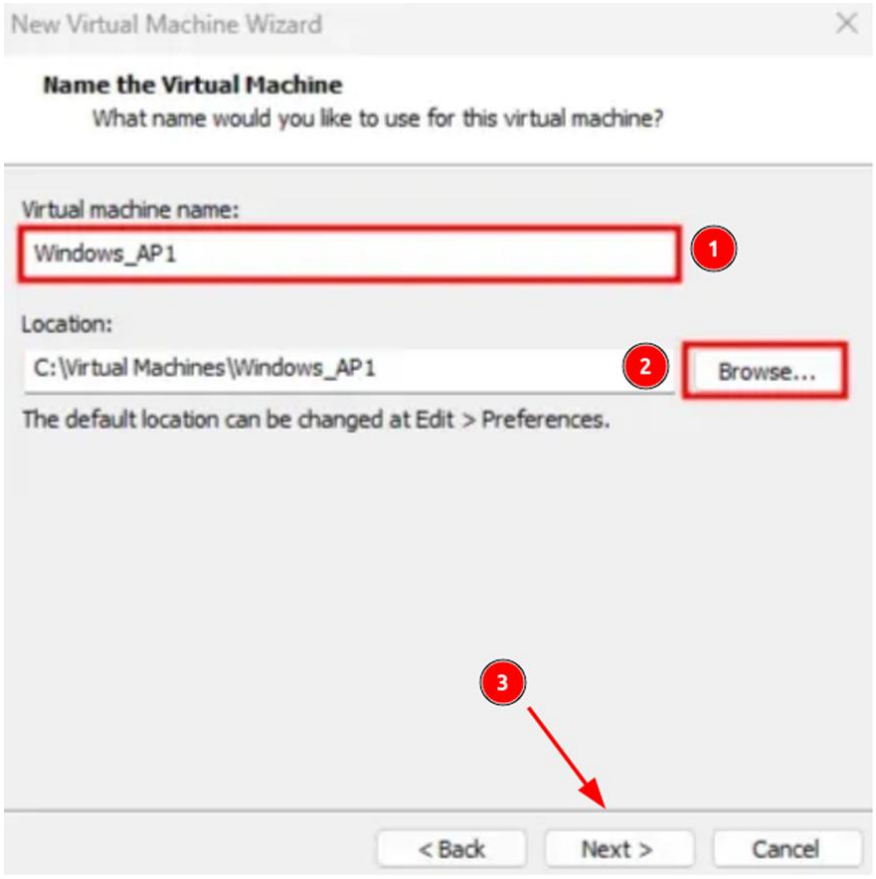
4. Choisir la source du système d'exploitation

- Vous aurez plusieurs choix qui apparaissent :
    - Sélectionnez **Installer disc image file (iso)** *(1)* et mettez votre image iso avec **Browse…** *(2)* (Pour trouver l'image de Windows rendez-vous sur le site officiel ou sur un autre site). Puis faites **Next** *(3)*.



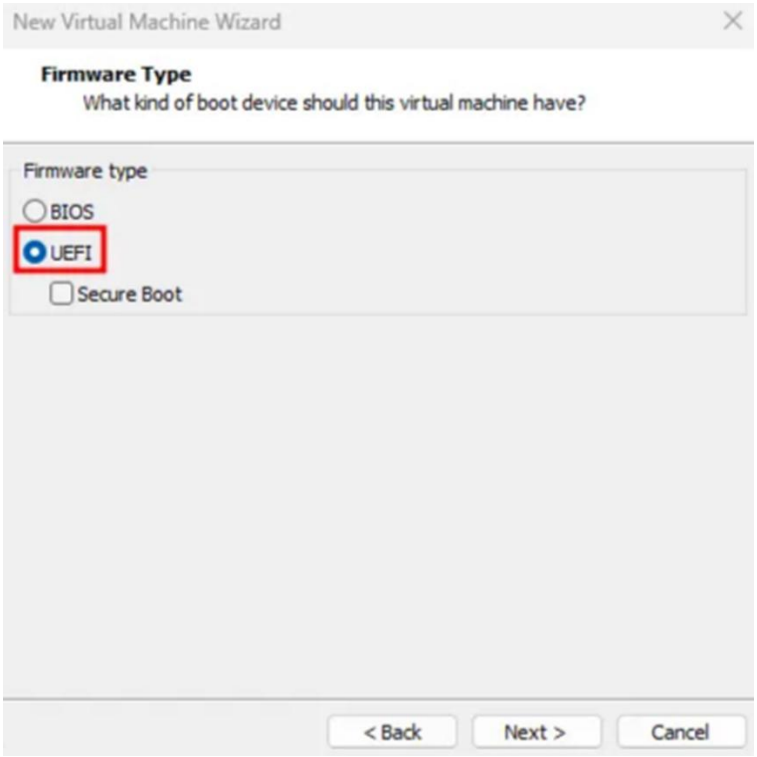
5. Nommer la VM et choisir l'emplacement

- Virtual machine name :
  - Donnez un nom significatif à votre VM, par exemple : **Windows_AP1** *(1)*.
  - Cliquez sur **Browse** *(2)* pour choisir où les fichiers de la VM seront enregistrés et **Next** *(3)*.



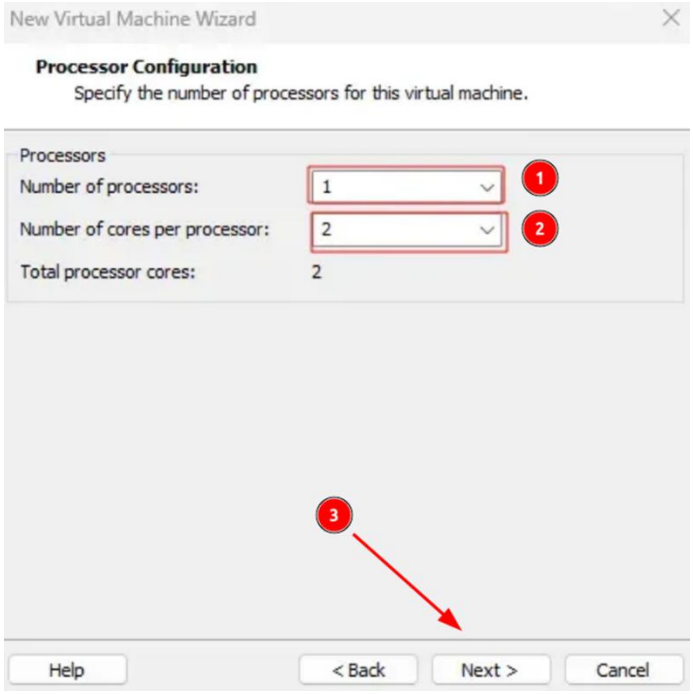
6. Configurez le Firmware Type

- Pour **Windows** nous vous conseillons de sélectionner **UEFI**.



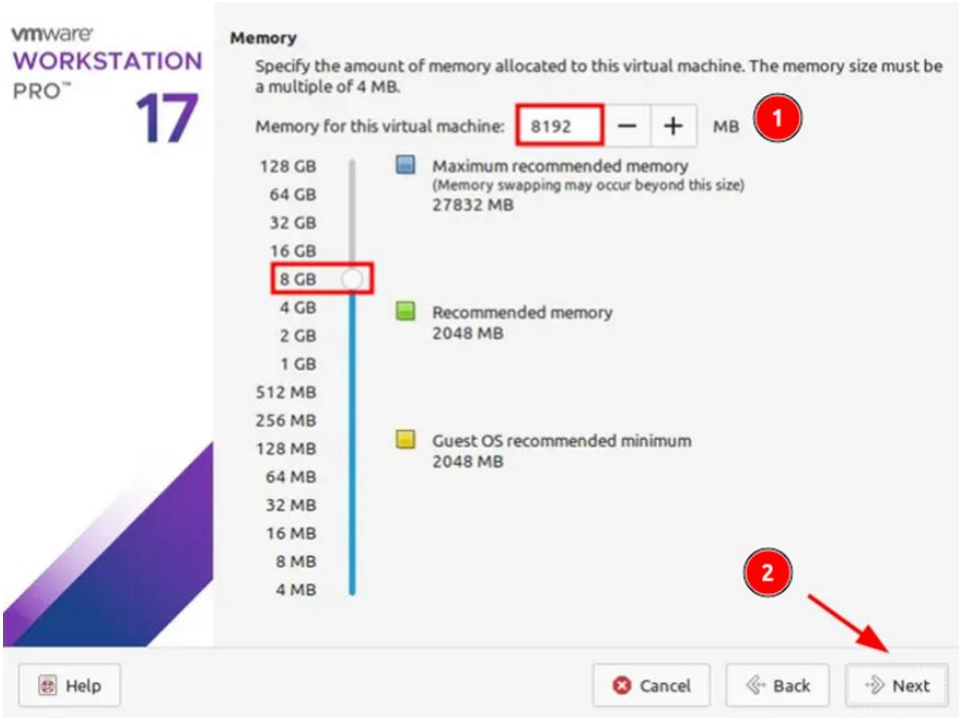
7. Configurer le processeur

- Pour **Number of processors** et **Number of cores per processor:**
  - Sélectionnez le nombre de **processeurs** utilisés pour la machine (par exemple : 1) *(1)*.
  - Sélectionnez le nombre de **cœurs par processeur** (par exemple : 2) *(2)*.
  - Puis faites **OK** *(3)*.



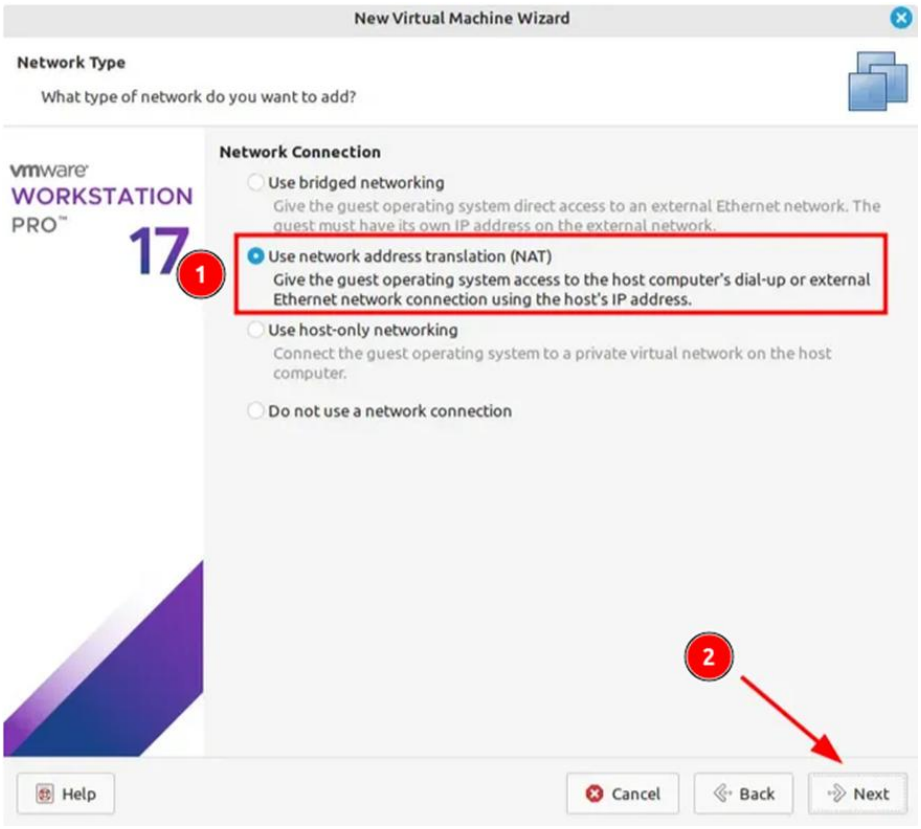
8. Configurer la mémoire

- Réglez la mémoire souhaitée pour le système en utilisant le curseur ou le champ numérique sous **Memory for this virtual machine** (par exemple, **8192 MB** *(1)* pour **8 Go**). Cliquez sur **Next** *(2)*.



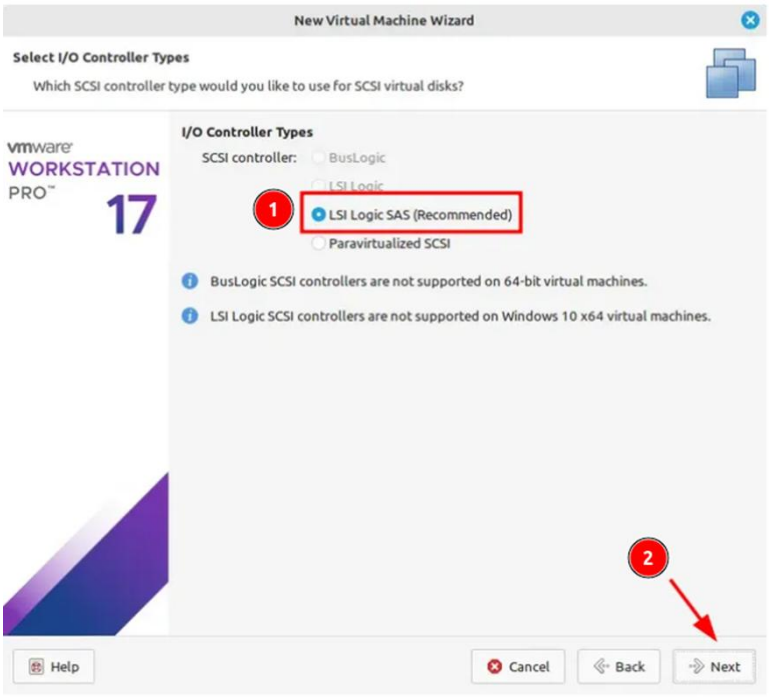
9. Configuration du réseau

- Il y a quatres options qui apparaissent, choisissez :
  - **Use network address translation (NAT)** *(1)* : pour accéder à Internet via l'hôte.
  - Cliquez sur **Next** *(2)*.



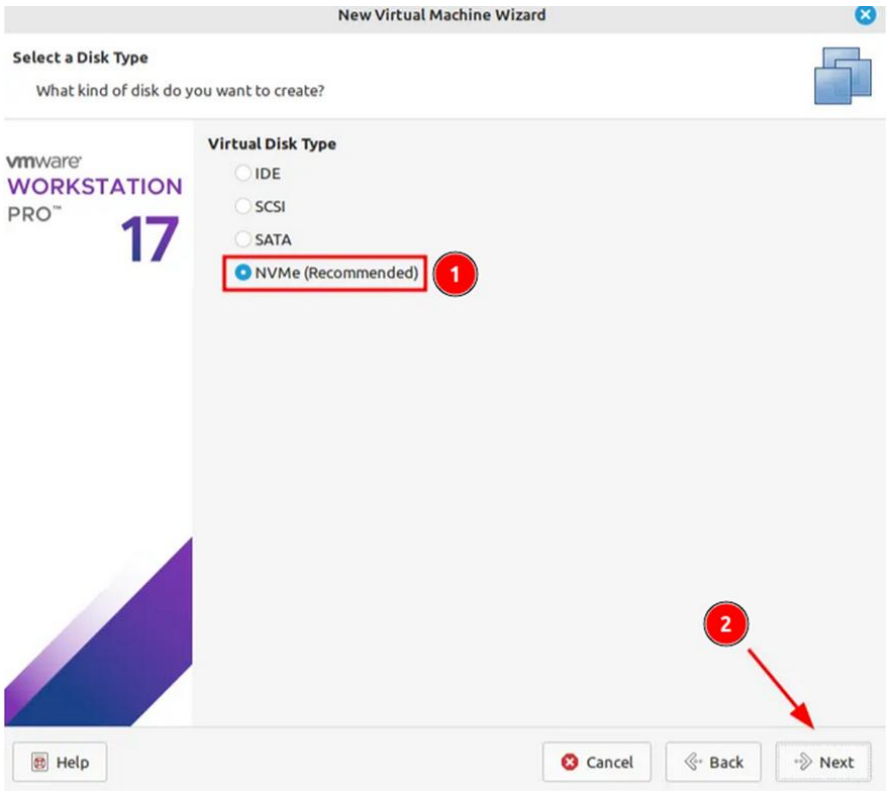
10. Configuration du contrôleur d'E/S

- Trois options apparaissent pour le contrôleur SCSI :
  - Choisissez **LSI Logic (Recommended)** *(1)*.
  - Cliquez sur **Next** *(2)*.

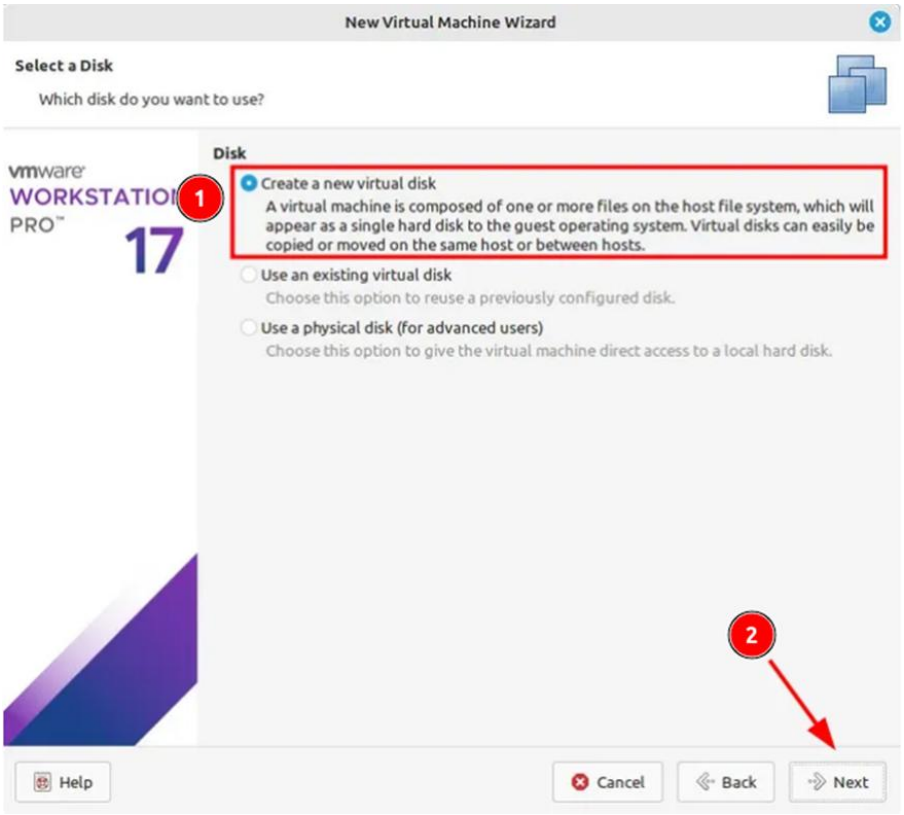


11.Configurer le disque dur

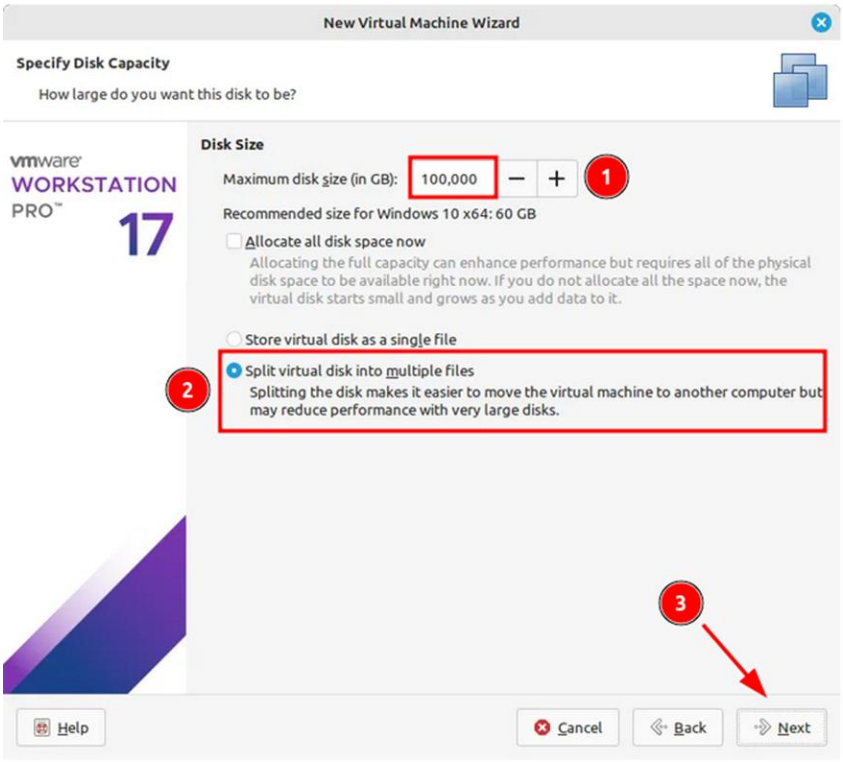
- **Virtual disk type :** Sélectionnez **NVMe (Recommended)** *(1)*, puis cliquez sur **Next** *(2)*.



- Choisissez le **Disque :**
  - Sélectionnez **Create a new virtual disk** *(1)*, puis cliquez sur **Next** *(2)*.

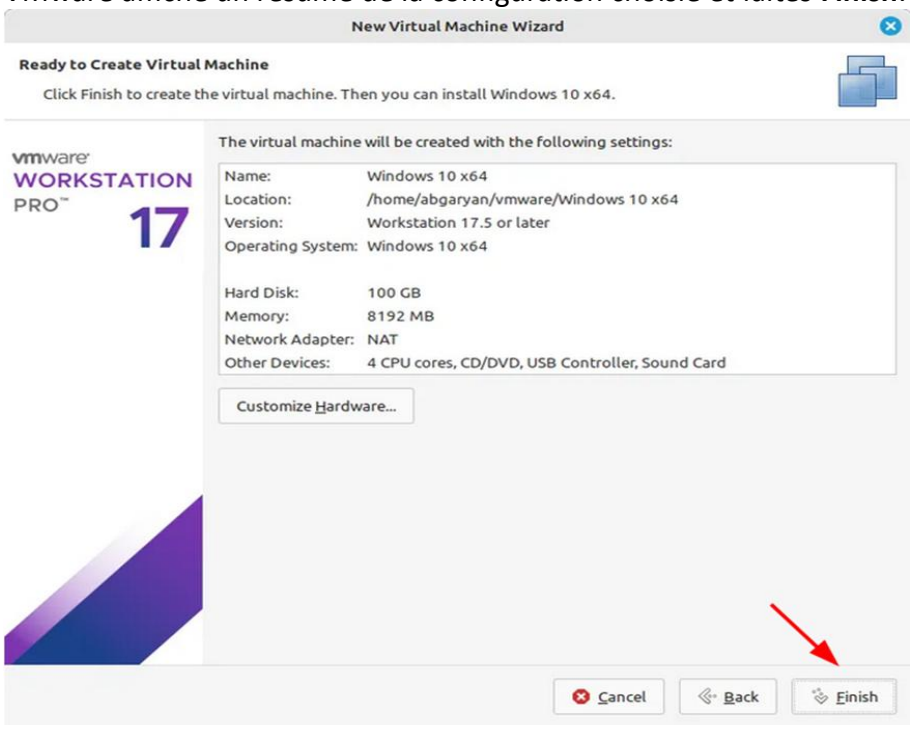


- **Taille du Disque :** Entrez **100 GB** (ou 60 GB) *(1)* et choisissez :
  - **Split virtual disk into multiple files** : divise le disque virtuel en plusieurs fichiers (meilleur pour la portabilité) *(2)* puis cliquez sur **Next** *(3)*.



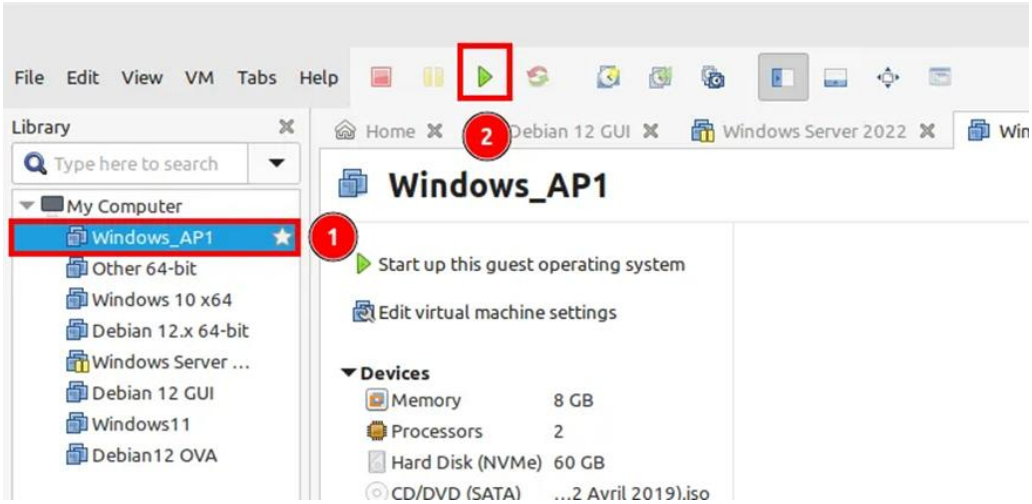
12. Vérification et personnalisation

- VMware affiche un résumé de la configuration choisie et faites **Finish**.



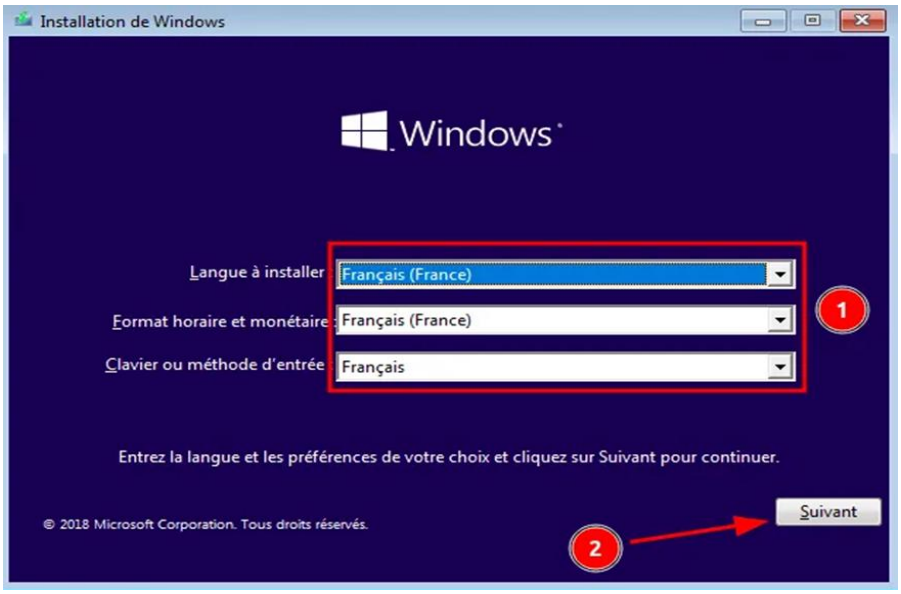
13. Lancement de la VM et installation de Windows

- Dans VMware, sélectionnez la VM que vous venez de créer *(1)* et cliquez sur **Power On** *(2)* pour démarrer la machine virtuelle.

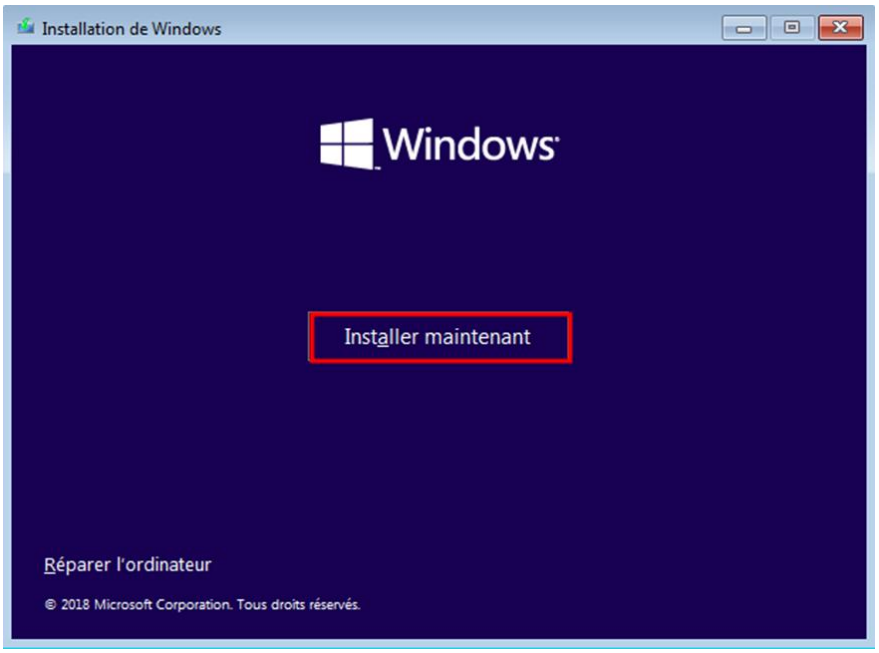


- Dès que ce message apparaît, appuyez sur n'importe quelle **touche** de votre clavier (Le faire rapidement sinon vous rencontrerez une erreur).

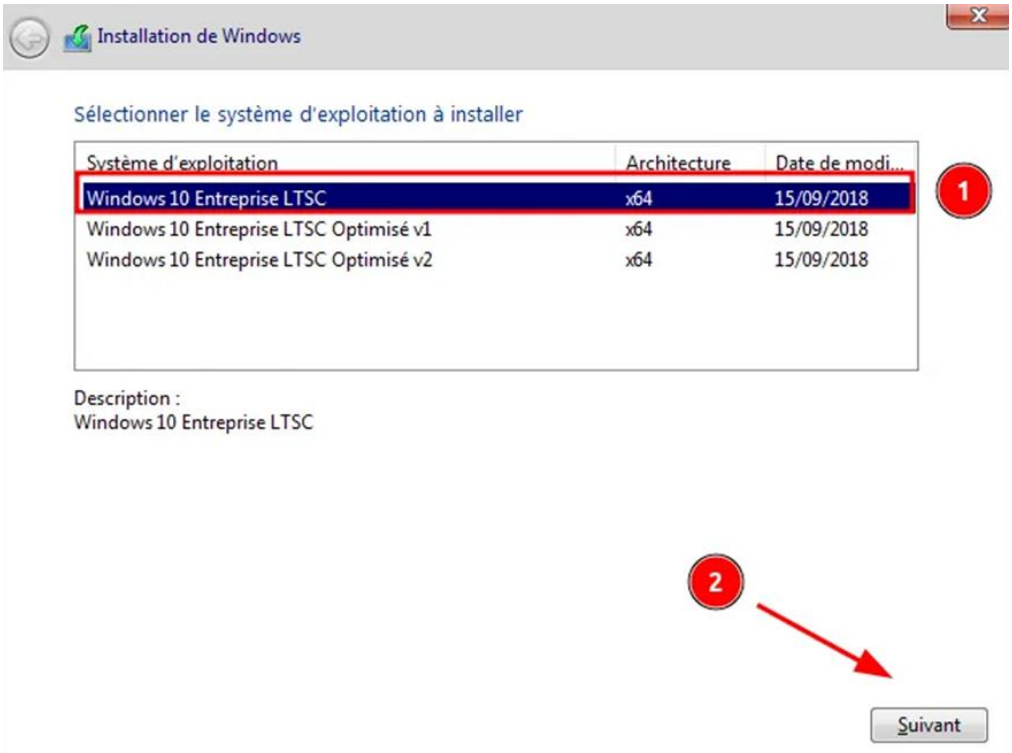
- Vous vous retrouverez ensuite sur **l'Installation de Windows**, choisir toutes les options en **Français** *(1)* et cliquez sur **Suivant** *(2)*.



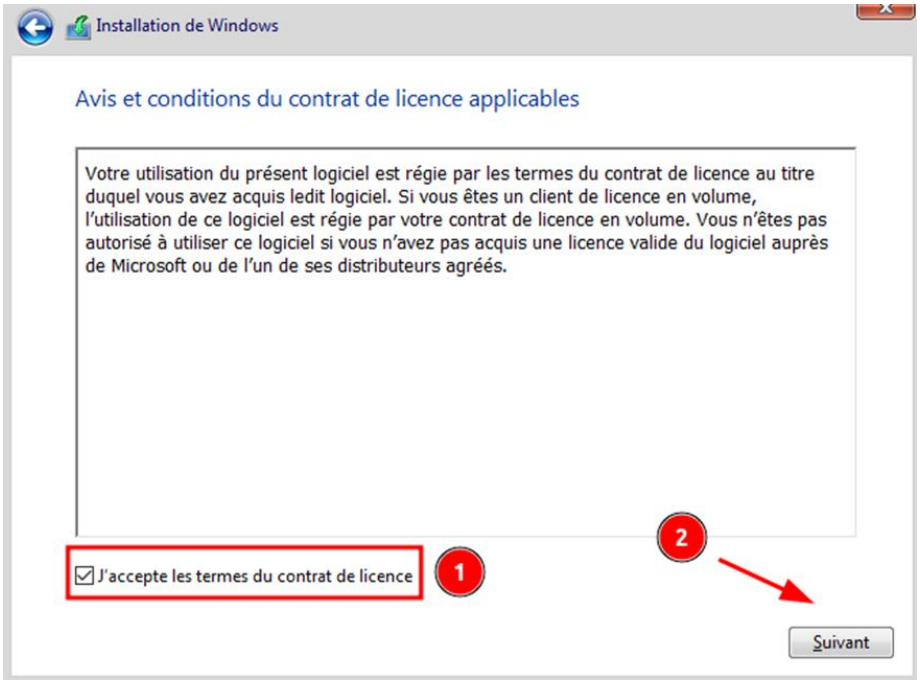
- Cliquez sur **Installer maintenant**.



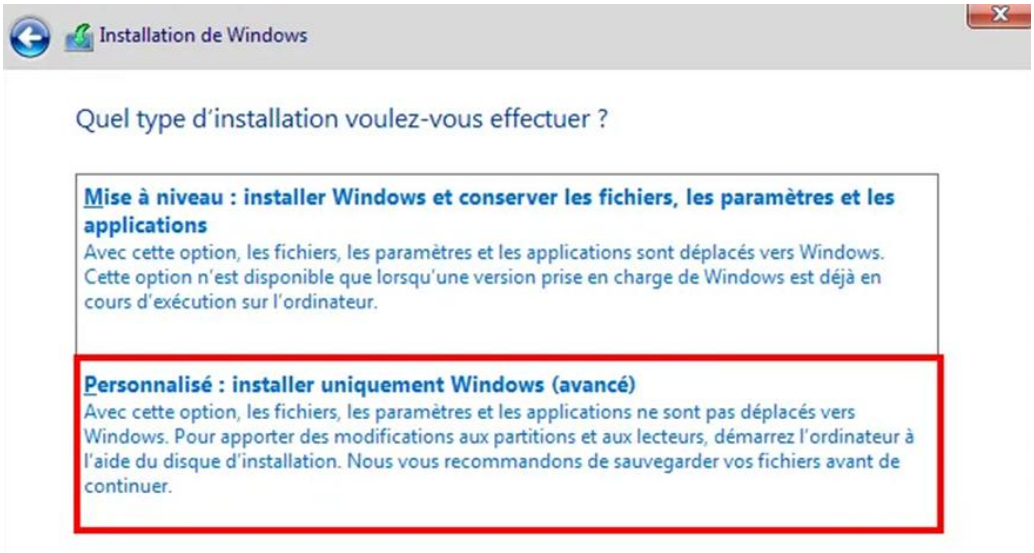
- Après l'installation, choisissez **Windows 10 Entreprise LTSC** *(1)* puis cliquez sur **Suivant** *(2)*.



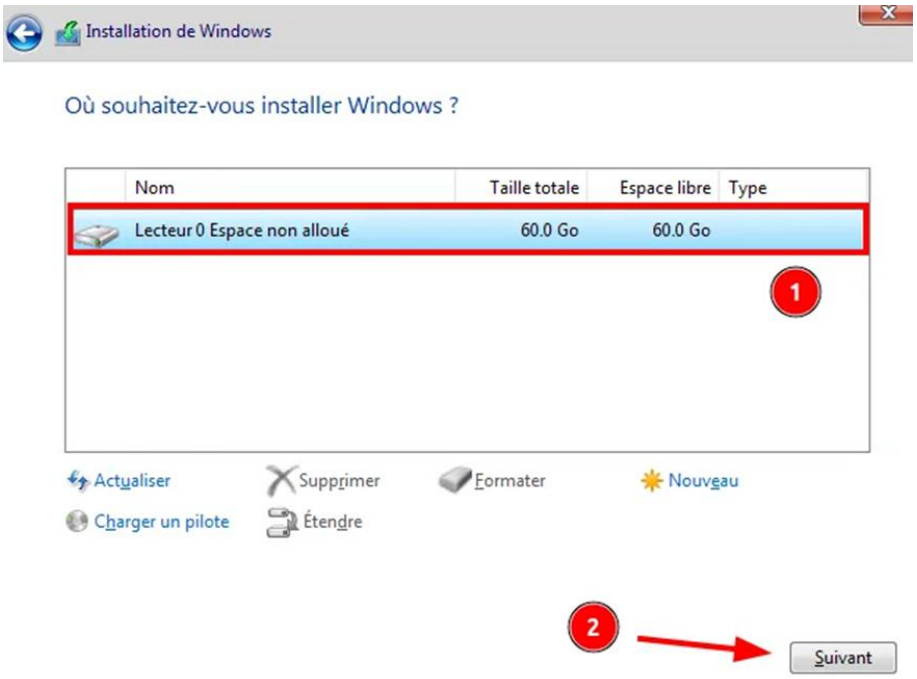
- Acceptez la case **J'accepte les termes du contrat de licence** *(1)* et faites **Suivant** *(2)*.



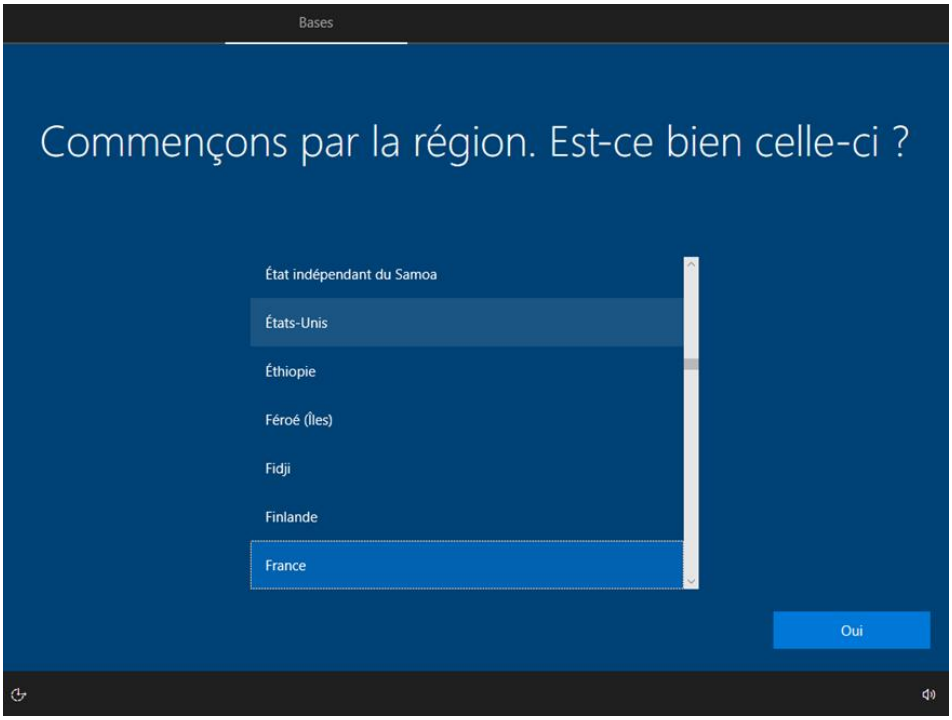
- Choisissez **Personnalisé : installer uniquement Windows (avancé)**.



- Sélectionnez votre **Lecteur** *(1)* et faites **Suivant** *(2)*.

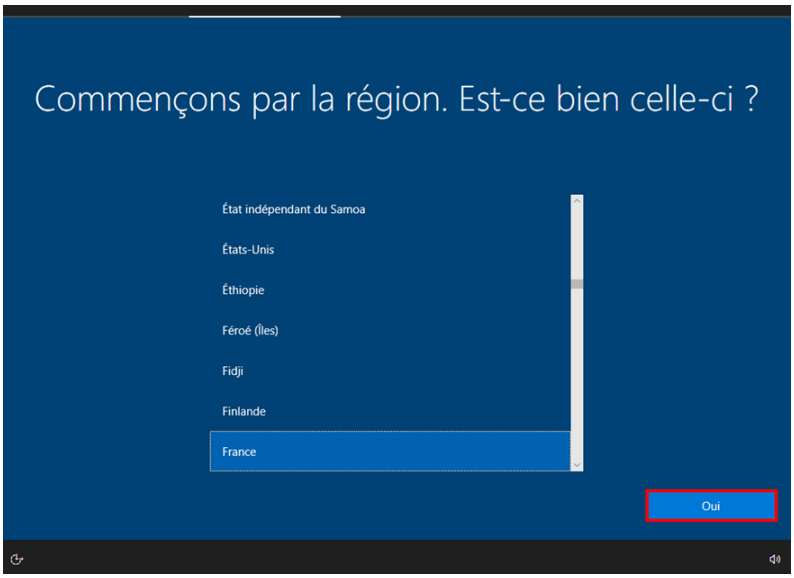


- Après l'installation sur le disque, vous tomberez sur ce choix (Ne cliquez surtout sur rien).

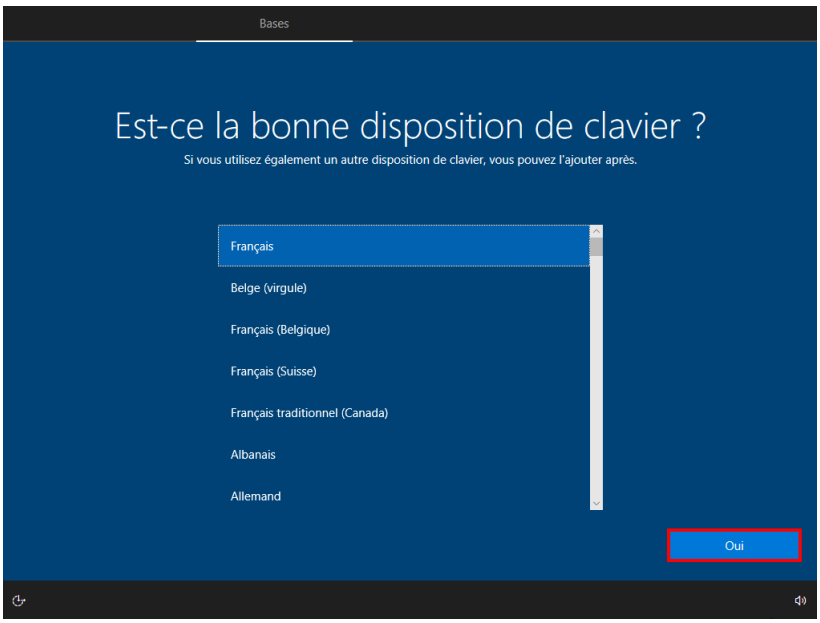


- Nous allons désactiver la connexion internet, pour cela, dans **VMware** en bas à droite vous avez une icône qui s'appelle **Network Adapter : NAT,** faites un clic-droit puis cliquez sur **Disconnect**.

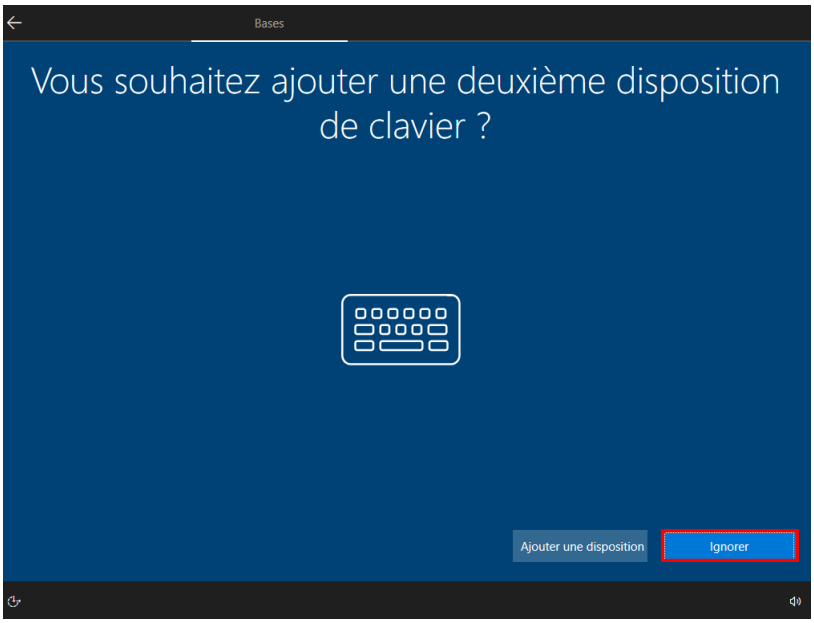
- Ensuite choisissez pour la région **Français** puis faites **Oui**.



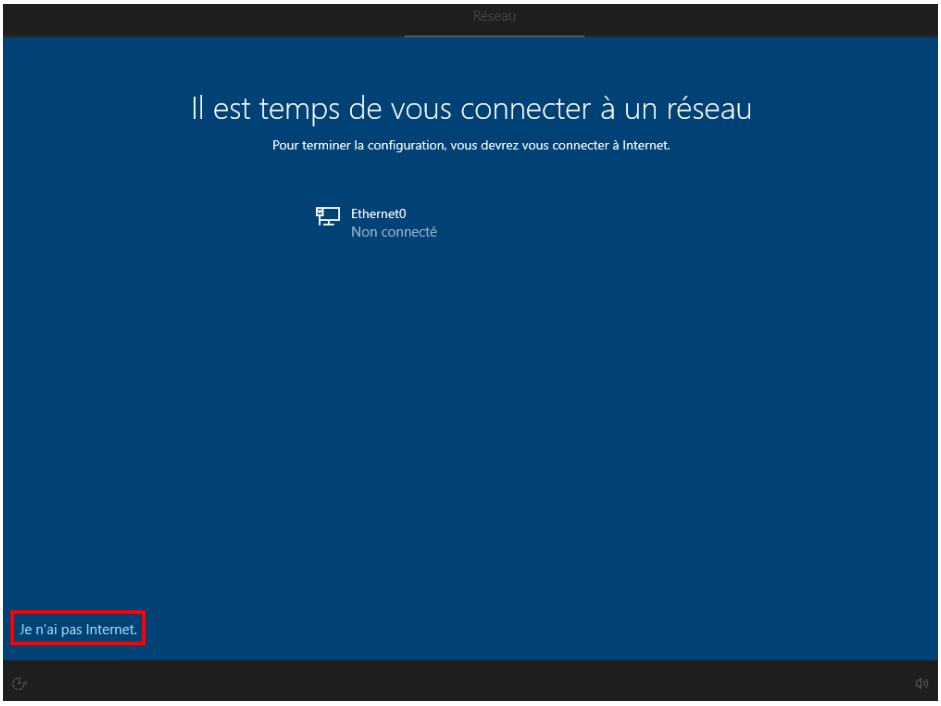
- Pour la disposition de clavier, choisissez **Français** puis faites **Oui**.



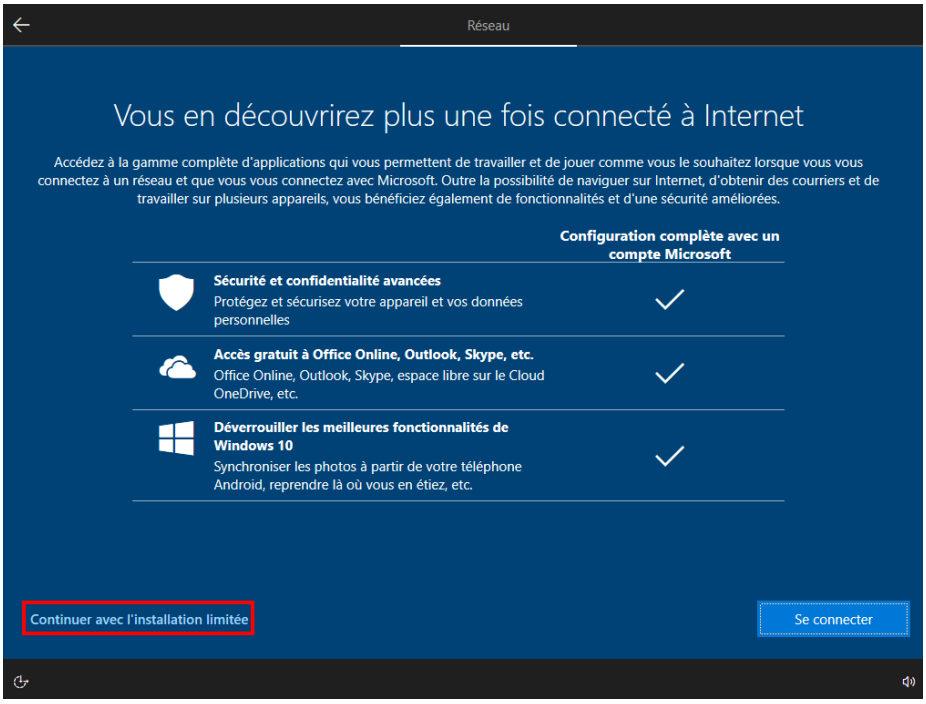
- Pour la disposition de clavier, faites **Ignorer**.



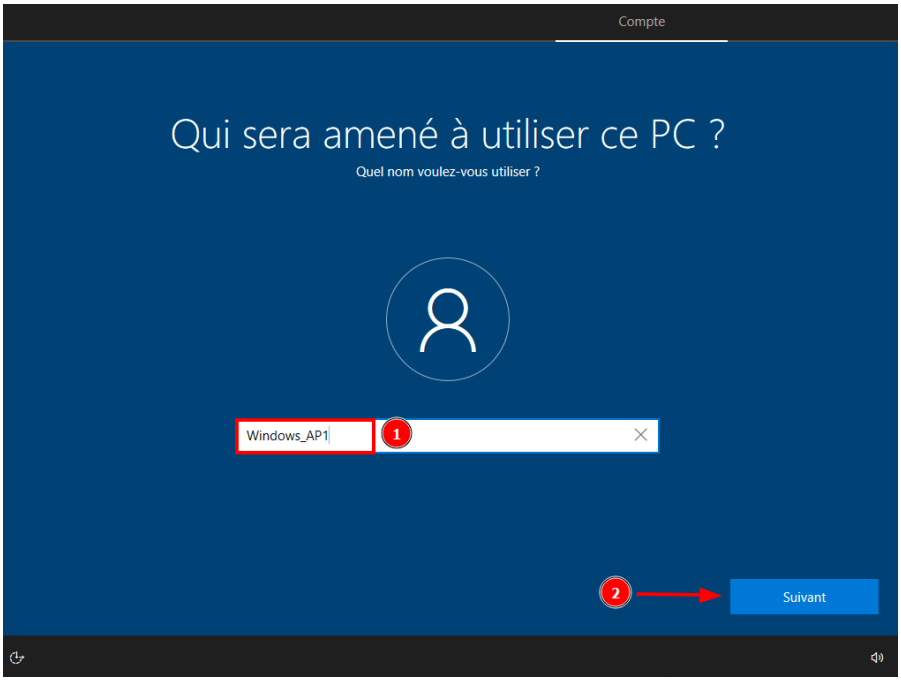
- Sélectionnez **Je n'ai pas Internet**.



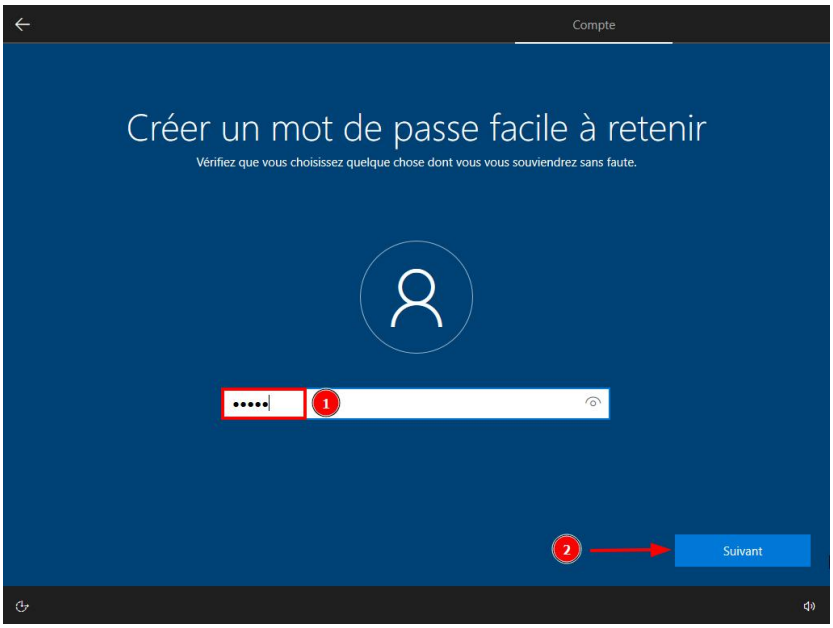
- Puis faites **Continuer avec l'installation limitée**.



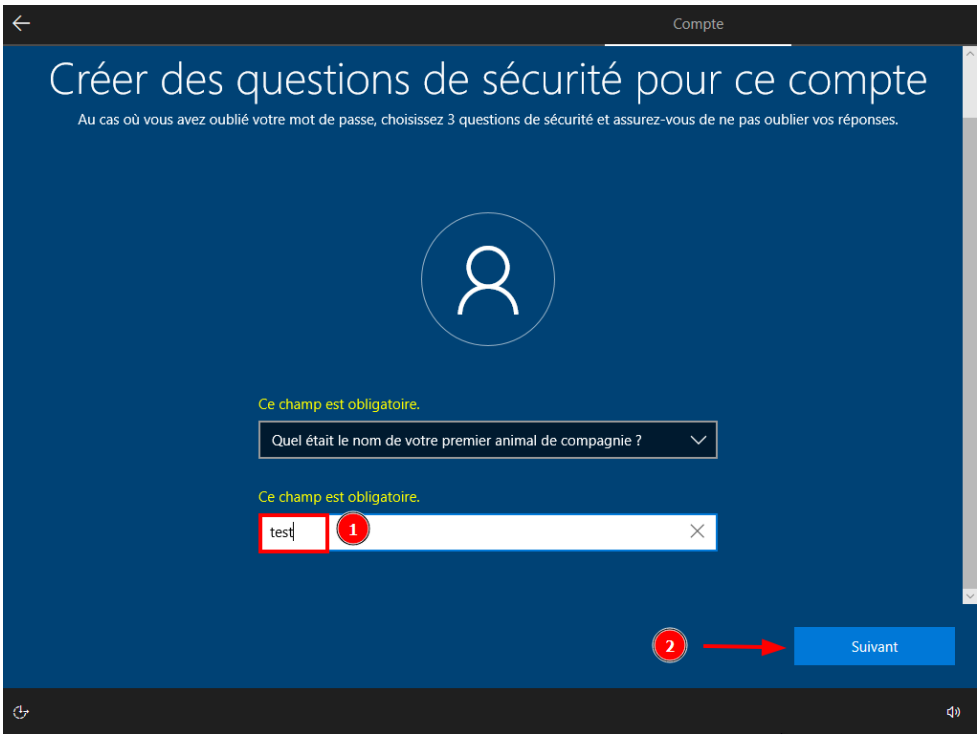
- Choisissez n'importe quel un nom pour le PC (Sachez que ce compte aura l'accès **Administrateur**) *(1)* et faites **Suivant** *(2)*.



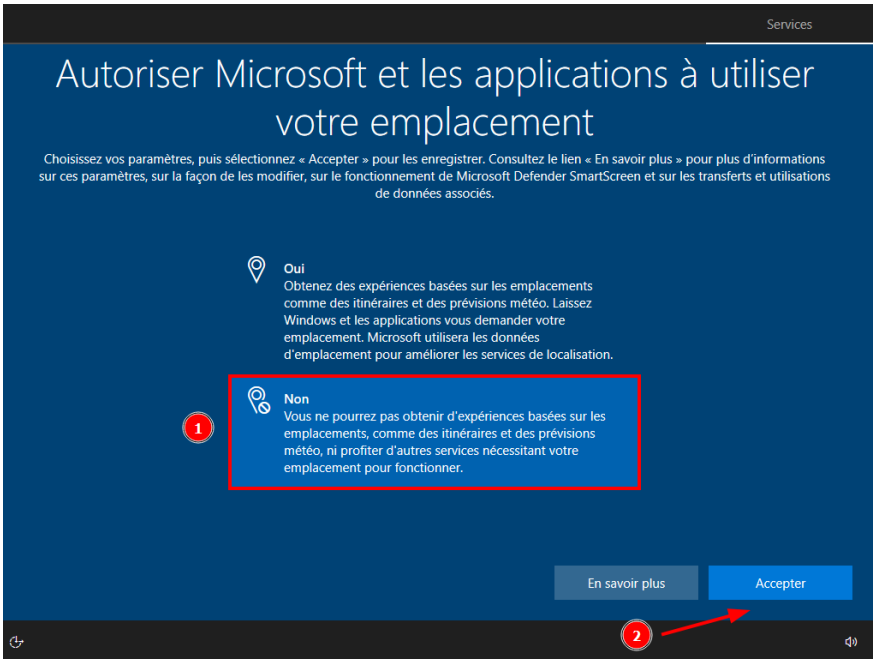
- Pour l'instant vous pouvez choisir un **Mot De Passe** facile à retenir *(1)* et faites **Suivant** *(2)* et confirmez le à nouveau.



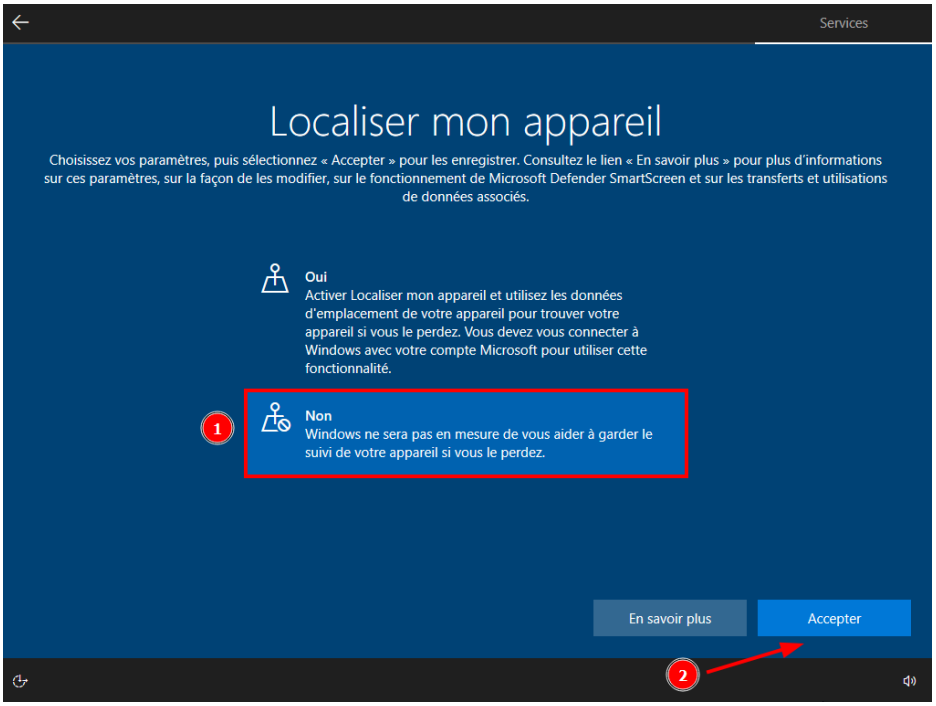
- Pour les questions de sécurité choisissez 3 différentes questions et mettez n'importe quelle information dans le **champ** *(1)* puis faites **Suivant** *(2)*.



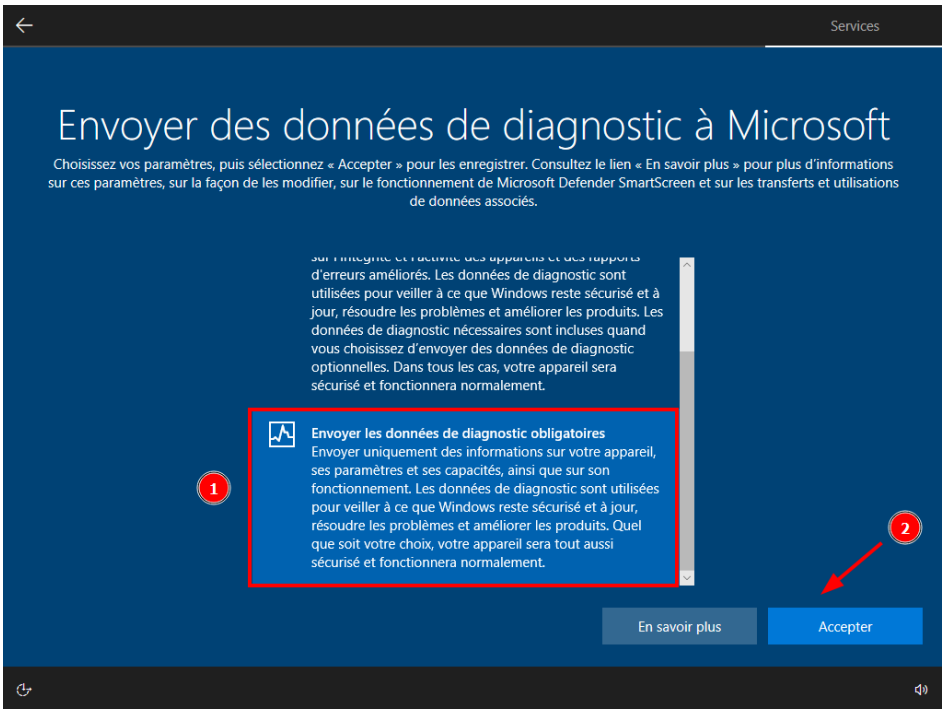
- Mettez **Non** *(1)* à l'option pour que Microsoft et les applications n'utilisent pas votre emplacement et faites **Accepter** *(2)*.



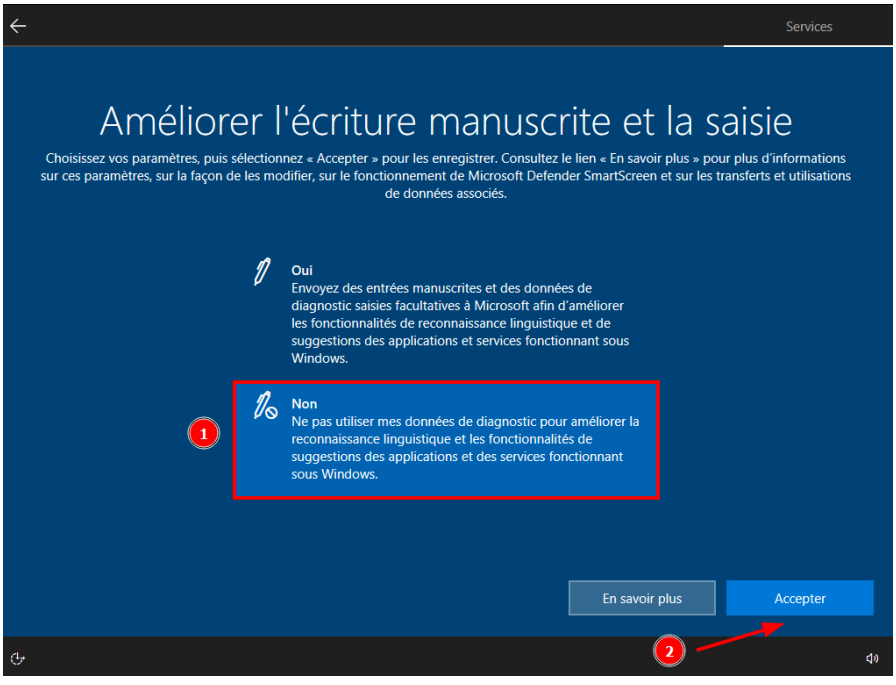
- Mettez **Non** *(1)* pour ne pas **localiser mon appareil** et faites **Accepter** *(2)*.



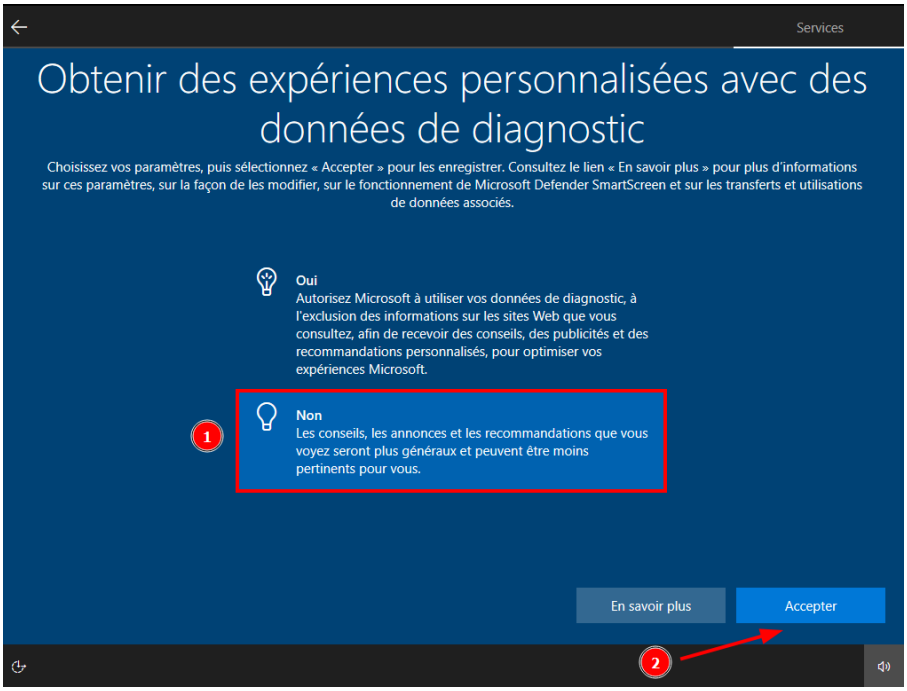
- Choisissez la **deuxième option** *(1)* pour n'envoyer que les diagnostics obligatoires à Microsoft et faites **Accepter** *(2)*.



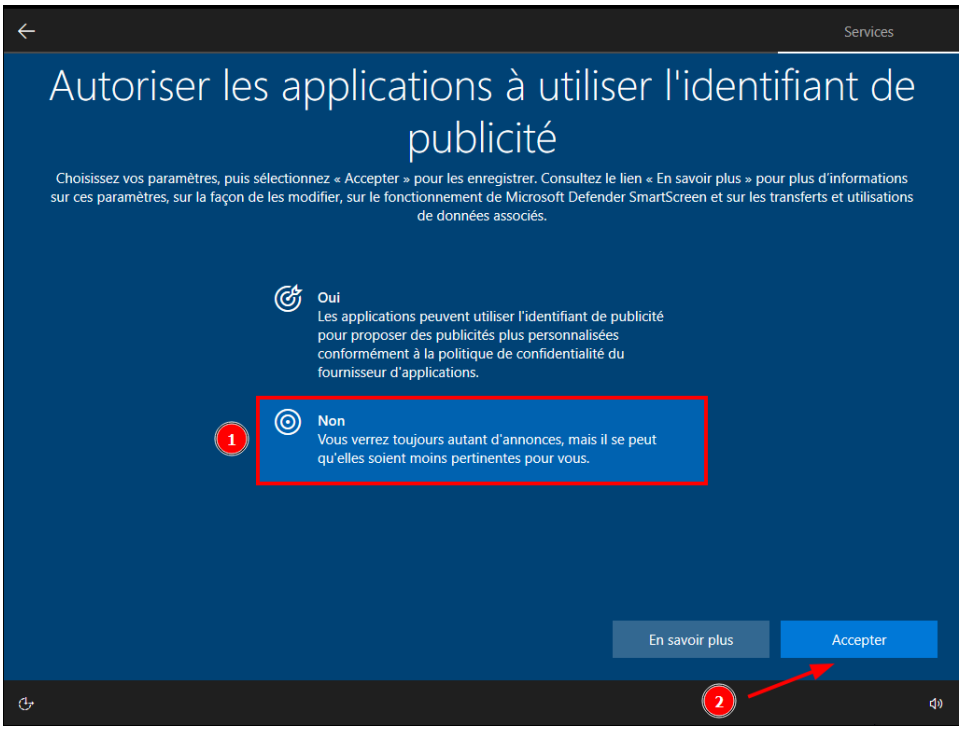
- Mettez **Non** *(1)* pour l'écriture manuscrite et la saisie et faites **Accepter** *(2)*.



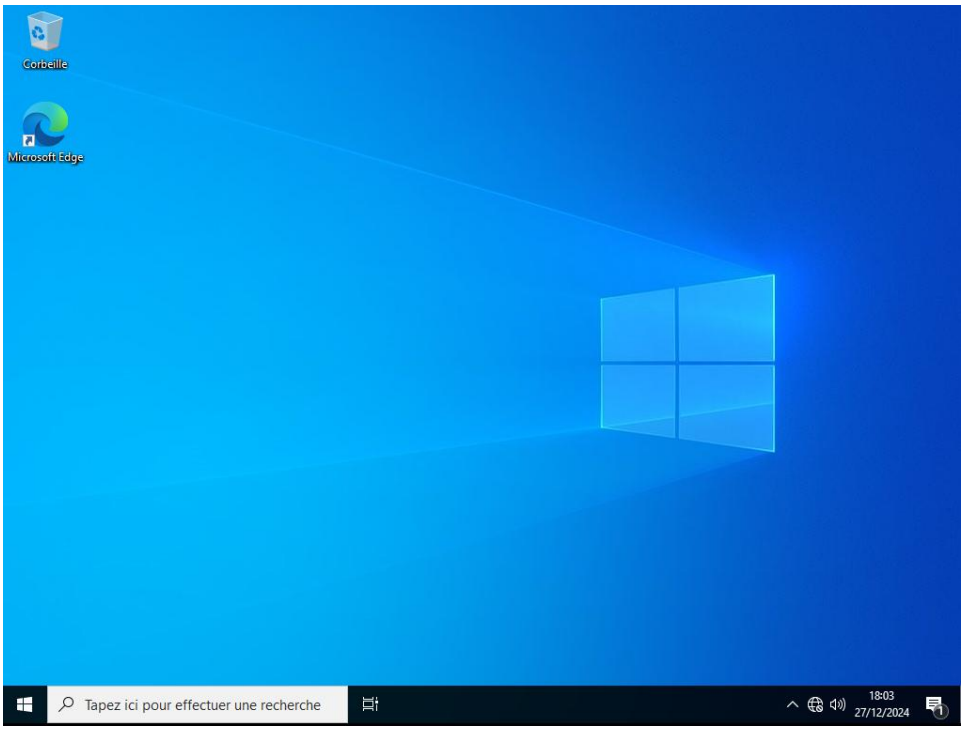
- Mettez **Non** *(1)* pour l'expériences personnalisées et faites **Accepter** *(2)*.



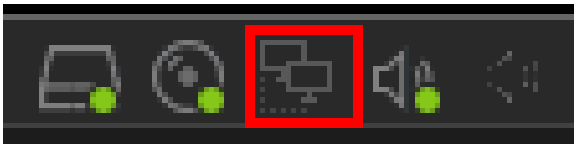
- Mettez **Non** *(1)* pour que les applications n'utilisent pas l'identifiant de publicité et faites **Accepter** *(2)*.



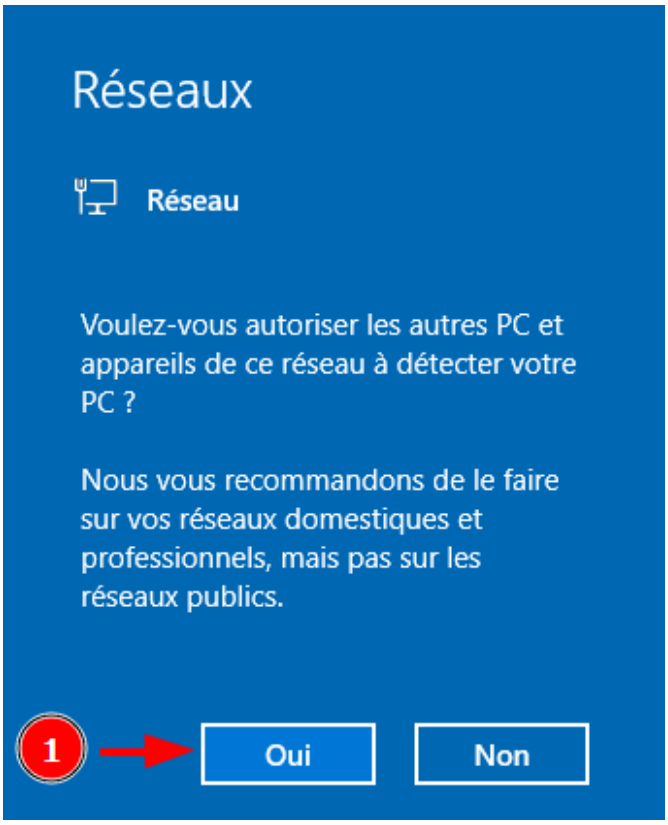
- Après cela, vous devrez attendre **quelques instants** pour que l'installation se termine, et vous devrez avoir l'interface **Windows** apparaître.

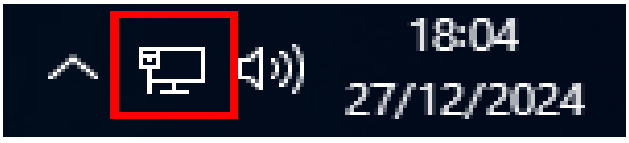


- Maintenant, nous devons réactiver la connexion, pour cela retournez au même endroit et faites un **clique-droit** puis **Connect**.



- Cette fiche devrait apparaître, cliquez sur **Oui** *(1)* et vous devriez voir en bas à droite de **Windows** la connexion filaire **rétablie**.





- Dernière étape, il nous faut faire une **Snapshot** pour en garder une nouvelle, pour cela **en haut à gauche** de **VMware** cliquez sur → **VM** → **Snapshot** → **Take Snapshot** , mettez y un **Nom** et cliquez sur **Take Snapshot**. Il faudra patienter **un moment** pour que la **Snapshot** s'effectue.

Bienvenue sur **Windows 10 Entreprise**.

DOCUMENTATION D'INSTALLATION

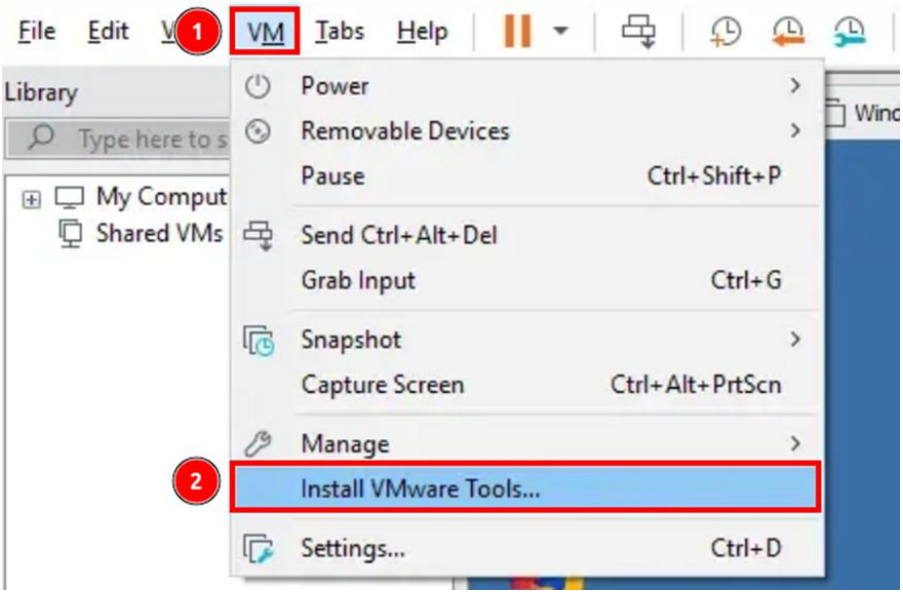
1. Installation du VMware tools

1. Introduction

- Dans cette étape, nous allons installer le **VMware tools** afin de pouvoir avoir des fonctionnalités en plus (comme d'avoir le plein écran).

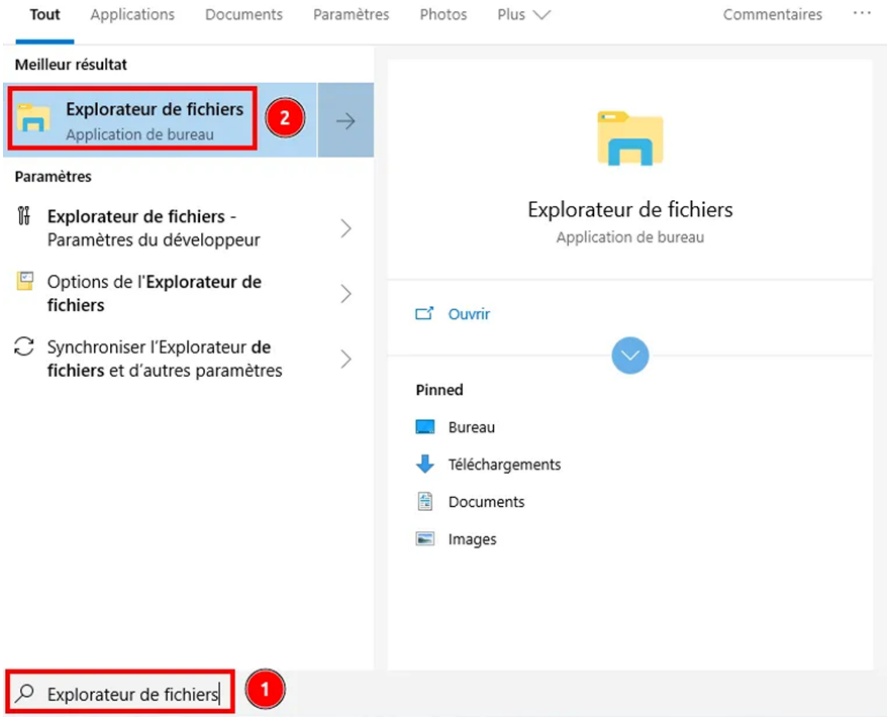
2. VMware tools

- Ouvrez votre VMware et allez sur votre VM Windows crée dans l'étape dernière :
    - Allez en haut à gauche et cliquez sur **VM** *(1)* et I**nstall VMware Tools…** *(2)*.

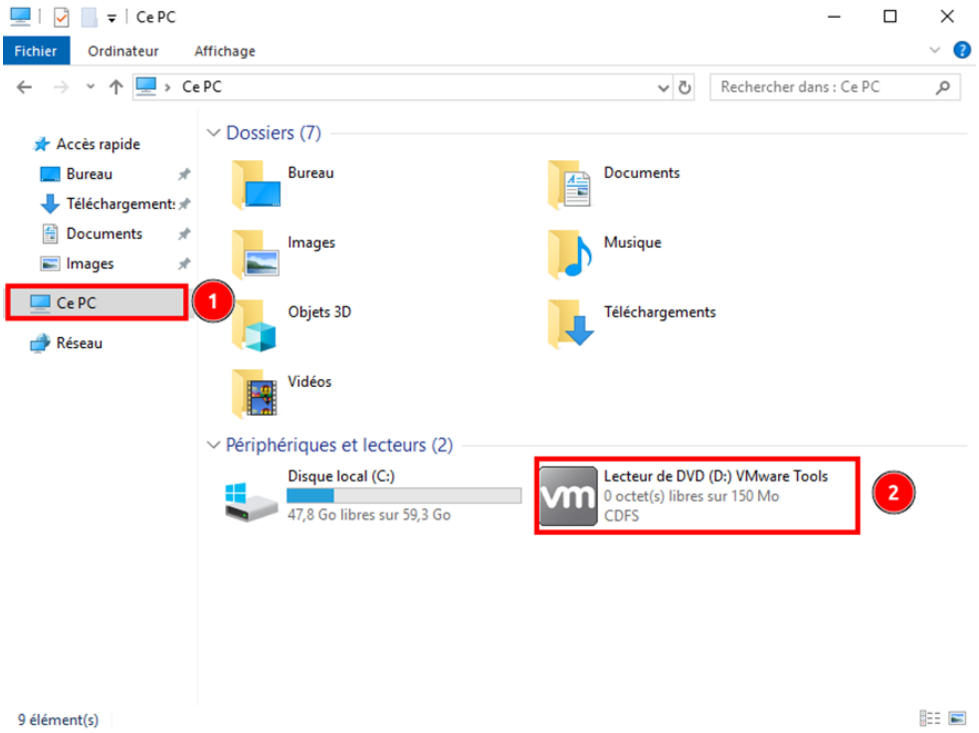


- Allez dans **Démarrer** puis entrez **Explorateur de fichiers** *(1)* et faites **Entrer** *(2)*.

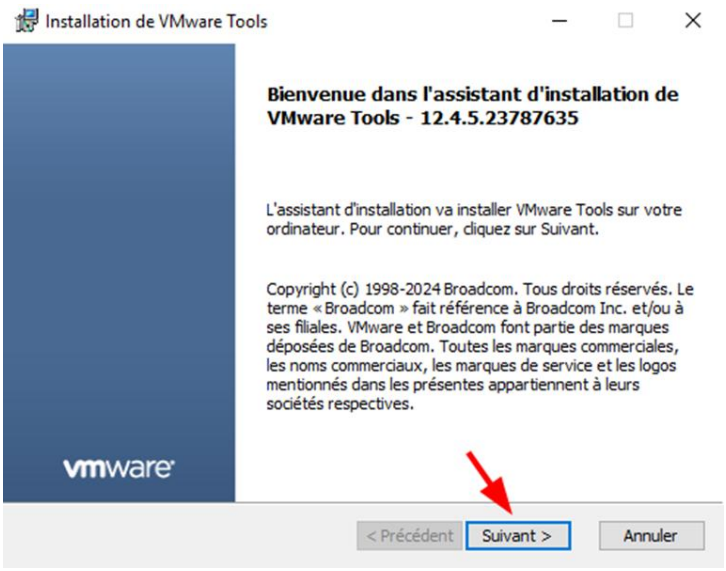
DOCUMENTATION D'INSTALLATION



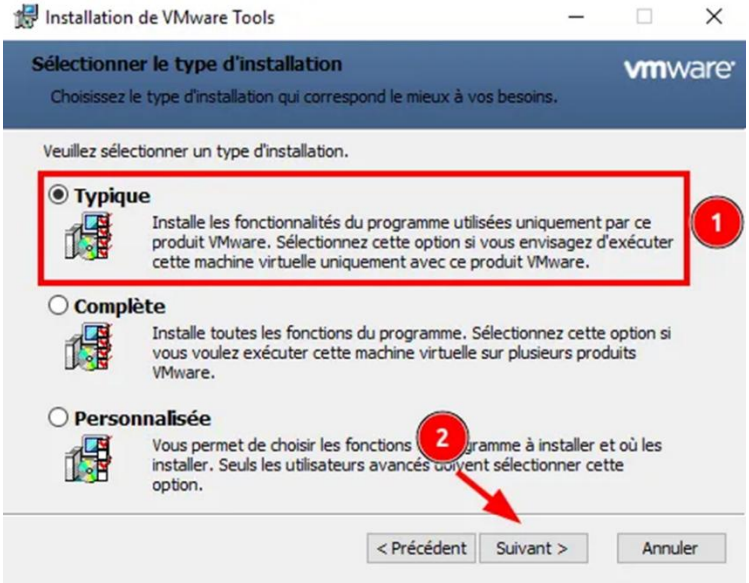
- Puis allez dans **Ce PC** *(1)* et double-cliquez sur **Lecteur de DVD (D:) VMware Tools** *(2)*.



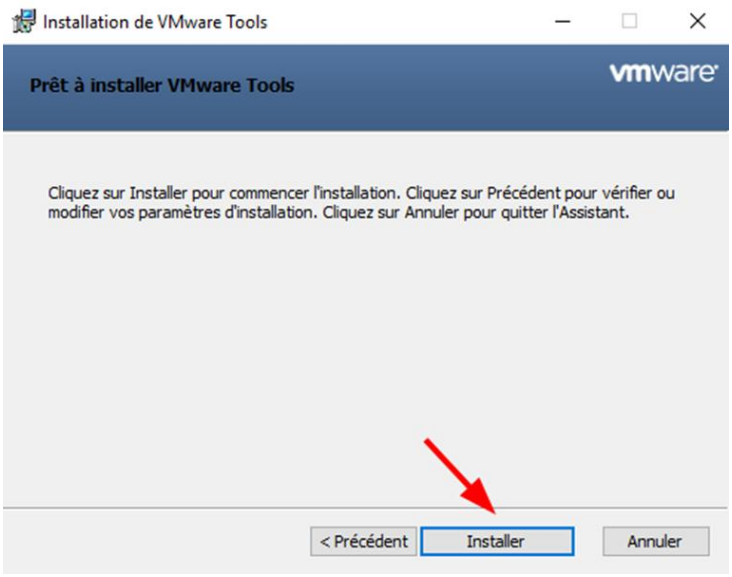
- Une fois sur l'installation, faites **Suivant**.



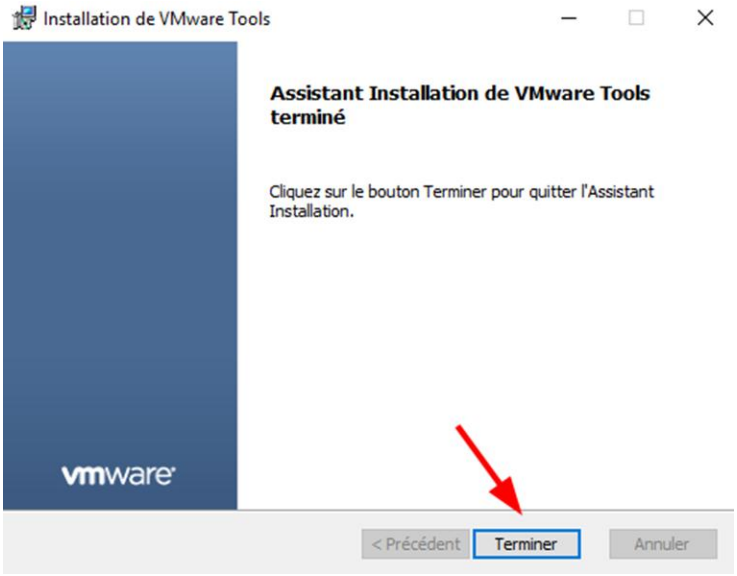
- Pour le type d'installation, sélectionnez **Typique** *(1)*.



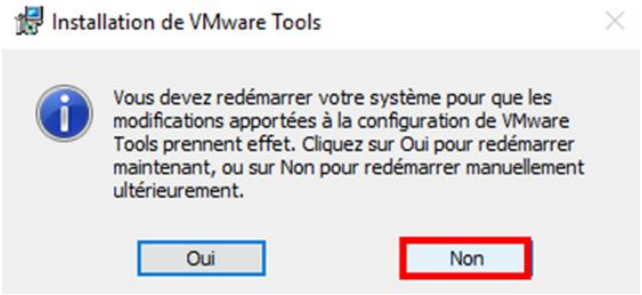
- Faites ensuite **Installer.**



- Puis l'installation va être terminé, cliquez sur **Terminer**.



- Enfin, mettez **Non** pour que votre système ne redémarre pas.



2. Documentation d'exploitation Windows

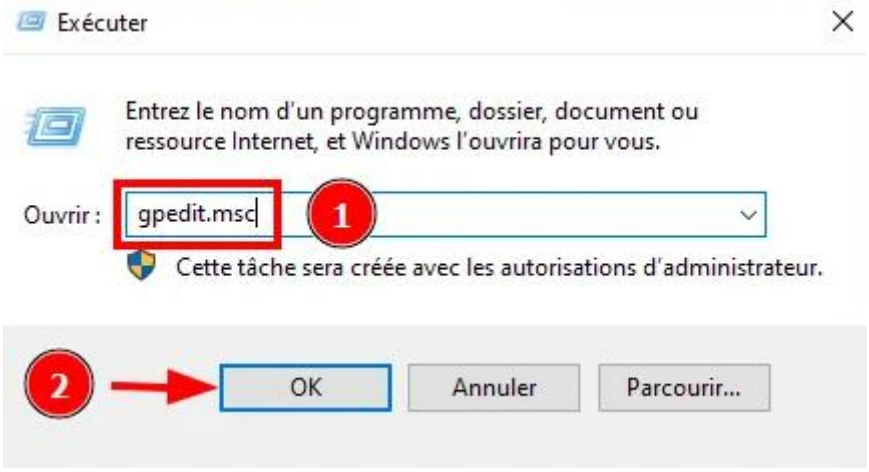
0. Paramètres biométriques et d'écran de verrouillage

1. Introduction

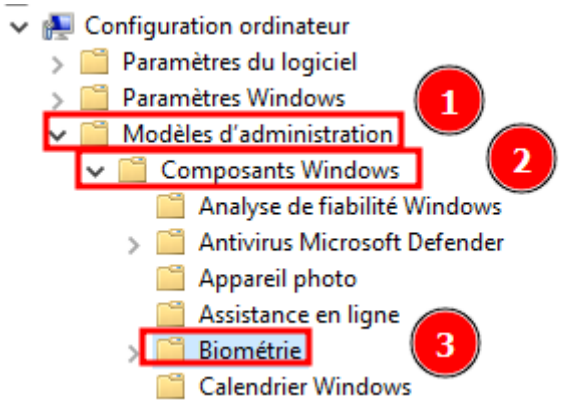
- Dans cette étape, nous allons configurer les paramètres liés à la **sécurité biométrique** et à l'écran de verrouillage sur **Windows 10 Entreprise**. Cette configuration est essentielle pour limiter les **risques d'accès non autorisé** via l'écran de connexion.

2. Activer Windows Hello

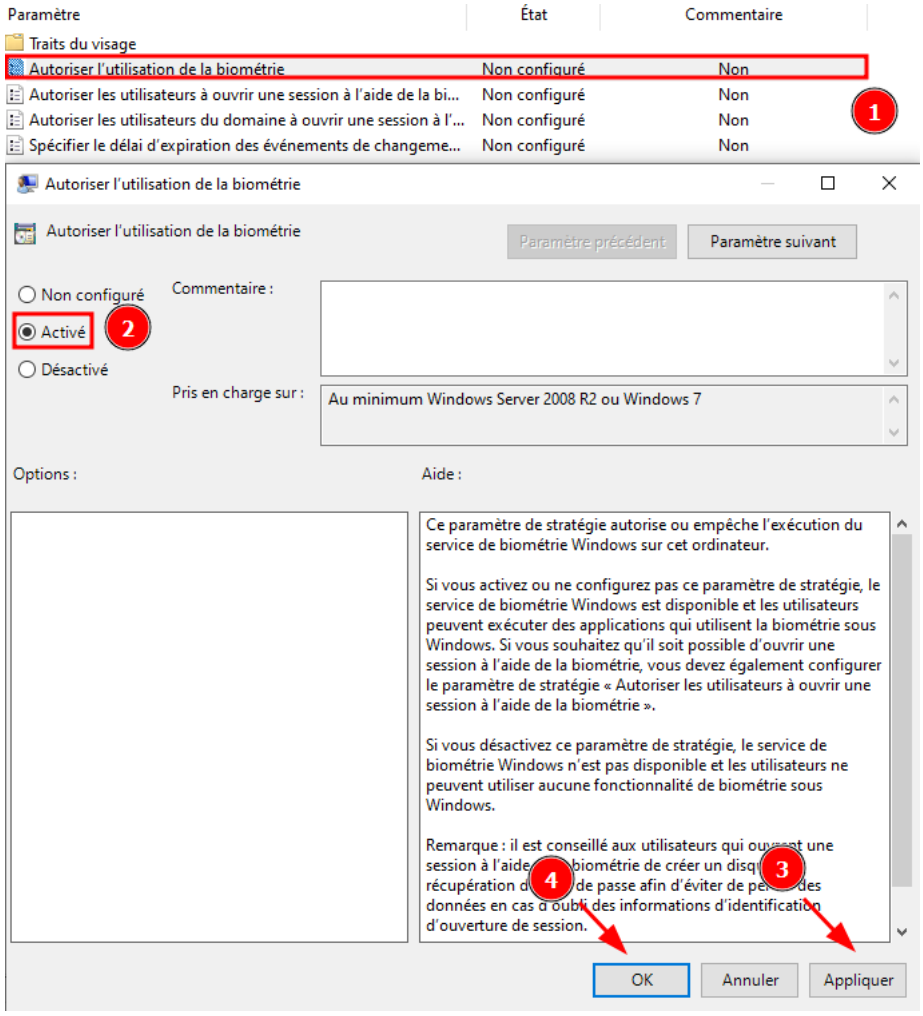
- Appuyez sur **Win + R**, tapez **gpedit.msc** *(1)*, puis appuyez sur **OK** *(2)*.



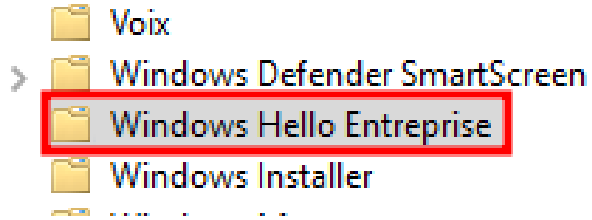
- Puis allez dans → **Modèles d'administration** *(1)* → **Composants Windows** *(2)* → **Biométrie** *(3)*.



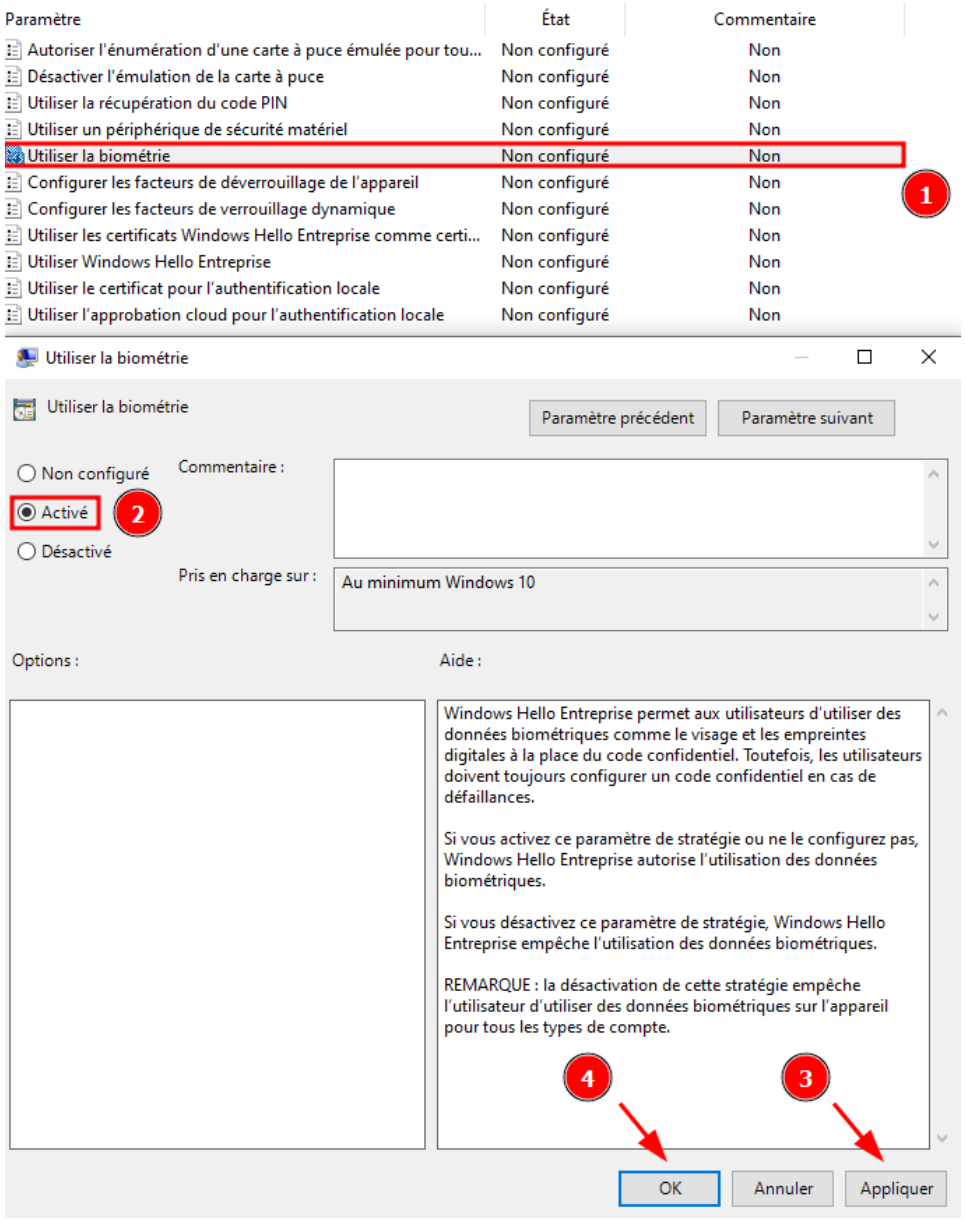
- Cliquez sur **Autoriser l'utilisation de la biométrie** *(1)* et **Activé** *(2)* l'option ensuite **Appliquer** *(3)* puis **OK** *(4)*.



- Puis allez dans **Windows Hello Entreprise.**



- Ouvrez **Utiliser la Biométrie** *(1)* et **Activé** *(2)* l'option ensuite **Appliquer** *(3)* puis **OK** *(4)*.



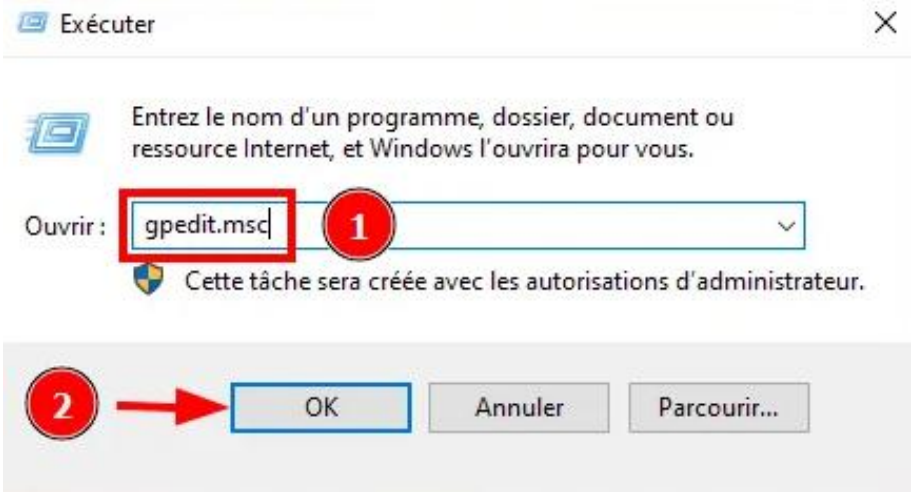
DOCUMENTATION D'EXPLOITATION

3. Configuration de la reconnaissance faciale avec anti-spoofing

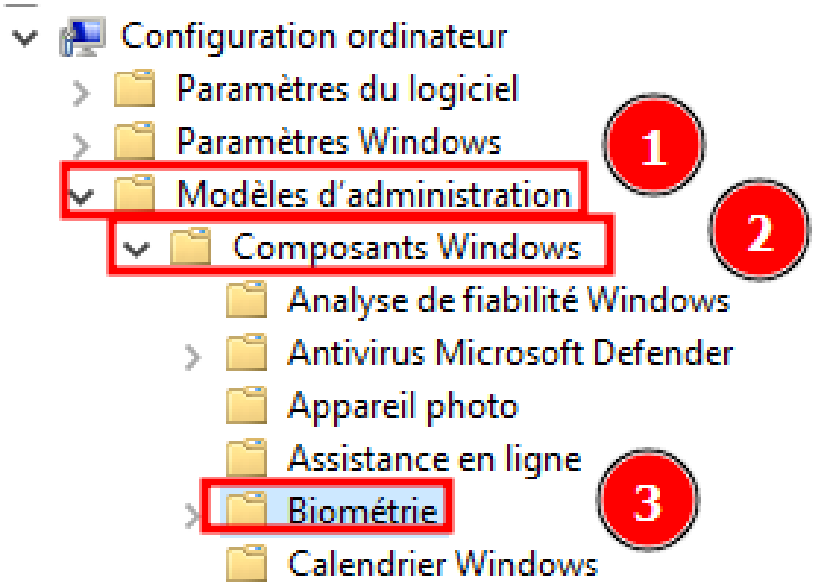
- Sous la section **Reconnaissance faciale (Windows Hello)**:
  - Si un appareil compatible est disponible, cliquez sur **Configurer**.
  - Suivez les instructions à l'écran pour enregistrer votre visage.

- Pour activer la protection **anti-spoofing:**

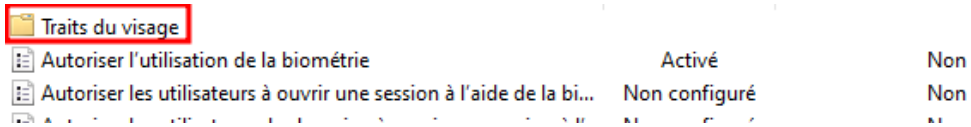
- Appuyez sur **Win + R**, tapez **gpedit.msc** *(1)*, puis appuyez sur **OK** *(2)*.



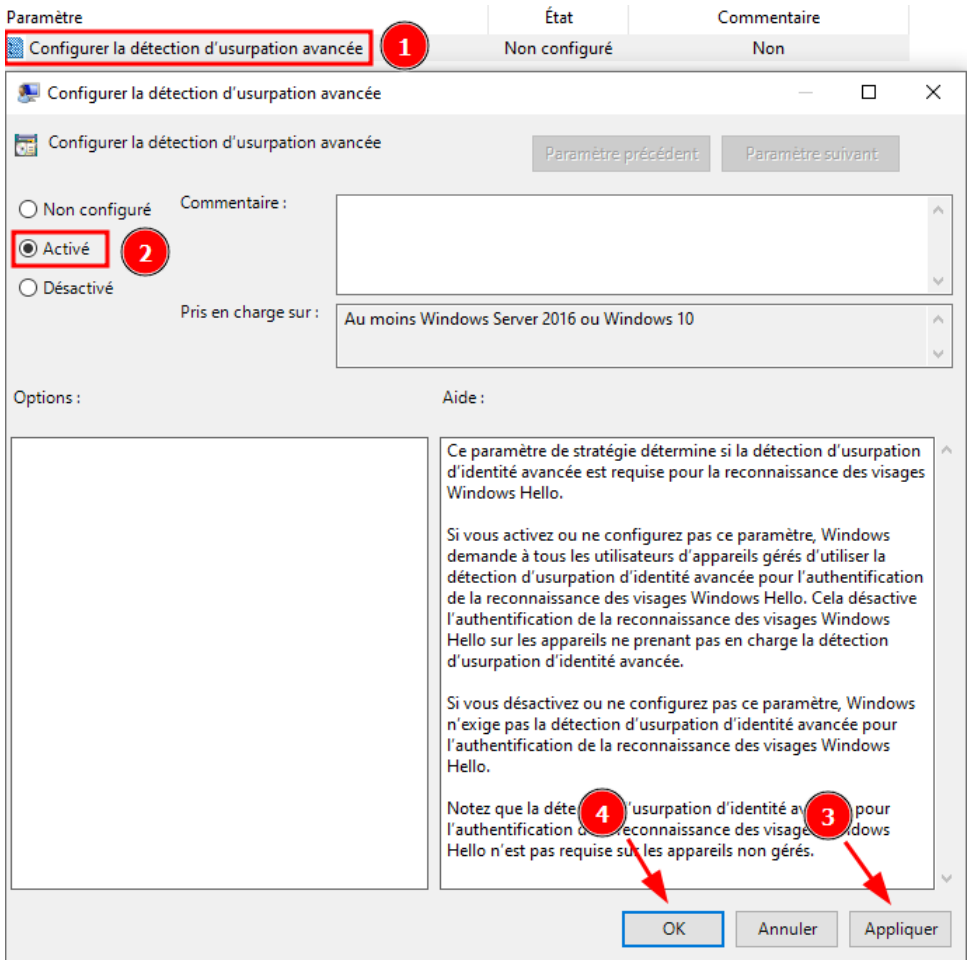
- Puis allez dans → **Modèles d'administration** *(1)* → **Composants Windows** *(2)* → **Biométrie** *(3)*.



- Cliquez sur **Traits du visage**.



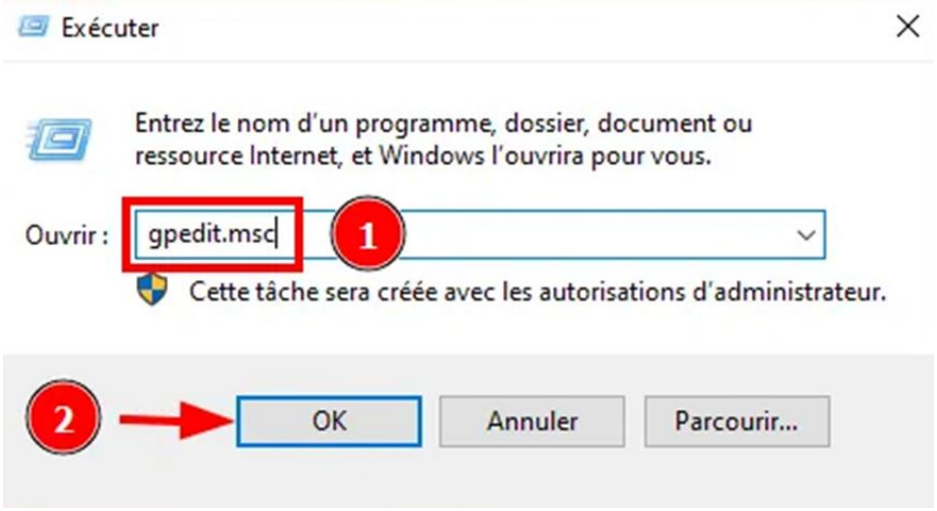
- Puis allez dans **Configurer la détection d'usurpation avancée** *(1)*, et **Activé** *(2)* l'option ensuite **Appliquer** *(3)* puis **OK** *(4)*.



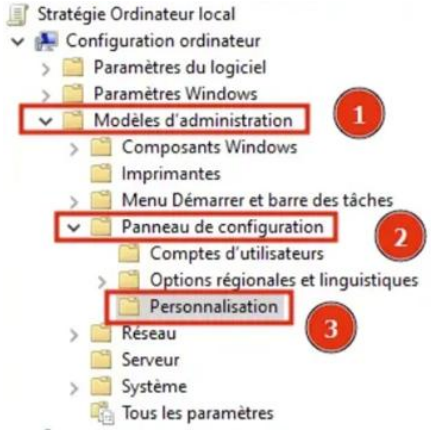
- Si cette option n'est pas disponible, vérifiez que votre caméra est compatible avec Windows Hello et prend en charge cette fonctionnalité.

4. Désactiver l'utilisation de la camera sur l'écran de verouillage

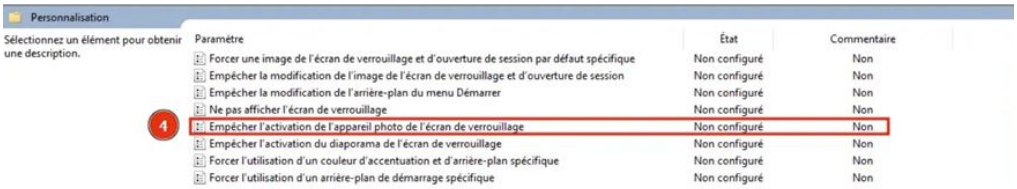
- Appuyez sur **Win + R**, tapez **gpedit.msc** *(1)*, puis appuyez sur **OK** *(2)*.



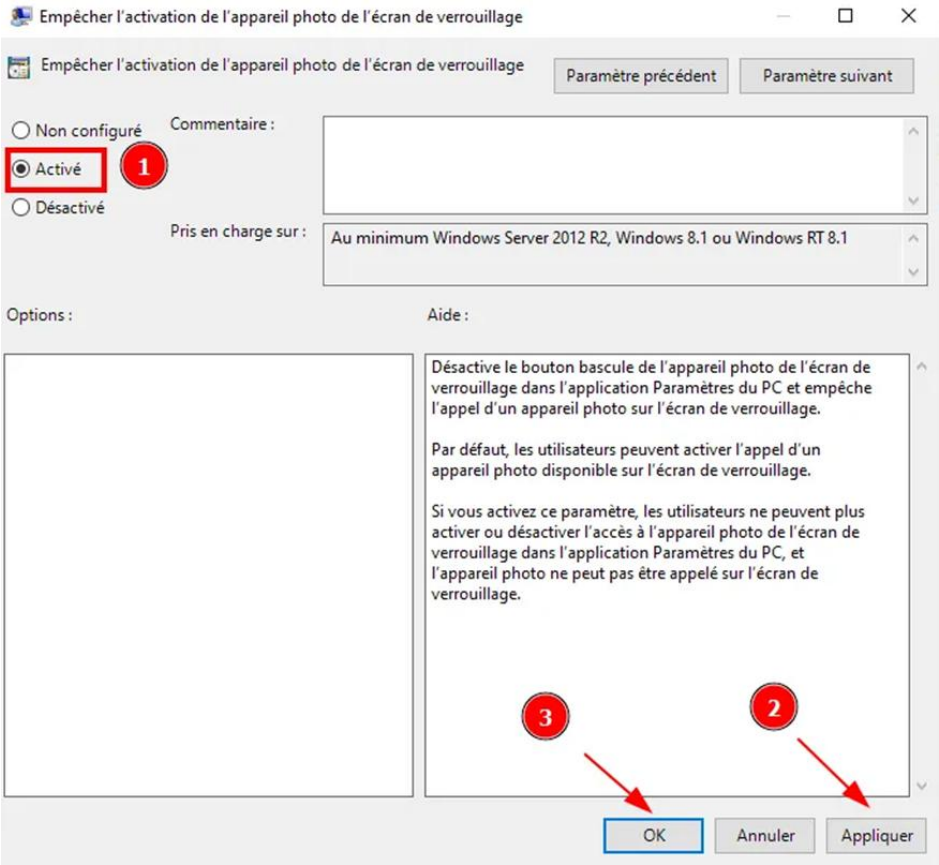
- Naviguez vers **Modèles d'administration** *(1)* → **Panneau de configuration** *(2)* → **Personnalisation** *(3)*.



- Puis allez dans → **Empêcher l'activation de l'appareil photo de l'écran de verrouillage** *(4)*.

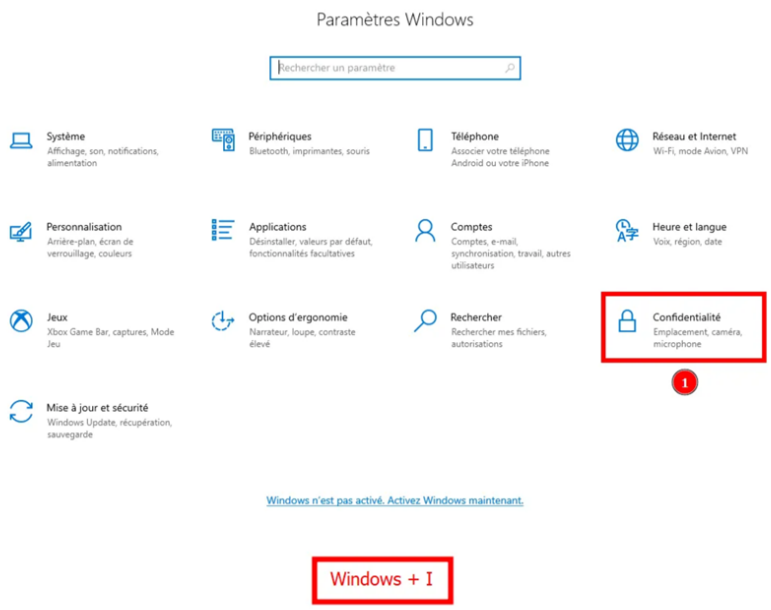


- Activer **Empêcher l'activation de l'appareil photo de l'écran de verrouillage** *(1)***,** faite **Appliquer** *(2)* puis **OK** *(3)*.

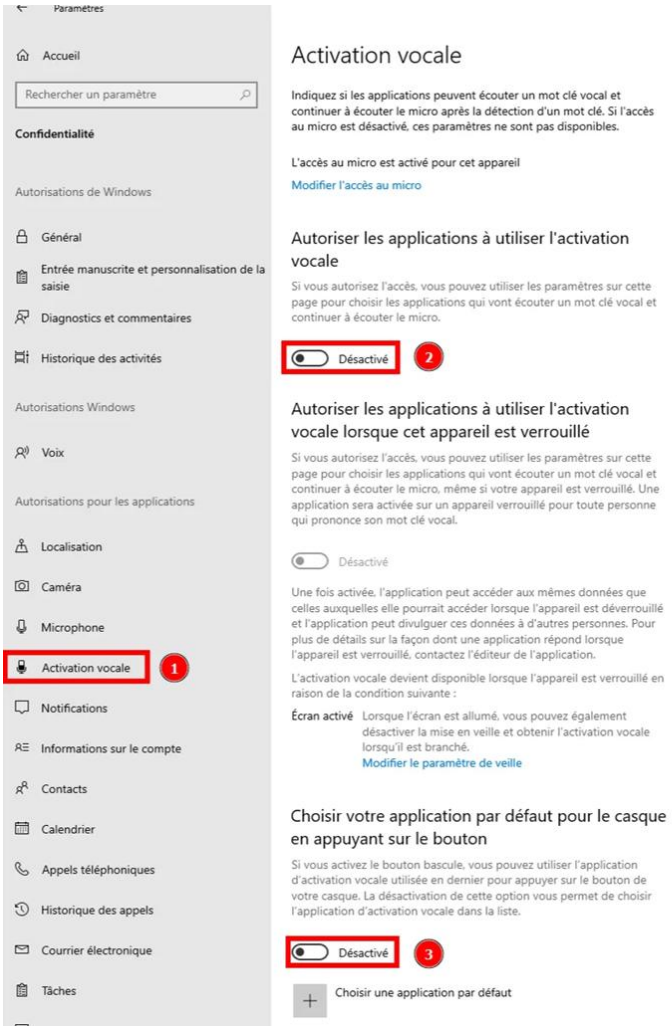


5. Empêcher l'activation vocale sur un appareil vérouillé

- Toujours dans la fenêtre des **Paramètres Windows (Windows + I)**, allez dans **Confidentialité** *(1).*



- Allez dans → **Activation vocale** *(1)*. Dans la section **Autoriser les applications à utiliser l'activation vocale** :
    - Désactivez l'option *(2)*.
    - Désactivez l'option **Choisir votre application par défaut pour le casque en appuyant sur le bouton** *(3)*.



6. Vérification finale

- Verrouillez votre session en appuyant sur **Win + L** pour vérifier les modifications:
  - La caméra ne doit pas s'activer automatiquement.
  - Aucun message ou option d'activation vocale ne doit apparaître.
  - Si la reconnaissance faciale est activée, testez son bon fonctionnement avec les paramètres de sécurité configurés.

7. Pourquoi ces étapes sont importantes ?

- **Reconnaissance faciale :** La protection anti-spoofing empêche des attaques utilisant des photos ou vidéos du visage de l'utilisateur.
- **Caméra :** Désactiver la caméra réduit les vecteurs d'attaques potentiels à l'écran de verrouillage.
- **Activation vocale :** Les commandes vocales depuis un appareil verrouillé peuvent être exploitées pour obtenir des informations ou exécuter des actions non autorisées.

1. DNS et sécurité réseau

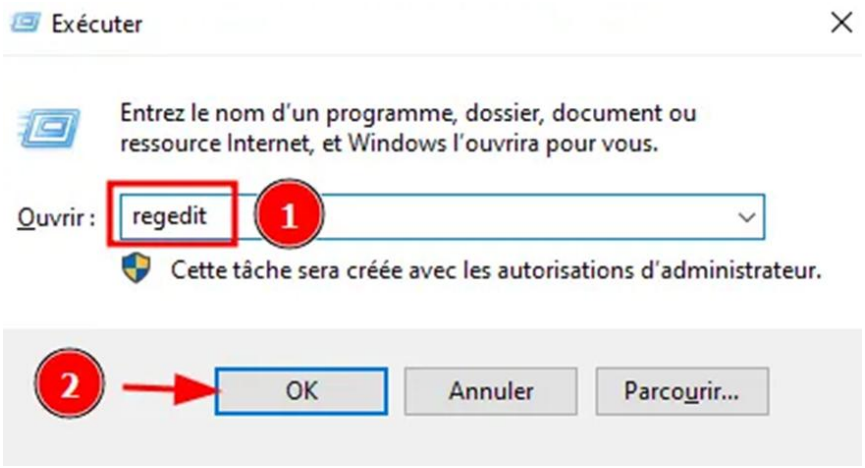
1. Introduction

Dans cette étape, nous allons configurer les paramètres DNS et réseau pour renforcer la sécurité du système. Cela inclut la désactivation de protocoles obsolètes et de configurations susceptibles d'être exploitées par des attaquants.

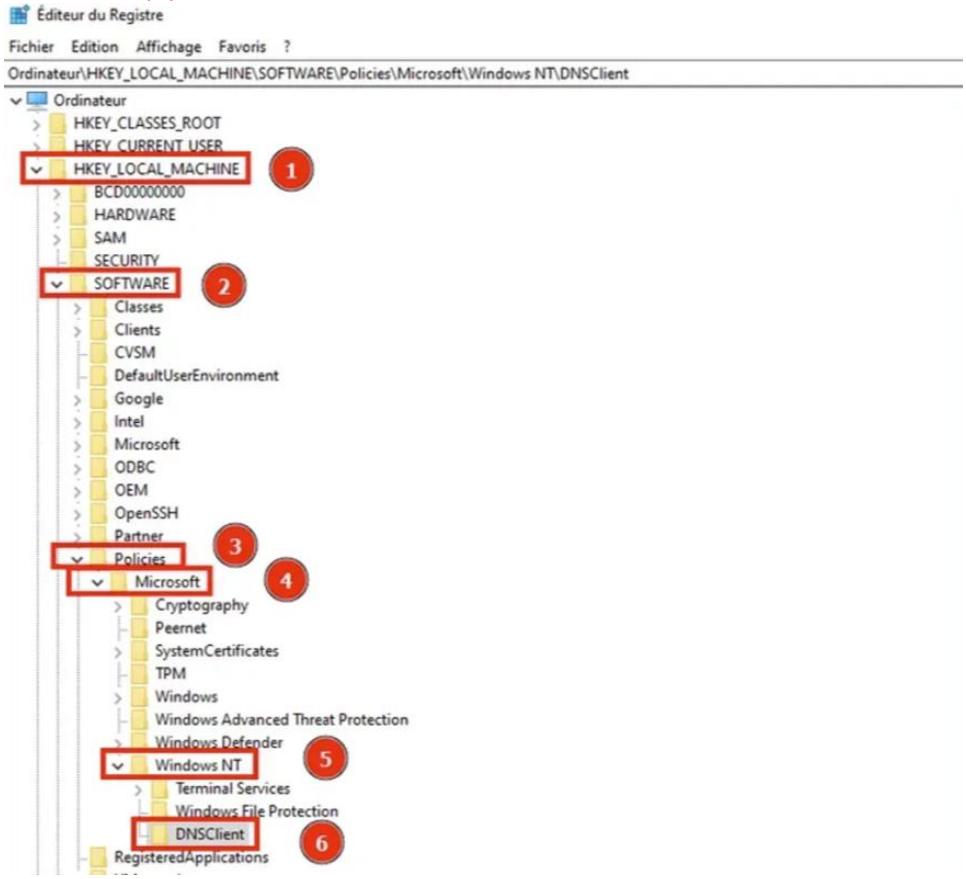
2. Désactiver la diffusion DNS Multicast

La diffusion DNS Multicast (mDNS) est utilisée pour la découverte de services sur un réseau local, mais elle peut également être exploitée pour des attaques.

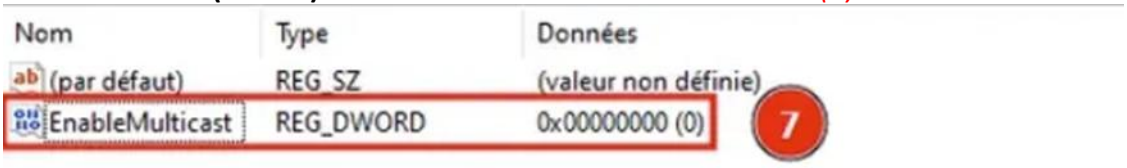
- Appuyez sur **Win + R**, tapez **regedit** *(1)*, puis appuyez sur **OK** *(2)*.



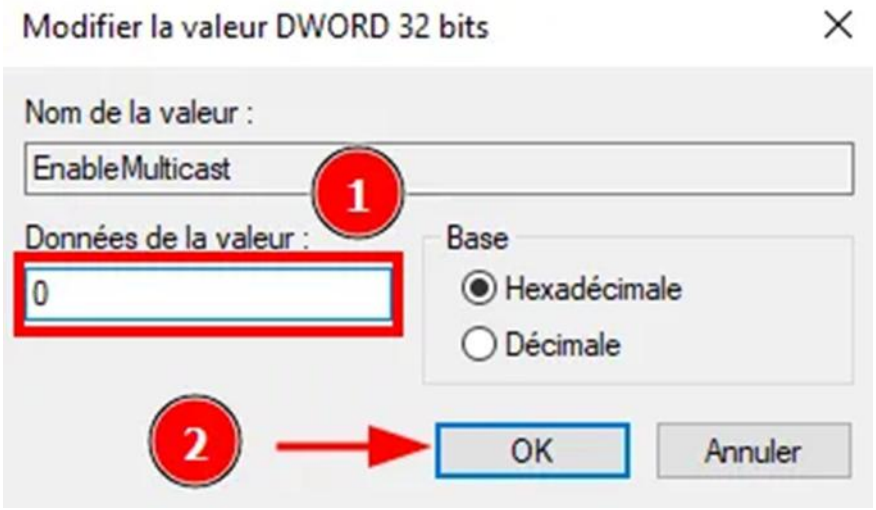
- Naviguez vers la clé suivante :
    - `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\DNSClient`
- Si la clé **DNSClient** n'existe pas, créez-la :
    - Faites un clic droit sur **Windows NT**, choisissez **Nouveau > Clé**, et nommez-la **DNSClient** *(6)*.



- À l'intérieur de **DNSClient**, faites un clic droit dans l'espace vide, choisissez **Nouveau > Valeur DWORD (32 bits)** et nommez la valeur **EnableMulticast** *(7)*.



- Double-cliquez dessus, définissez la valeur sur **0** *(1)*, puis cliquez sur **OK** *(2)*.



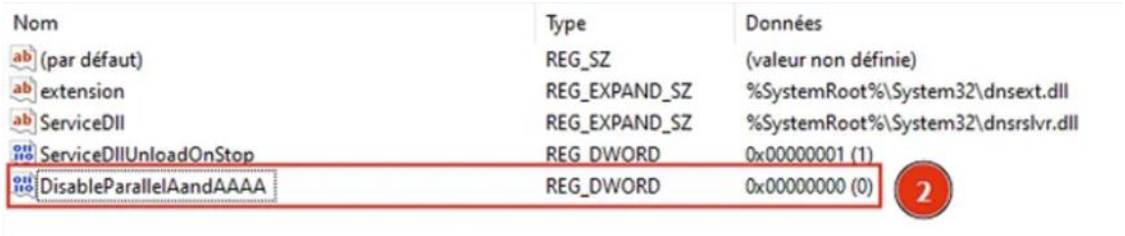
- Redémarrez pour appliquer les modifications.

3. Désactiver les requêtes DNS parallèles A et AAAA

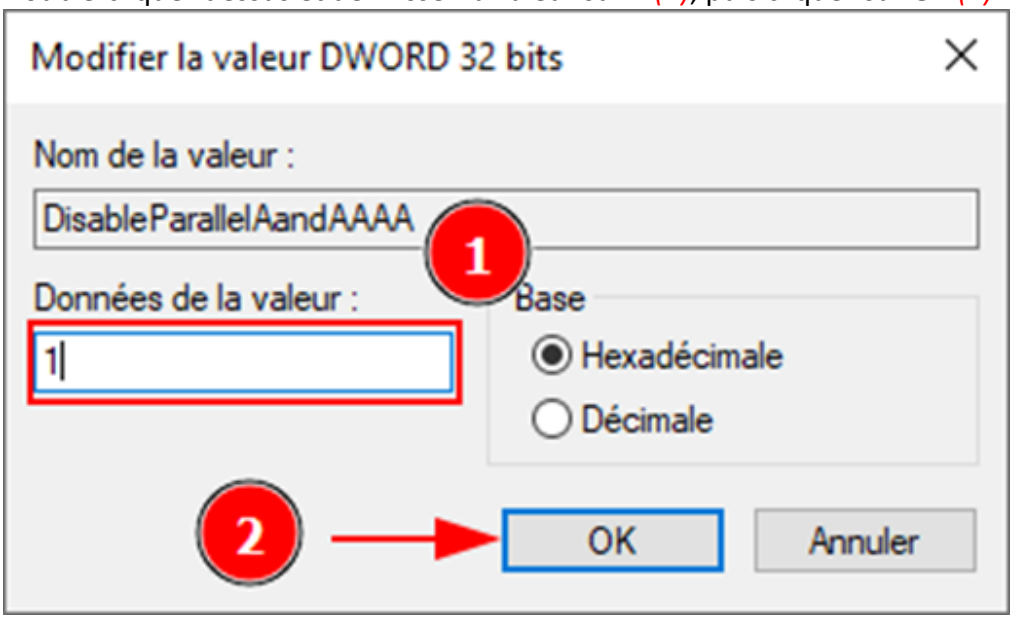
Les requêtes parallèles peuvent augmenter la surface d'attaque en permettant à un attaquant de détourner les requêtes DNS.

- Retournez dans l'Éditeur de Registre (**regedit**).
- Accédez à la clé suivante :
  - `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters`

- Faites un clic droit dans l'espace vide, choisissez **Nouveau > Valeur DWORD (32 bits)**.
  - Nommez la valeur **DisableParallelAandAAAA** *(2)*.



- Double-cliquez dessus et définissez la valeur sur **1** *(1)*, puis cliquez sur **OK** *(2)*.

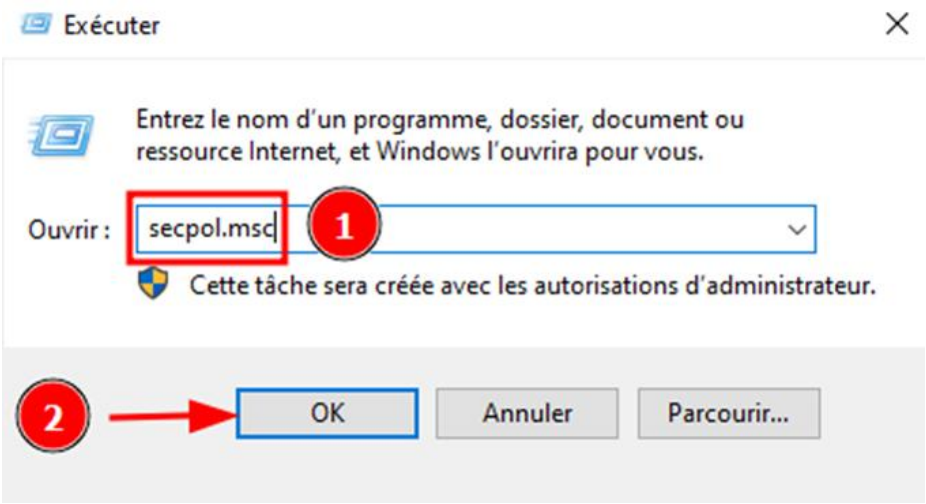


- Redémarrez pour appliquer les modifications.

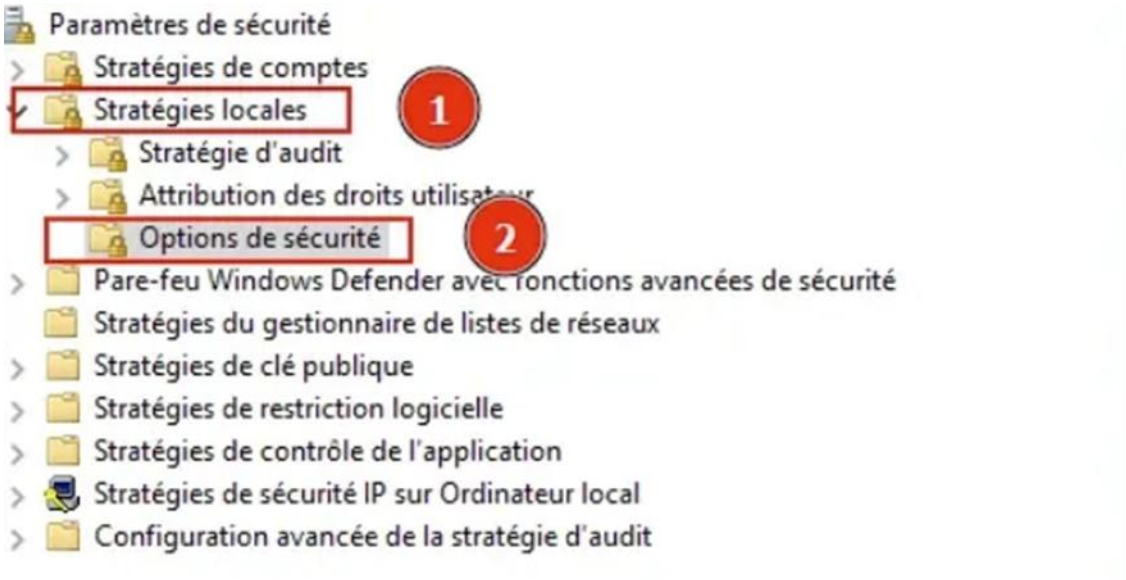
4. Désactiver NTLMv1

NTLMv1 est une méthode d'authentification obsolète et vulnérable.

- Configurer la **Stratégie de Sécurité Locale:**
  - Appuyez sur **Win + R**, tapez **secpol.msc** *(1)*, et appuyez sur **OK** *(2)*.

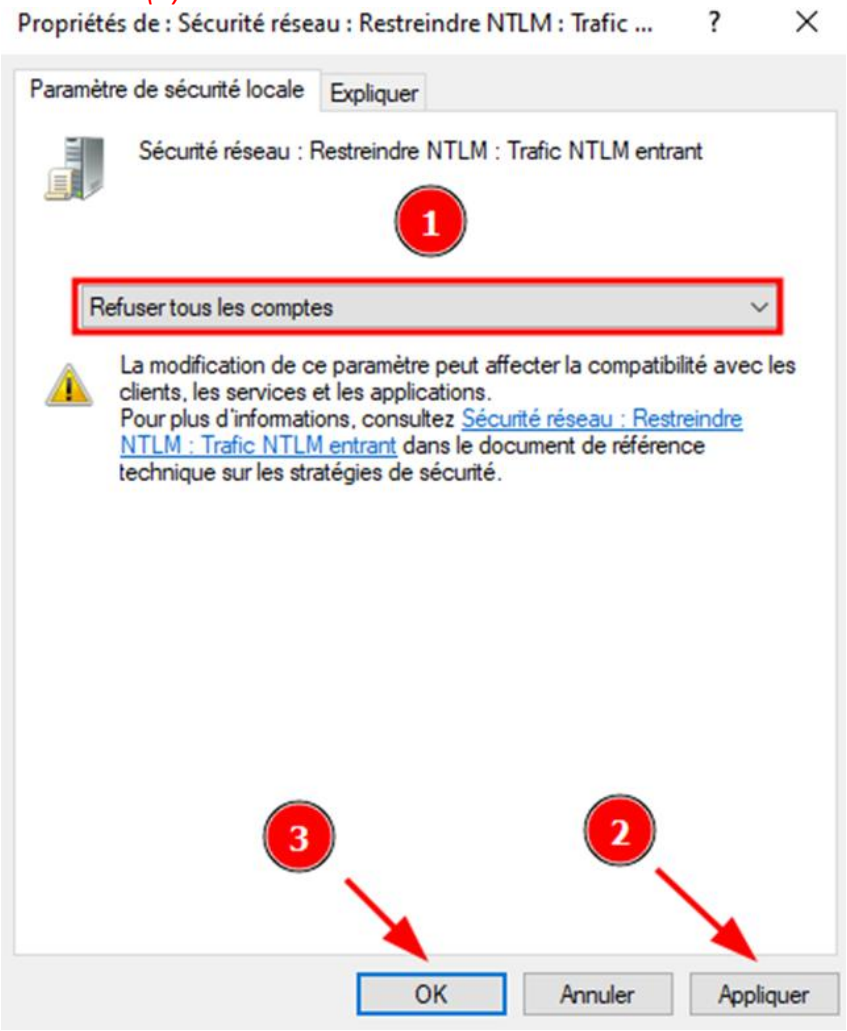


- Dans la console, accédez à → **Stratégies locales** *(1)* → **Options de sécurité** *(2)*.



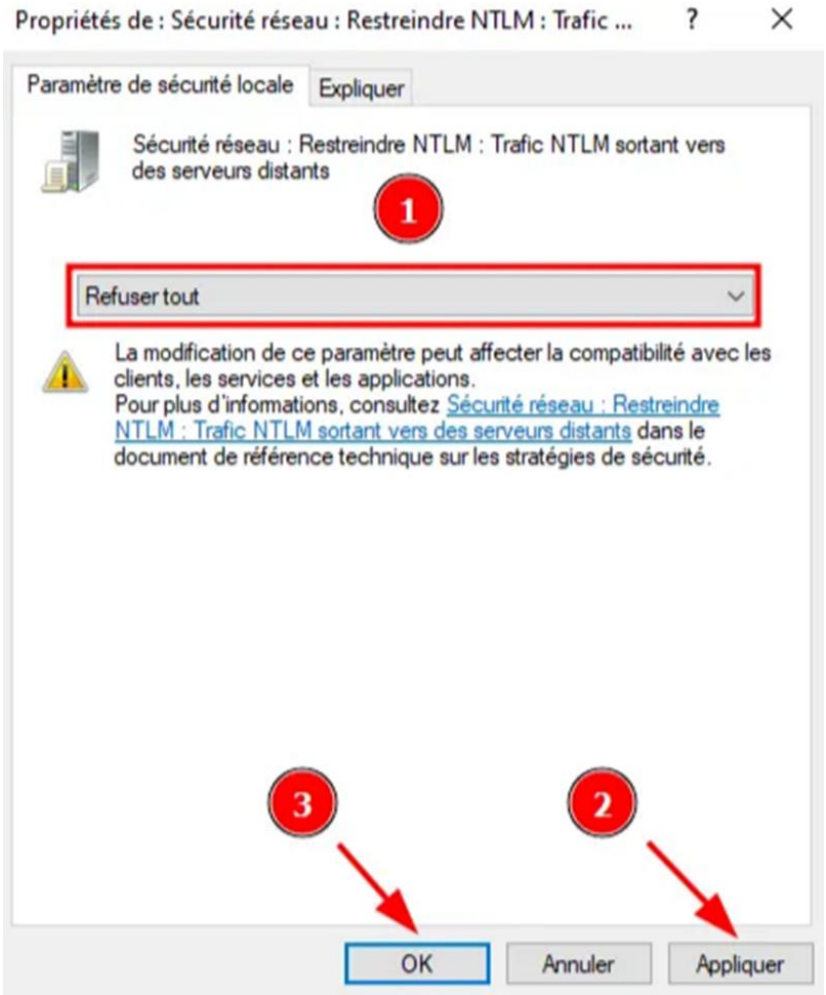
- Localisez l'option **Sécurité réseau : Restreindre NTLM : Trafic NTLM entrant** *(3)*.

- Double-cliquez dessus et sélectionnez **Refuser tous les comptes** *(1)* puis **Appliquer** *(2)* et faite **OK** *(3)*.



- Faites de même pour **Sécurité réseau : Restreindre NTLM : trafic NTLM sortant**.

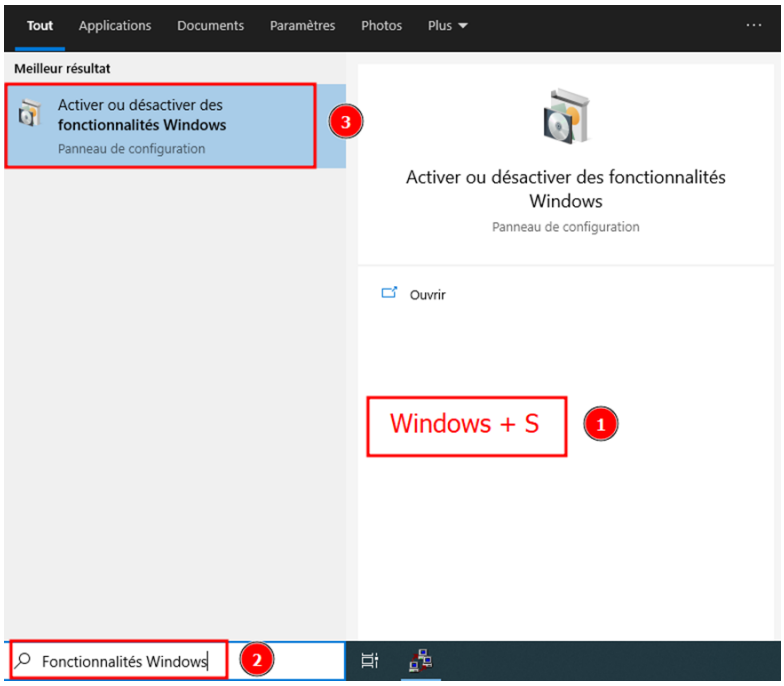
- Double-cliquez dessus et sélectionnez **Refuser tout** *(1)* puis **Appliquer** *(2)* et faite **OK** *(3)*.



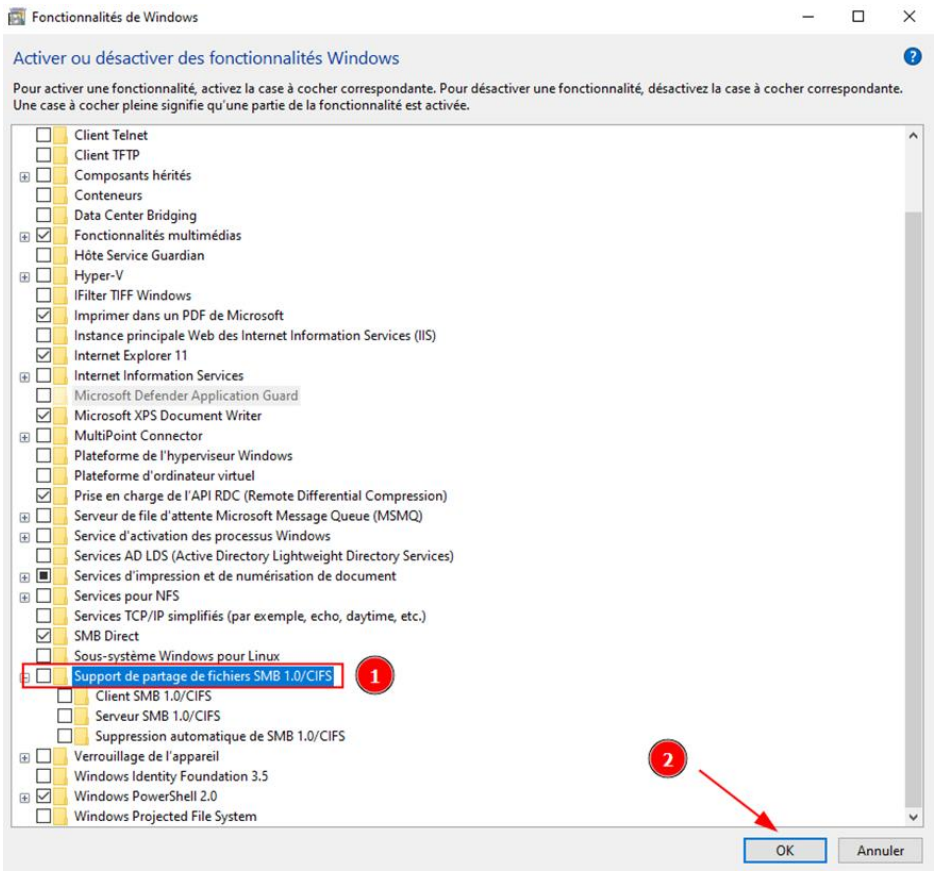
5. Désactiver SMBv1

SMBv1 est un protocole de partage de fichiers vulnérable qui doit être désactivé.

- Désactiver **SMBv1** via les fonctionnalités Windows:
  - Appuyez sur **Win + S** *(1)*, tapez **Fonctionnalités Windows** *(2)*, et sélectionnez **Activer ou désactiver des fonctionnalités Windows** *(3)*.



- Faites défiler jusqu'à **Support de partage de fichiers SMB 1.0/CIFS et** décochez cette option *(1)* puis cliquez sur **OK** *(2)*.

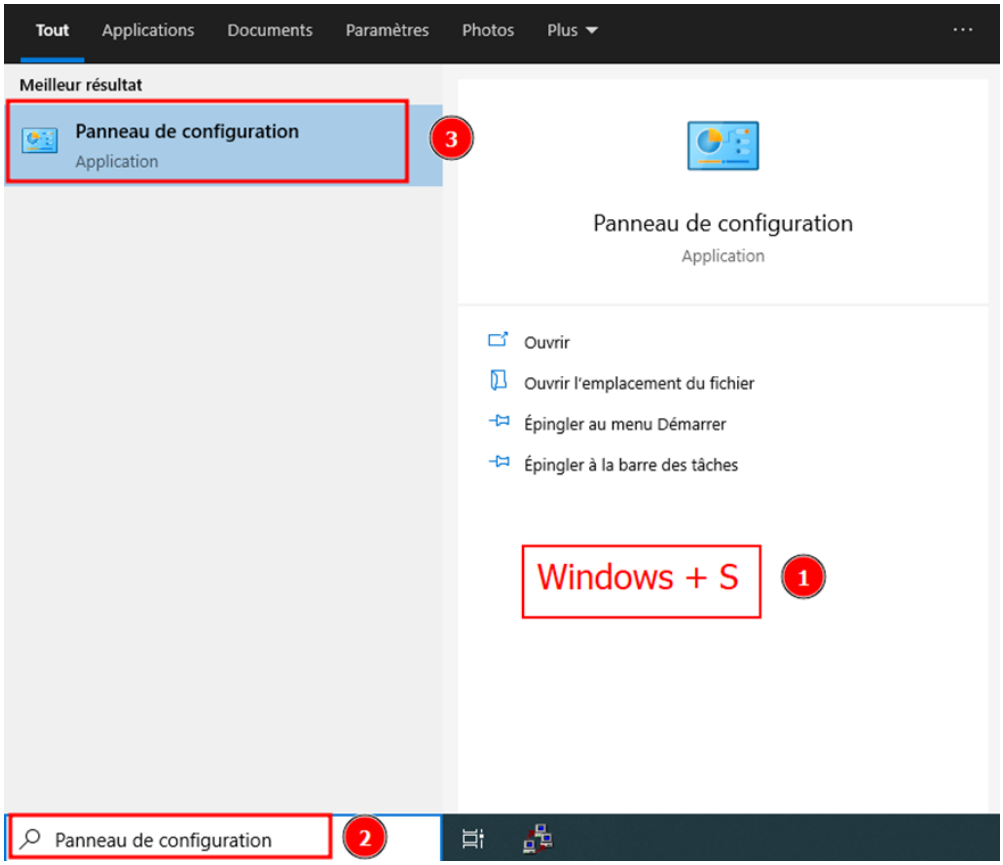


- Redémarrez votre machine.

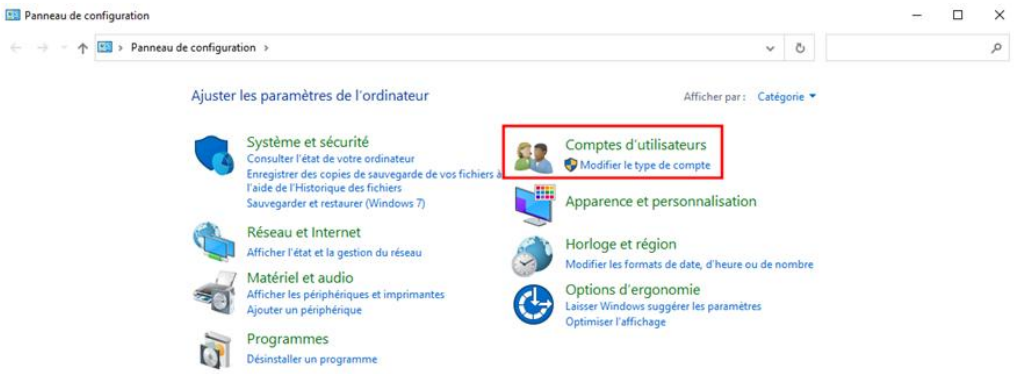
6. Activer et configurer l'UAC (User Account Control)

L'UAC est une couche de sécurité qui demande une confirmation avant d'exécuter des actions nécessitant des privilèges élevés.

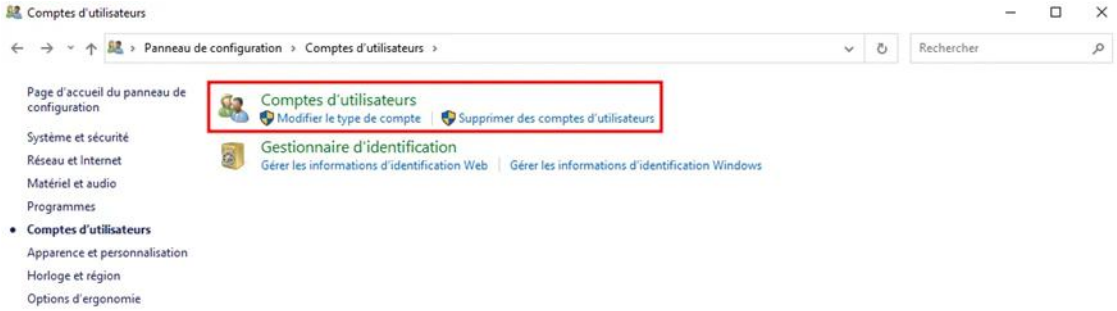
- Configurer **l'UAC:**
  - Appuyez sur **Win + S** *(1)*, tapez **Panneau de configuration** *(2)*, et ouvrez-le *(3)*.



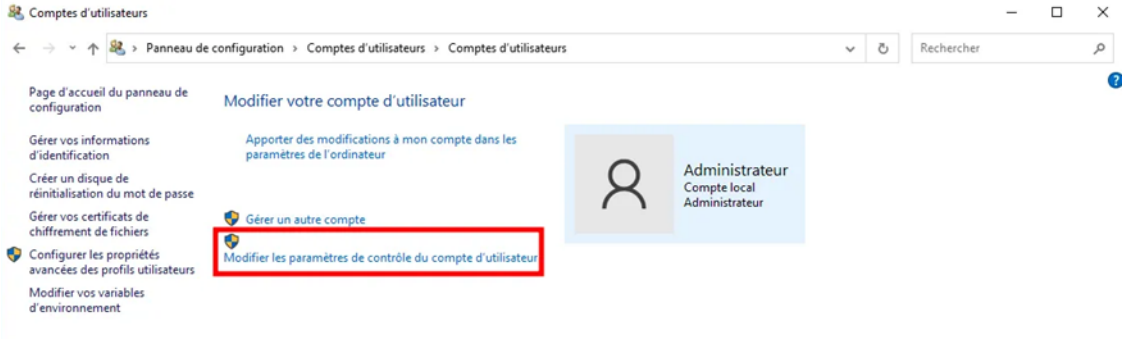
- Allez dans → **Comptes d'utilisateurs.**



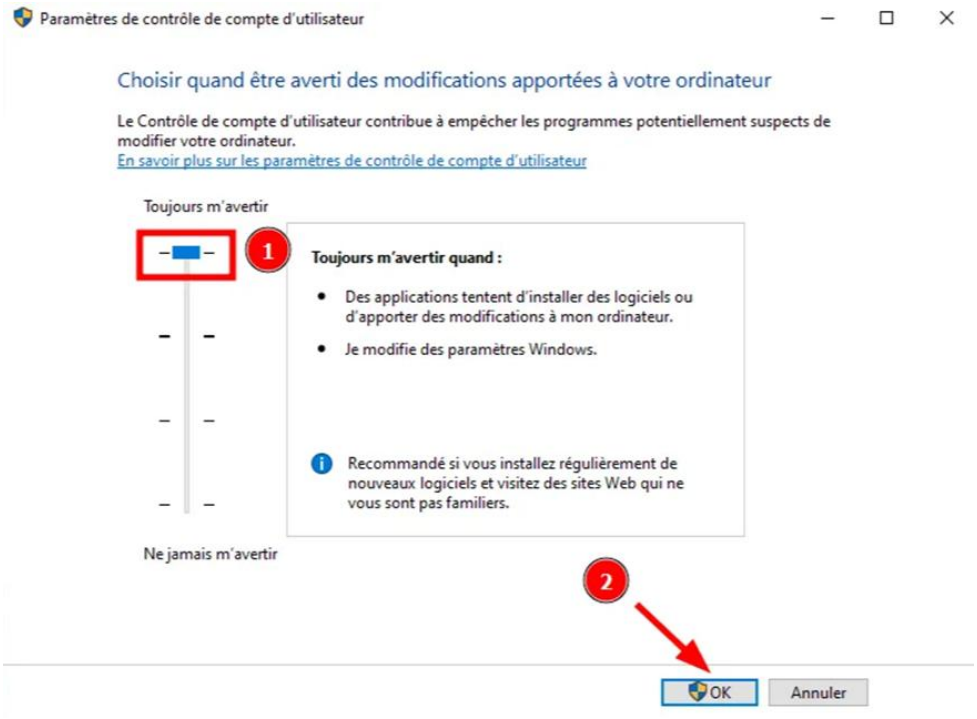
- Allez dans → **Comptes d'utilisateurs.**



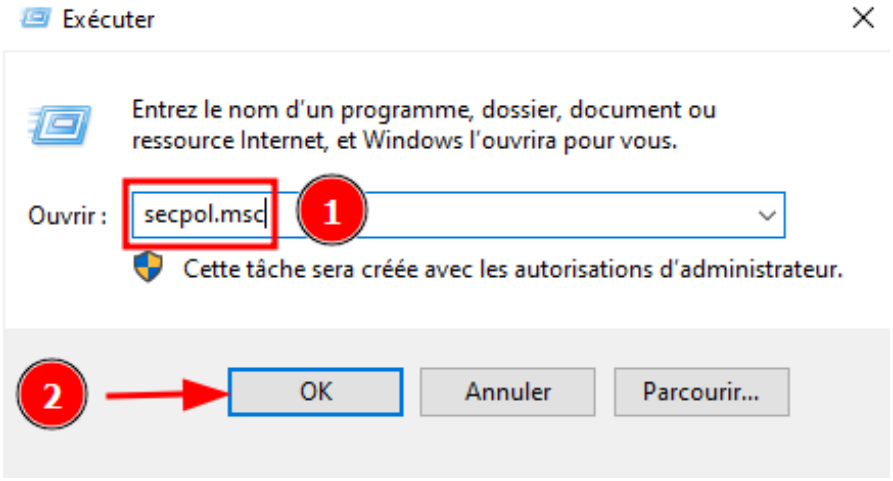
- Allez dans **Modifier les paramètres de contrôle de compte d'utilisateur**.



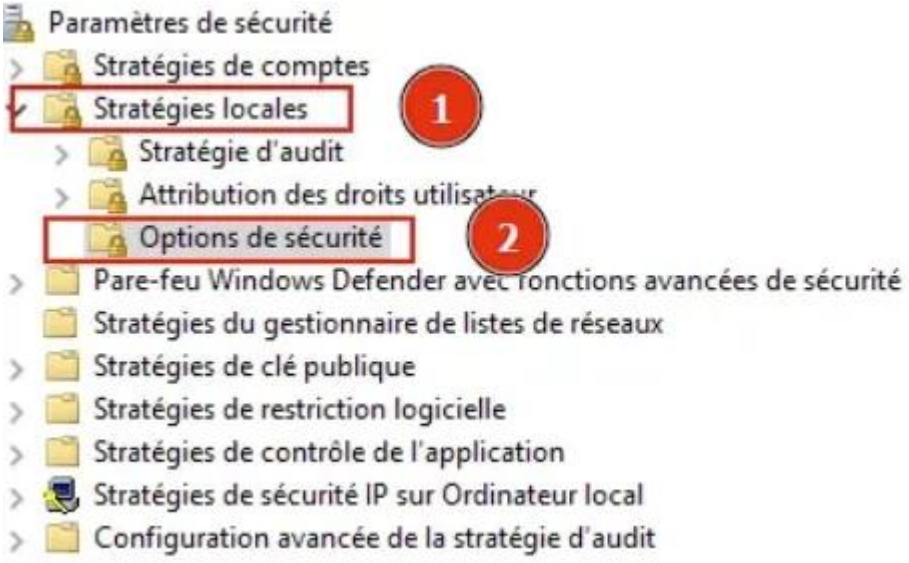
- Réglez le curseur sur **Toujours m'avertir** (le niveau le plus élevé) *(1)* puis cliquez sur **OK** *(2)*.



- Appuyez sur **Win + R**, tapez **secpol.msc** *(1)*, et appuyez sur **OK** *(2)*.



- Accédez à → **Stratégies locales** *(1)* → **Options de sécurité** *(2)*.



- Faite la même chose pour les options ci-dessous :
  - Arrêt : effacer le fichier d'échange de mémoire virtuelle : **Activé.**
  - Contrôle de compte d'utilisateur : élever uniquement les exécutables signés et validés : **Activé.**
  - Cryptographie système : force une protection forte des clés utilisateur enregistrées sur l'ordinateur : **Activé.**
  - Auditer l'accès aux objets système globaux : **Activé**.
  - Auditer : auditer l'utilisation des privilèges de sauvegarde et de restauration : **Activé**.
  - Activer l'UAC pour les administrateurs : **Activé**.

6. Pourquoi ces étapes sont importantes ?

- **mDNS et requêtes parallèles DNS :** Ces fonctions augmentent la surface d'attaque et peuvent être utilisées pour l'espionnage ou la redirection des requêtes DNS.
- **NTLMv1 et SMBv1 :** Ces protocoles obsolètes sont des cibles privilégiées pour les attaques (par ex. EternalBlue).
- **UAC :** L'activation de l'UAC protège contre les exécutions non autorisées en demandant une validation explicite pour les opérations sensibles.

2. Sécurité des mots de passe et de l'authentification

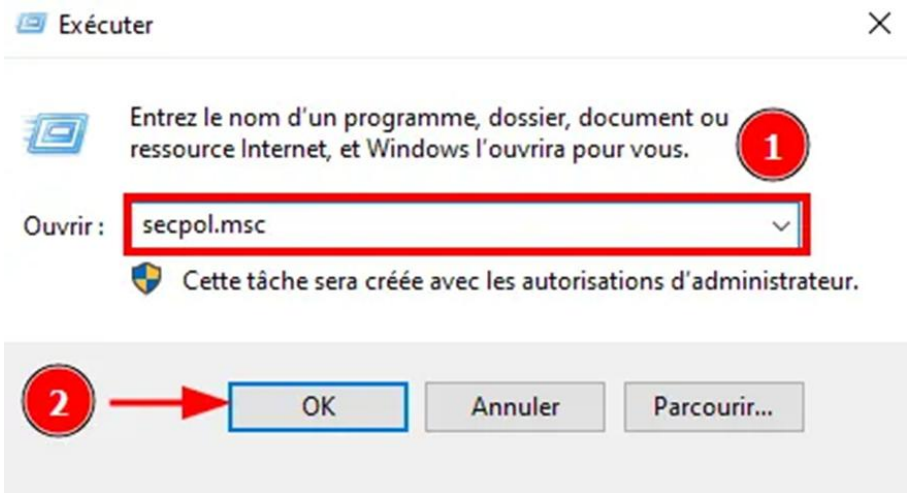
1. Introduction

- Dans cette étape, nous allons appliquer des politiques renforcées pour les mots de passe et l'authentification afin de minimiser les risques liés aux comptes utilisateurs.

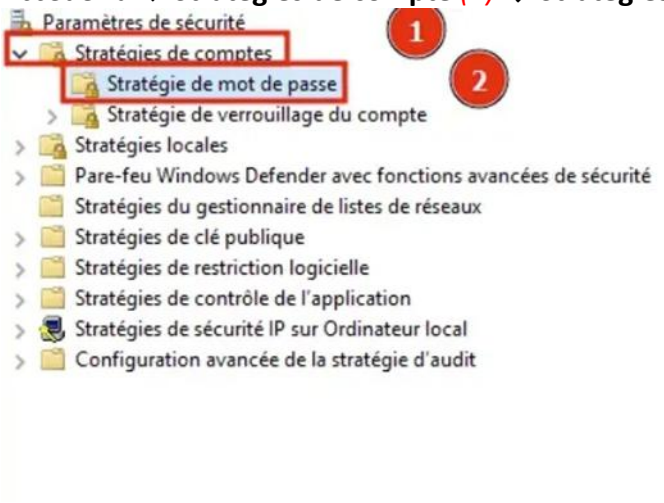
2. Politique de mots de passe

- La politique doit exiger des mots de passe complexes, longs, et régulièrement changés.

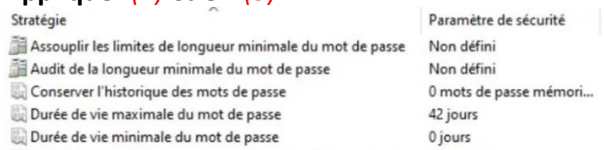
- **Configurer via la stratégie de sécurité locale:**
  - Appuyez sur **Win + R**, tapez **secpol.msc** *(1)*, et appuyez sur **OK** *(2)*.

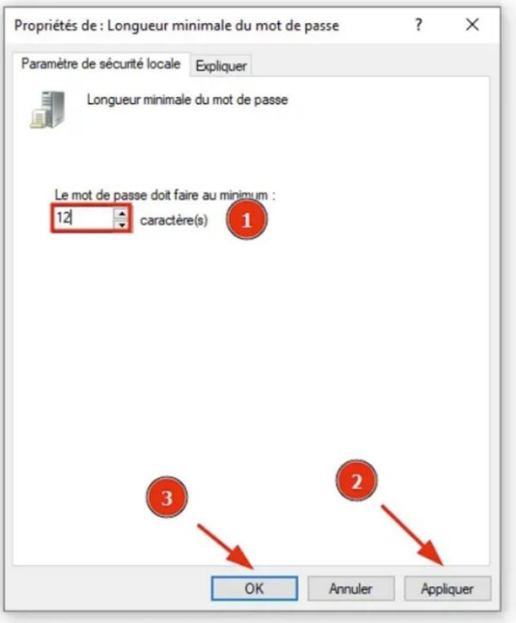


- Accédez à → **Stratégies de compte** *(1)* → **Stratégies de mot de passe** *(2)*.

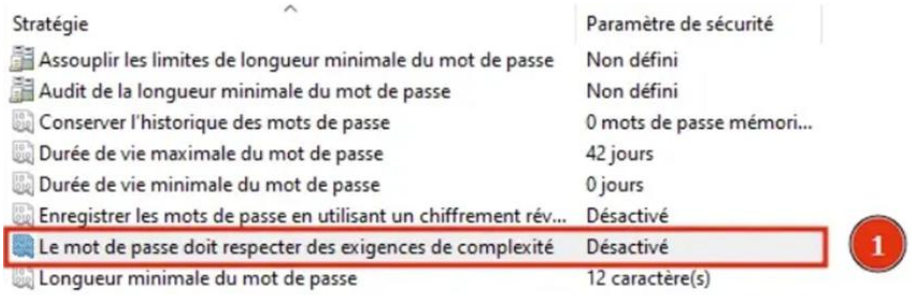


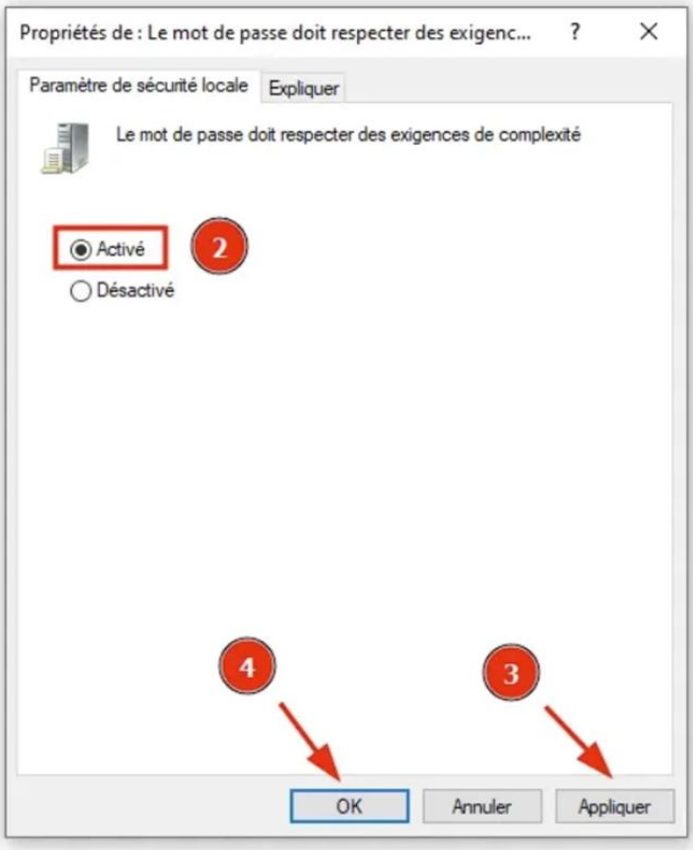
- Modifiez les paramètres suivants :
  - **Longueur minimale du mot de passe** : définissez à **12 caractères** *(1)* puis faites **Appliquer** *(2)* et **OK** *(3)*.



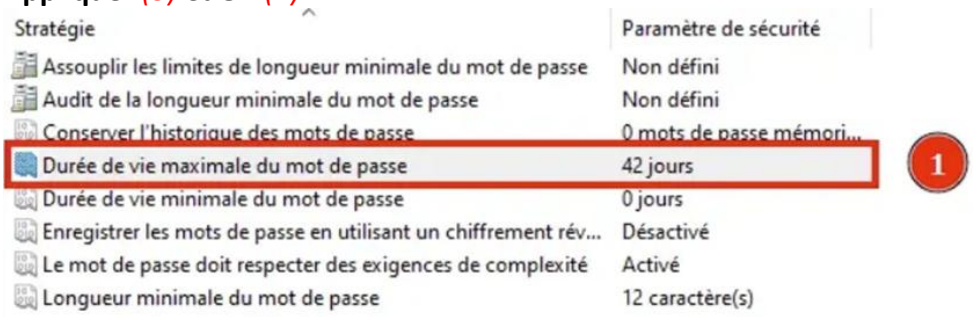


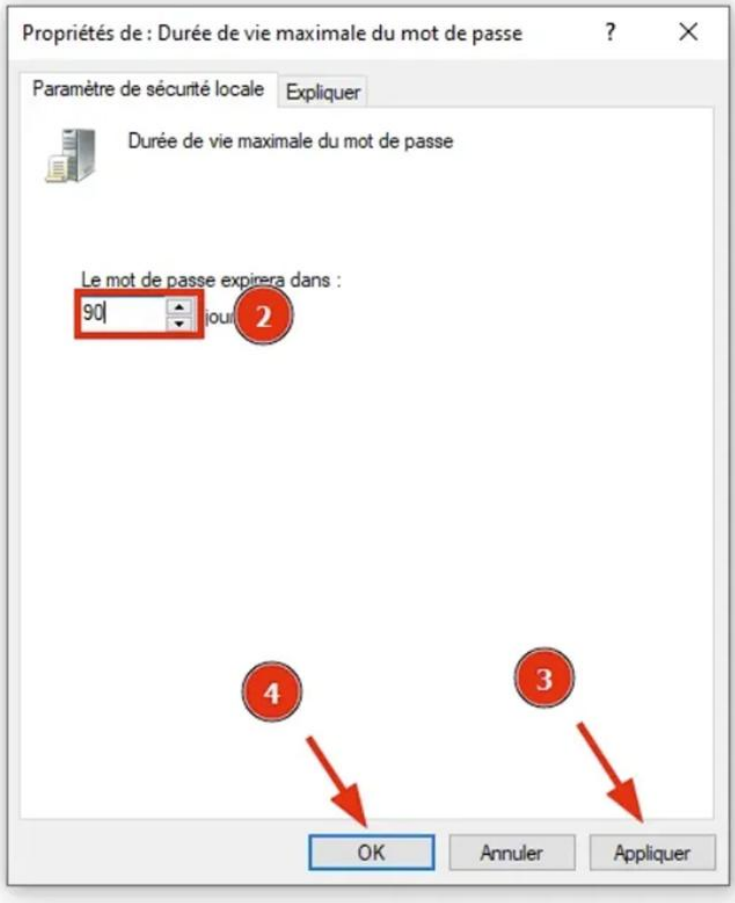
- **Le mot de passe doit respecter des exigences de complexité** *(1)* : activez l'exigence de complexité *(2)* puis faites **Appliquer** *(3)* et **OK** *(4)*.



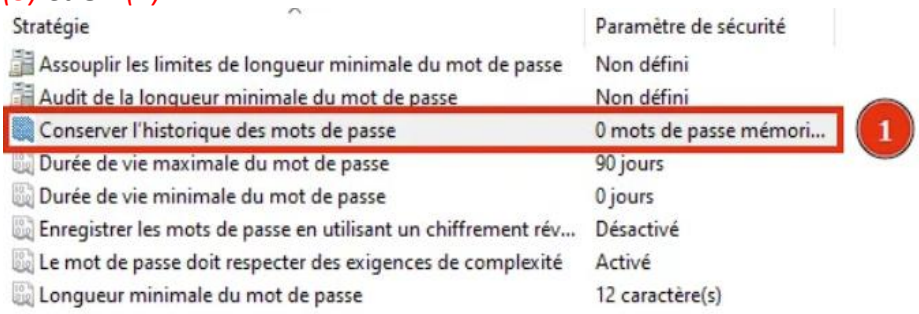


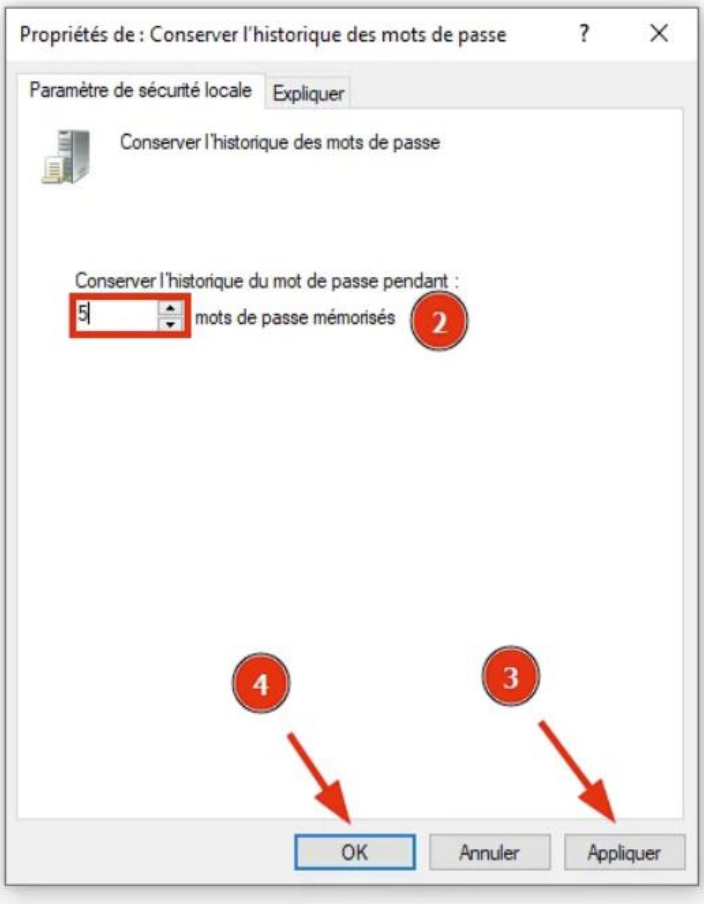
- **Durée de vie maximale du mot de passe** *(1)* : définissez à **90 jours** *(2)* puis faites **Appliquer** *(3)* et **OK** *(4)*.





- **Conserver l'historique des mots de passe** *(1)* : définissez à **5** *(2)* puis faites **Appliquer** *(3)* et **OK** *(4)*.





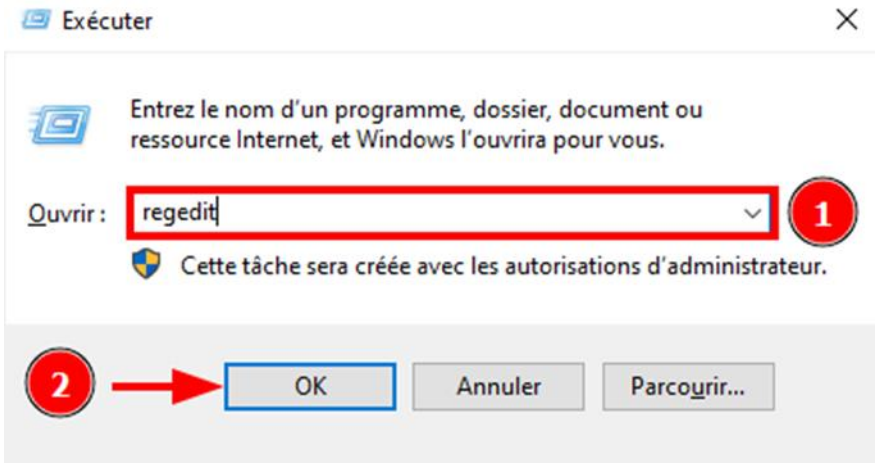
3. Tester la politique

- Changez un mot de passe utilisateur pour vérifier que les nouvelles règles s'appliquent.

4. Désactiver l'enregistrement des mots de passe en clair en mémoire

- Cette mesure protège les informations d'identification contre les attaques.

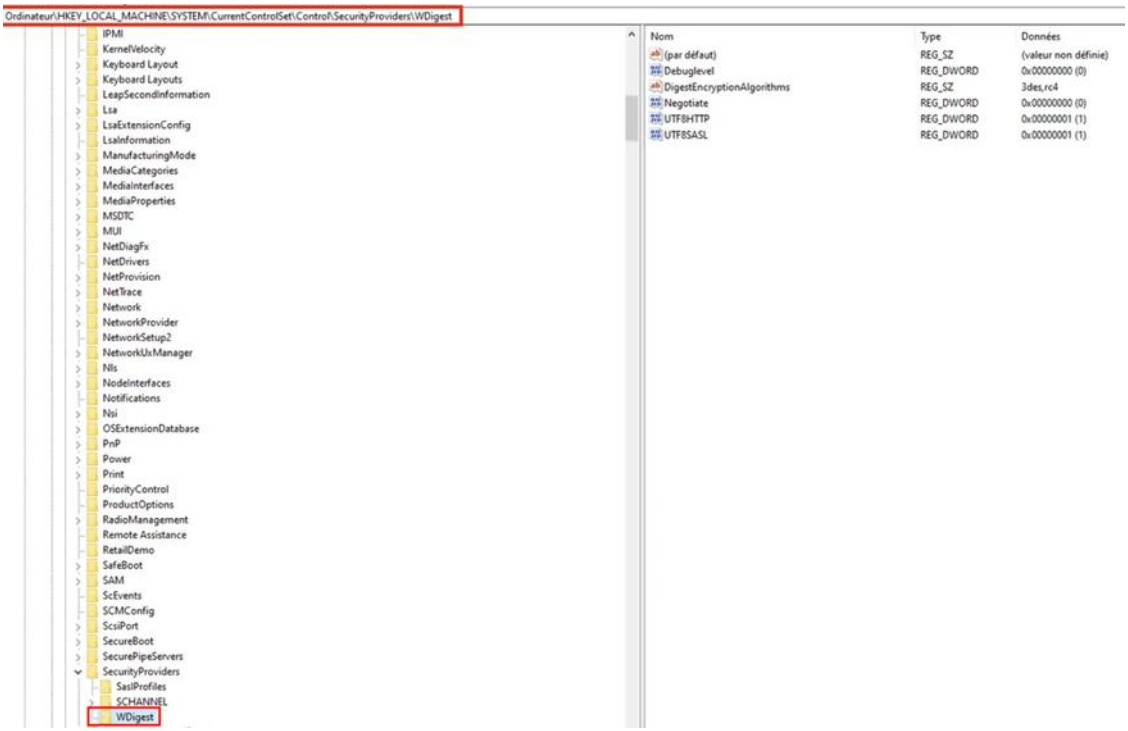
- Modifier le **Registre:**
  - Appuyez sur **Win + R**, tapez **regedit** *(1)*, puis appuyez sur **OK** *(2)*.



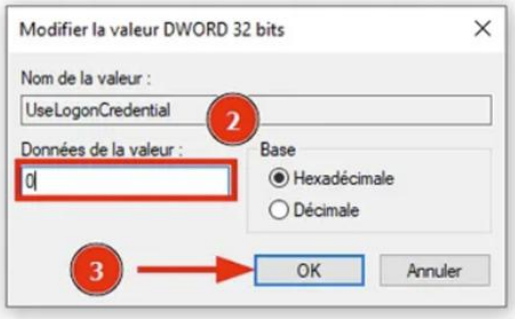
- Naviguez vers la clé suivante :
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest`

- Si la clé **WDigest** n'existe pas, créez-la.

DOCUMENTATION D'EXPLOITATION



- Créez une nouvelle valeur DWORD (32 bits) nommée **UseLogonCredential** *(1)*.
- Double-cliquez dessus et définissez la valeur à **0** *(2)* **et** faites **OK** *(3)*.

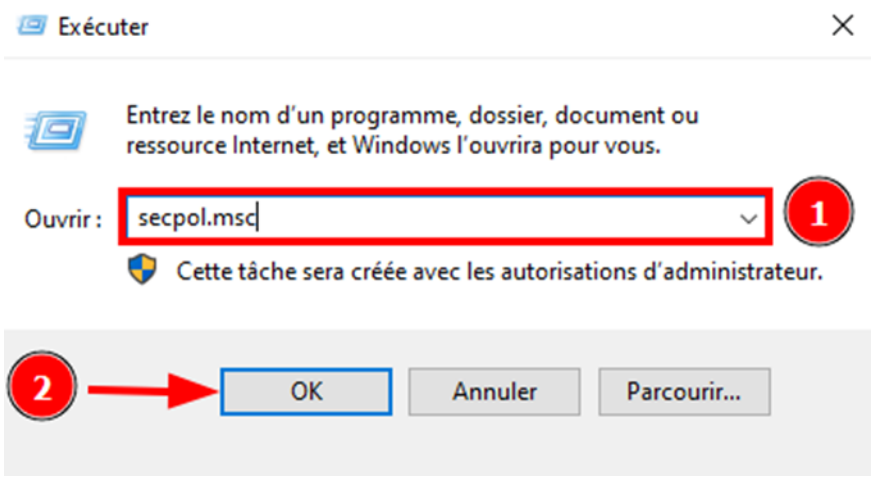


- Les modifications seront appliquées après le **redémarrage**.

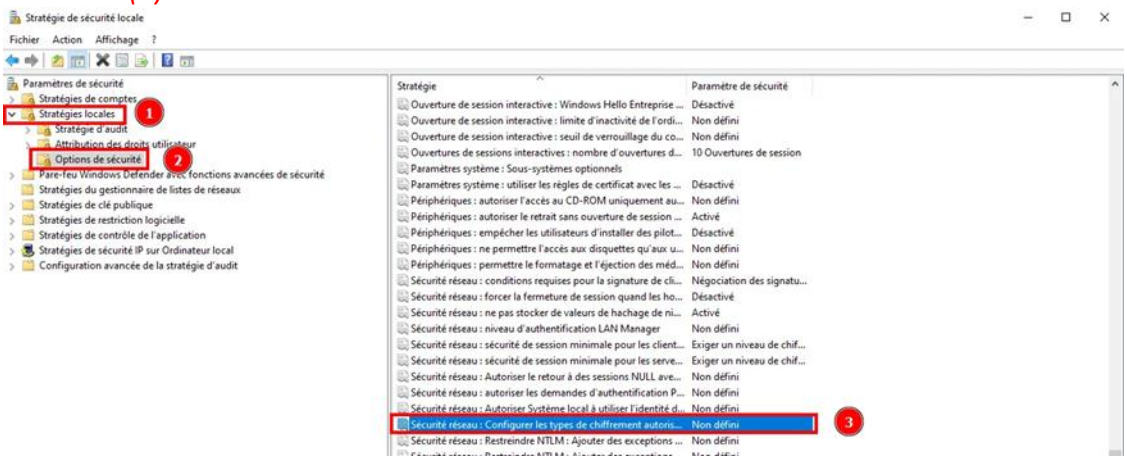
5. Restreindre les types de chiffrement Kerberos

- Cela renforce les communications sécurisées dans le cadre de l'authentification réseau.

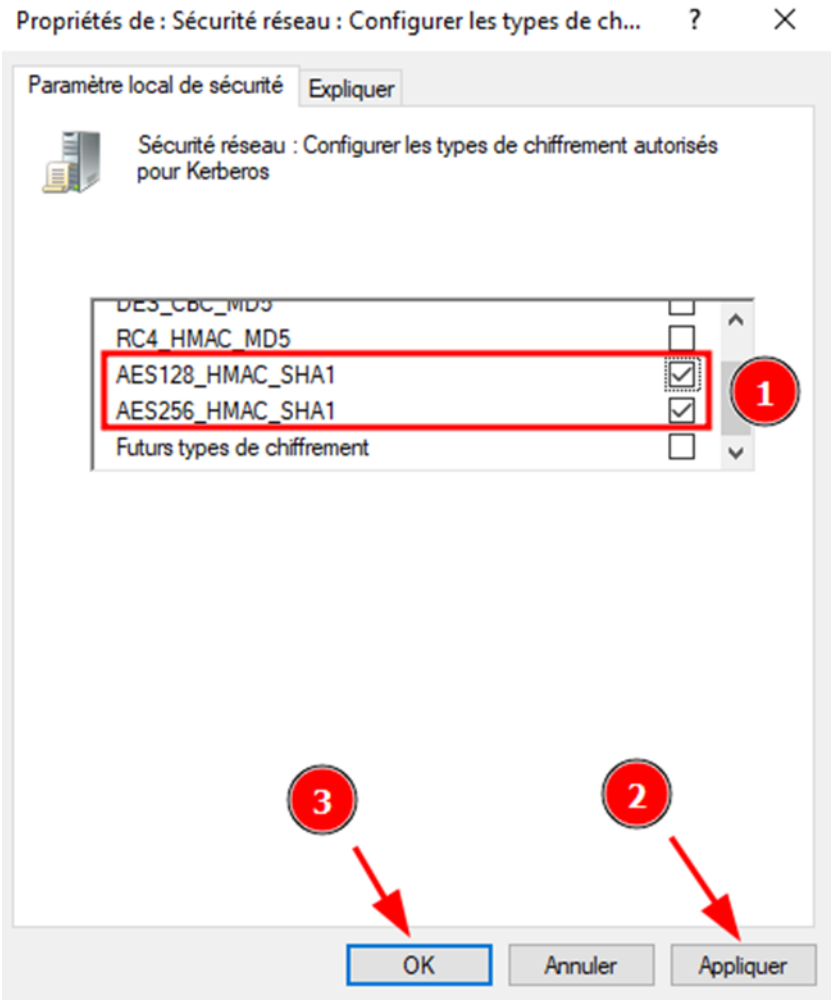
- Configurer via la **stratégie de sécurité locale:**
  - Ouvrez **secpol.msc** *(1)* puis faites **OK** *(2)*.



- Accédez à → **Stratégies locales** *(1)* → **Options de sécurité** *(2)*.
- Localisez **Sécurité réseau : Configurer les types de chiffrement autorisés pour Kerberos** *(3)*.



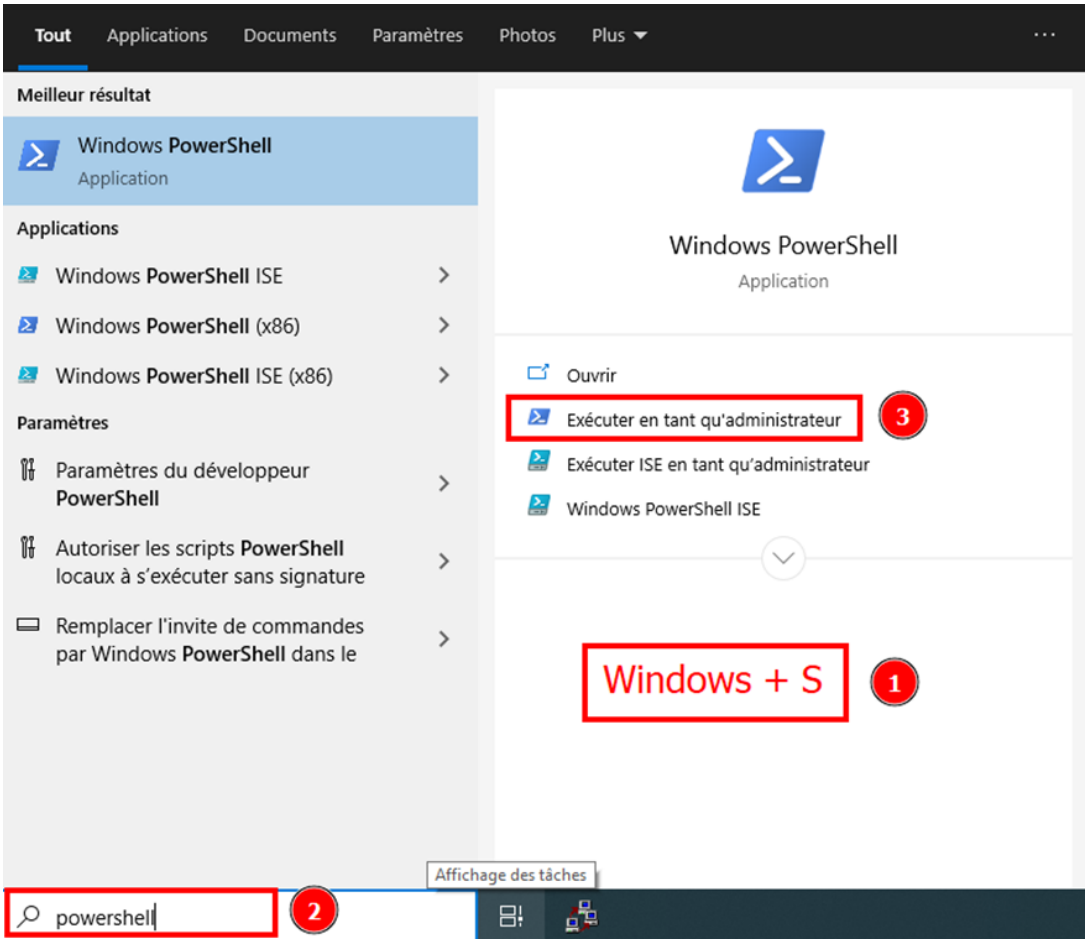
- Activez uniquement les types suivants :
  - **AES128_HMAC_SHA1** et **AES256_HMAC_SHA1** *(1)* puis faites **Appliquer** *(2)* et **OK** *(3)*.



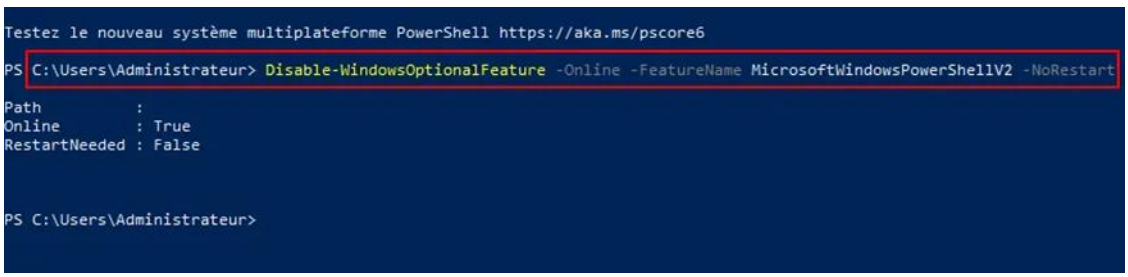
6. Désactiver PowerShell V2

- **PowerShell V2** est obsolète et contient des vulnérabilités.

- Désactiver via **PowerShell:**
  - Faites **Windows + S** *(1)*, puis ouvrez une fenêtre **PowerShell** *(2)* en mode **Administrateur** *(3)*.



- Exécutez la commande suivante :
  - `Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2 -NoRestart`

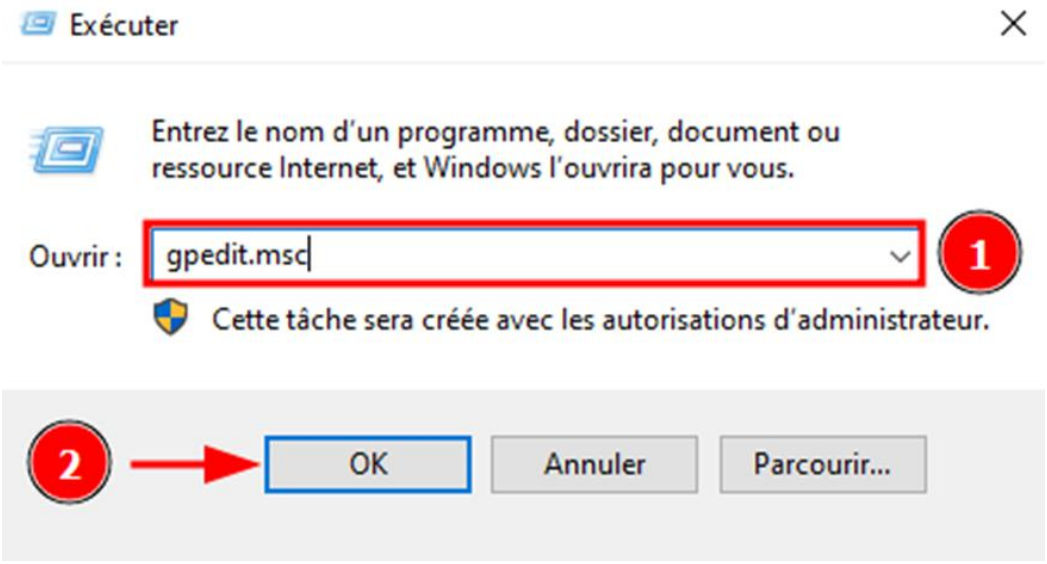


- Redémarrez pour finaliser la désactivation.

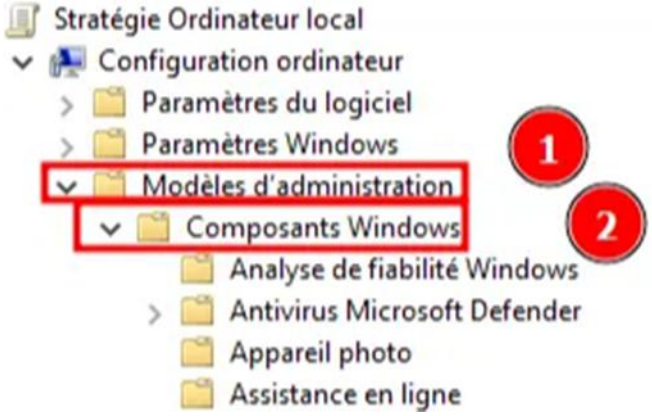
7. Désactiver AutoRun

- AutoRun peut être exploité pour exécuter automatiquement des logiciels malveillants à partir de supports externes.

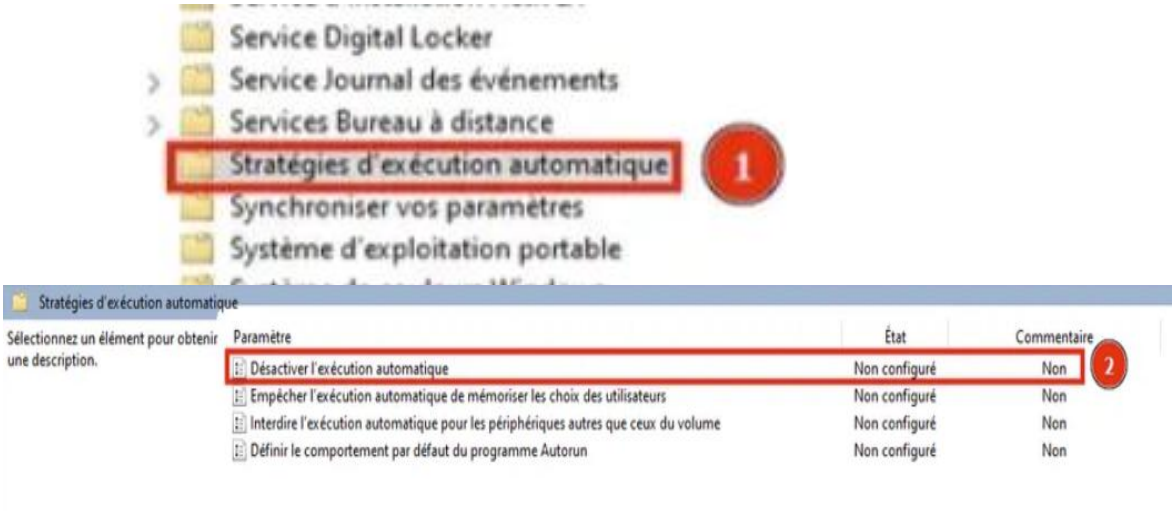
- Modifier les paramètres **AutoRun :**
    - Appuyez sur **Win + R**, tapez **gpedit.msc** *(1)*, puis appuyez sur **OK** *(2)*.



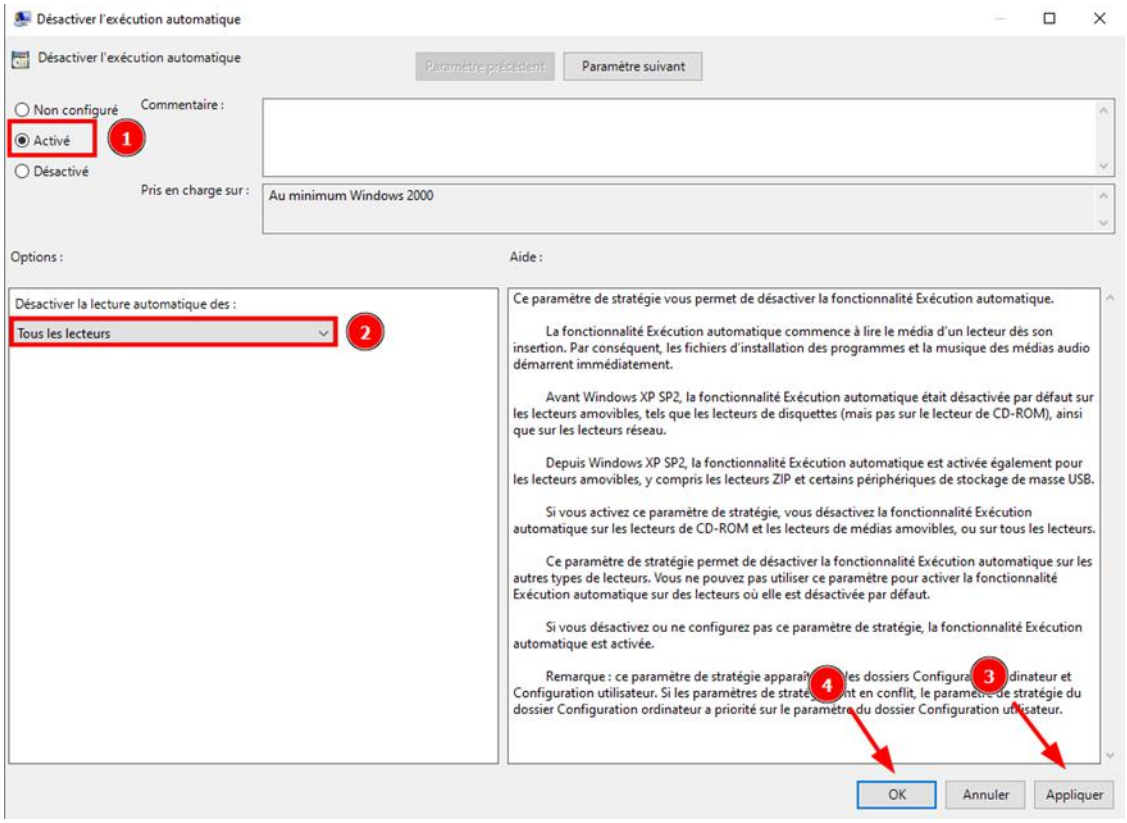
- Naviguez vers → **Modèles d'administration** *(1)* → **Composants Windows** *(2)*.



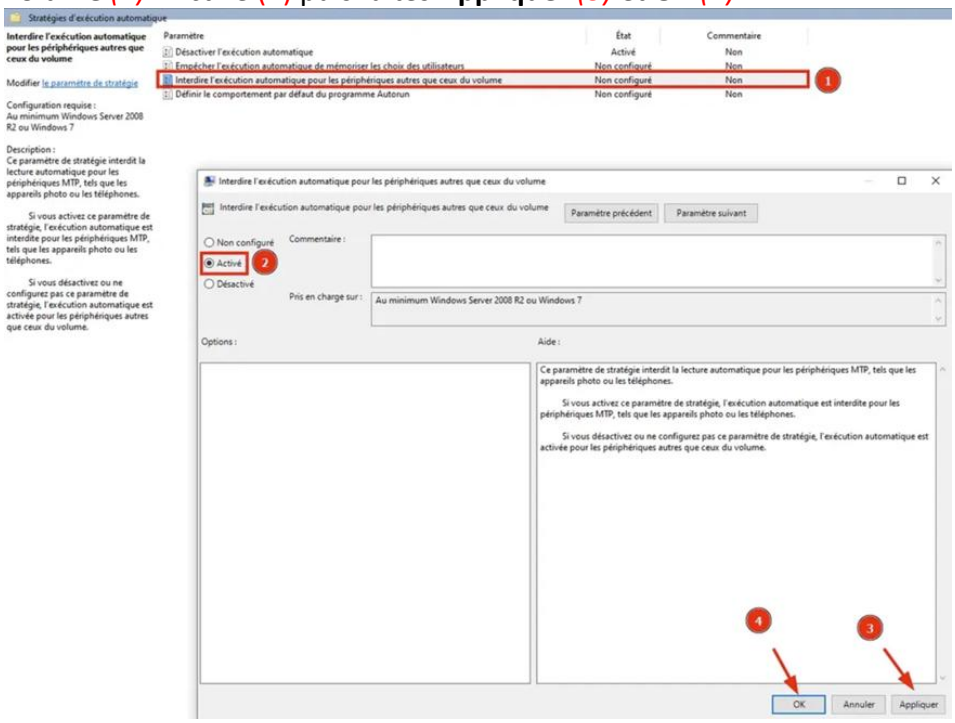
- Puis vers → **Stratégies d'exécution automatique** *(1)* puis double-cliquez sur **Désactiver l'exécution automatique** *(2)*.



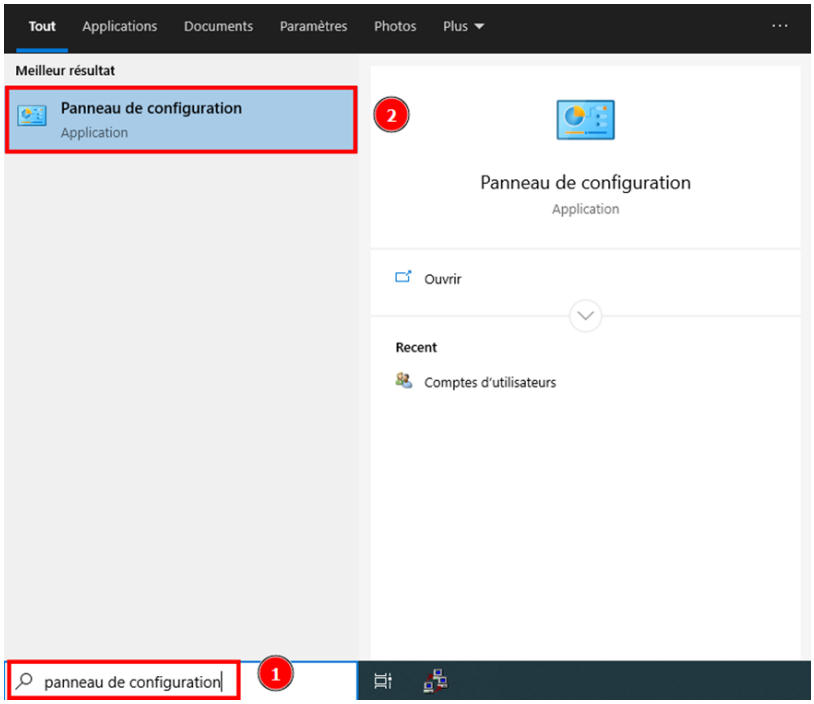
- Activez la politique suivante :
    - **Désactiver l'exécution automatique :** Activé (1) sur **Tous les lecteurs** *(2)* puis faites **Appliquer** *(3)* et **OK** *(4)*.



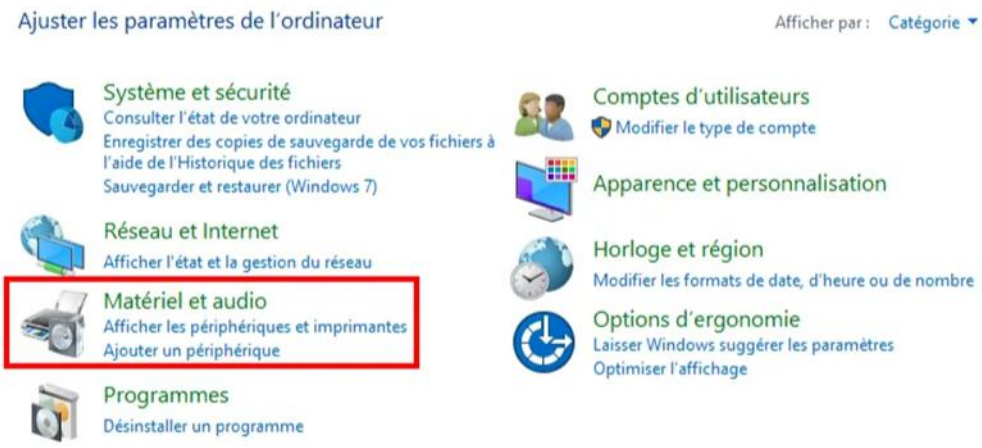
- Activez la politique suivante :
  - **Interdire l'exécution automatique pour les périphériques autres que ceux du volume** *(1)* **:** Activé (2) puis faites **Appliquer** *(3)* et **OK** *(4)*.



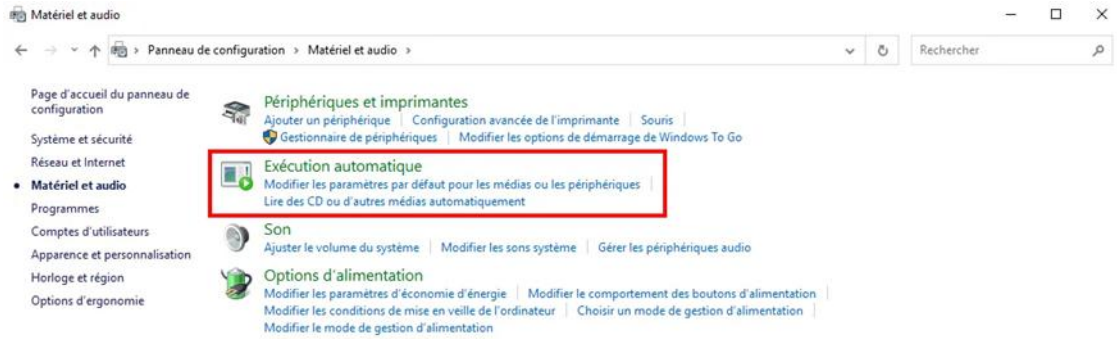
- Vérifier via le **Panneau de configuration :**
  - Allez dans → **Panneau de configuration** *(1,2)*.



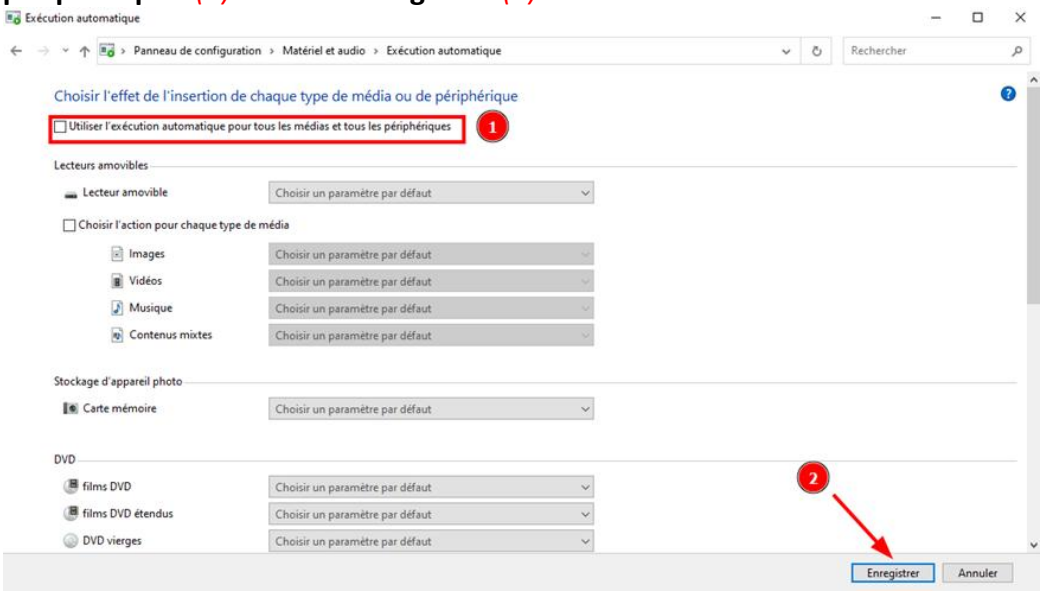
- Allez dans → **Matériel et audio.**



- Allez dans → **Exécution automatique.**



- Décochez **Utiliser l'exécution automatique pour tous les médias et tous les périphériques** *(1)* et faites **Enregistrer** *(2)*.



8. Pourquoi ces étapes sont importantes ?

- **Mots de passe:** Des mots de passe complexes et bien gérés réduisent les risques d'accès non autorisé.
- **Authentification:** Les protocoles sécurisés (Kerberos AES, désactivation des mots de passe en clair) minimisent les vulnérabilités dans les environnements réseau.
- **AutoRun:** Bloquer AutoRun protège contre les logiciels malveillants transportés sur des périphériques externes.

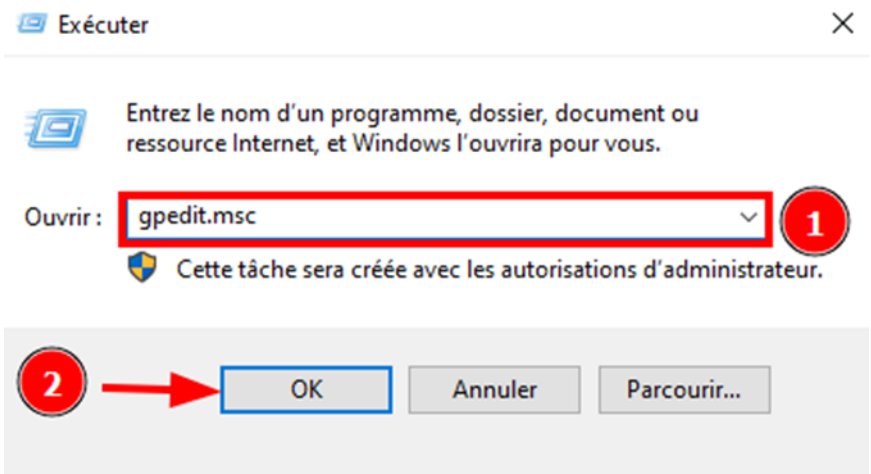
3. Protection réseau

1. Introduction

- Dans cette étape, nous allons renforcer la sécurité réseau en activant des signatures de protocole, en configurant des paramètres de sécurité pour les membres du domaine local, et en activant SmartScreen pour protéger les utilisateurs contre les sites malveillants.

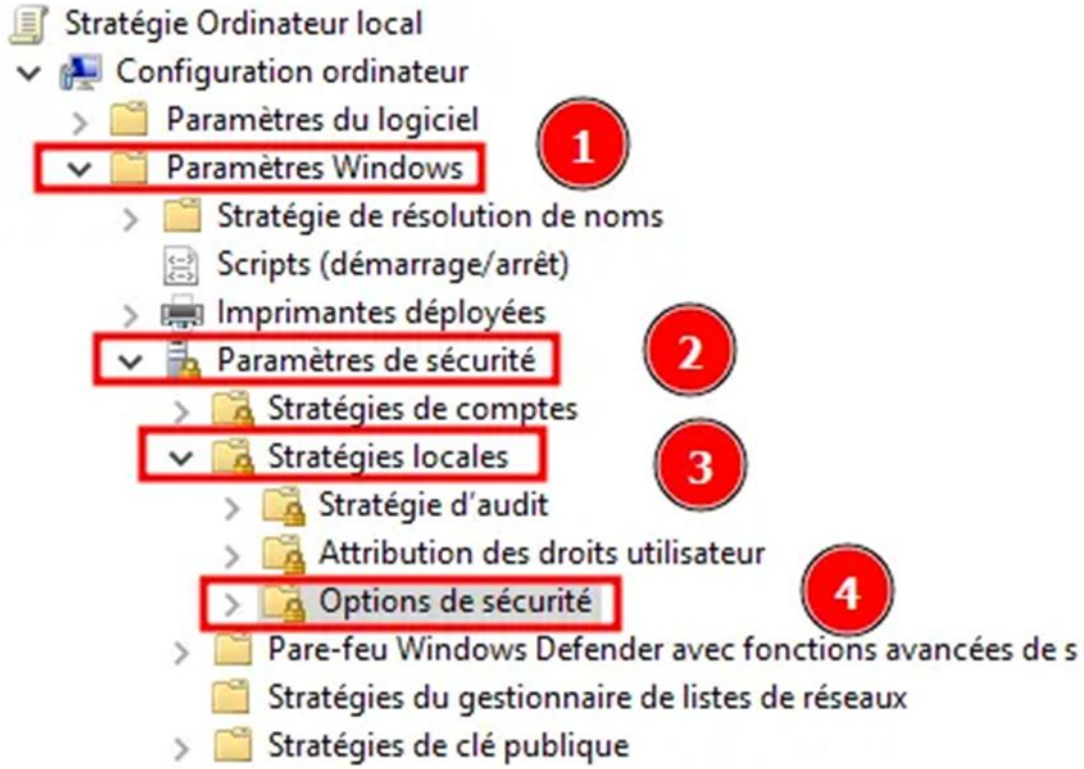
2. Activer les signatures SMB/LDAP

- Configurer les signatures **SMB:**
  - Appuyez sur **Win + R**, tapez **gpedit.msc** *(1)*, et appuyez sur **OK** *(2)*.

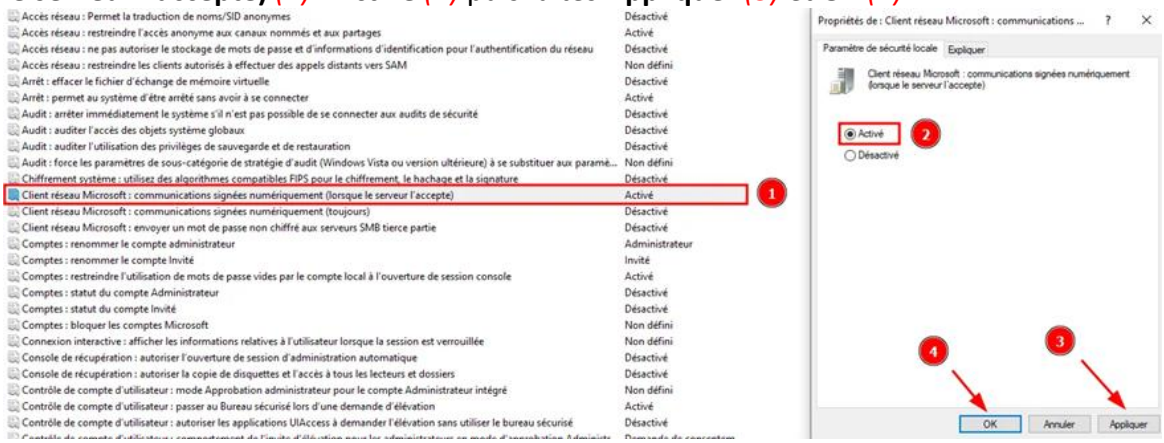


DOCUMENTATION D'EXPLOITATION

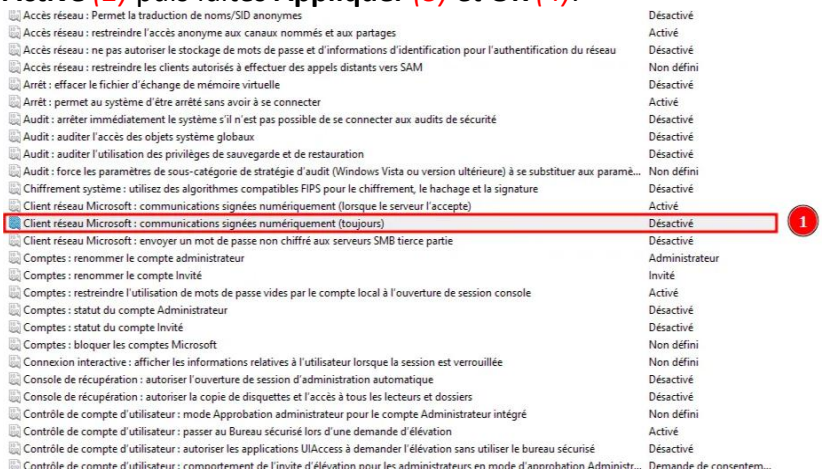
- Accédez à → **Paramètres Windows** *(1)* → **Paramètres de sécurité** *(2)* → **Stratégies locales** *(3)* → **Options de sécurité** *(4)*.



- Modifiez les paramètres suivants :
  - **Client réseau Microsoft : communications signées numériquement (lorsque le serveur l'accepte)** *(1)* : **Activé** *(2)* puis faites **Appliquer** *(3)* et **OK** *(4)*.



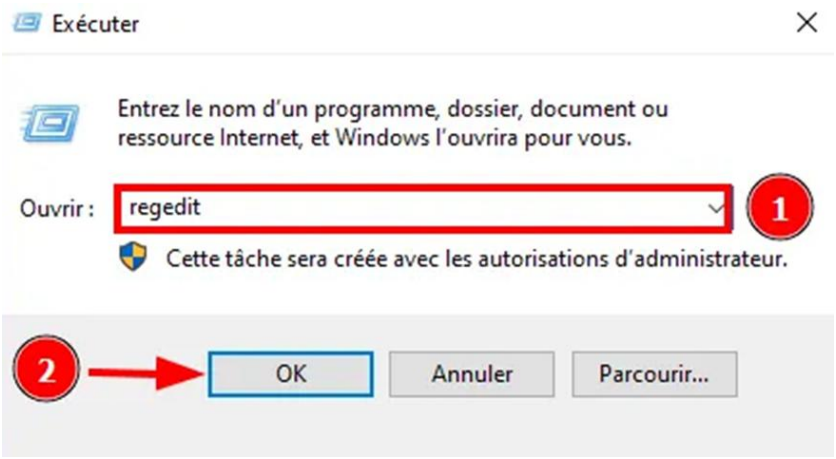
- **Client réseau Microsoft : communications signées numériquement (toujours)** *(1)* : **Activé** *(2)* puis faites **Appliquer** *(3)* et **OK** *(4)*.



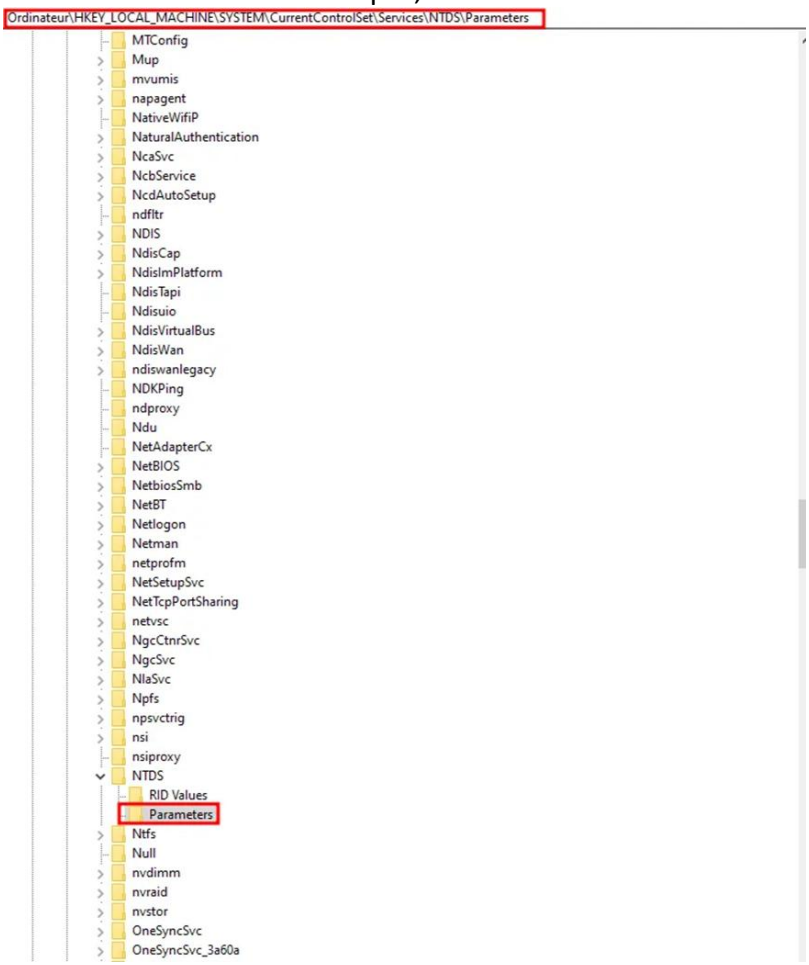
- **Client réseau Microsoft : envoyer un mot de passe non chiffré aux serveurs SMB tierce partie** *(1)* : **Désactivé** *(2)* puis faites **Appliquer** *(3)* et **OK** *(4)*.

3. Configurer les signatures LDAP

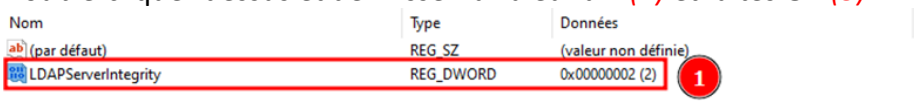
- Modifier le **Registre:**
  - Appuyez sur **Win + R**, tapez **regedit** *(1)*, puis appuyez sur **OK** *(2)*.

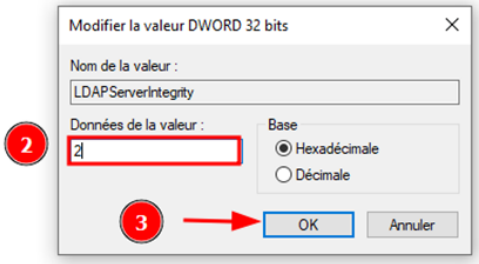


- Naviguez vers la clé suivante :
    - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters`
- Si la clé **Parameters** n'existe pas, créez-la.



- Créez une nouvelle valeur DWORD (32 bits) nommée **LDAPServerIntegrity** *(1)*.
- Double-cliquez dessus et définissez la valeur à **2** *(2)* et faites **OK** *(3)*.



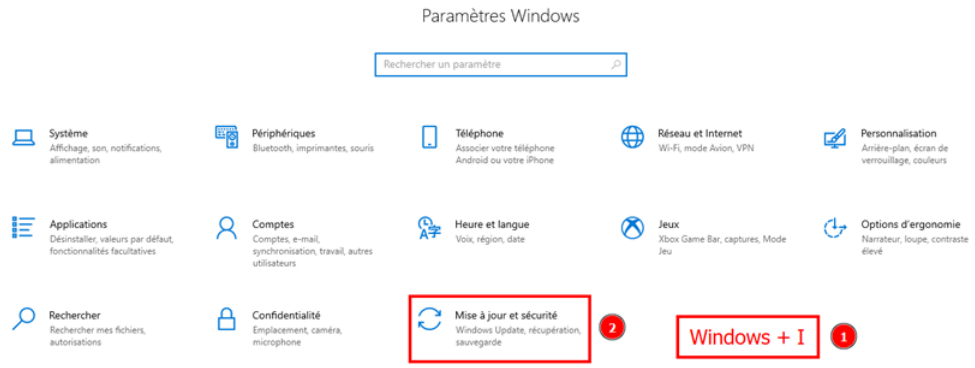


- Les modifications seront appliquées après le redémarrage.

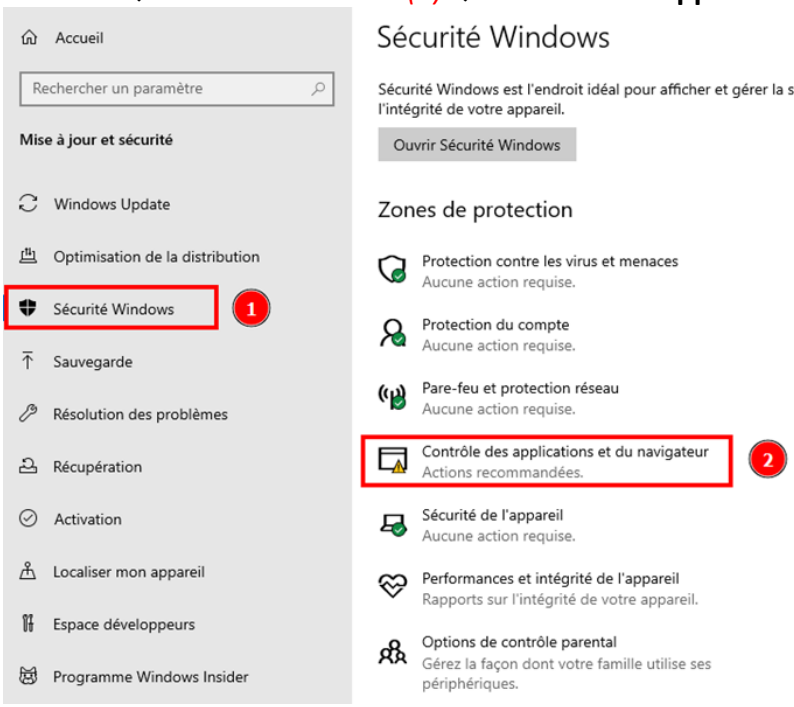
4. Activer SmartScreen

- SmartScreen aide à identifier et bloquer les sites Web ou fichiers malveillants.

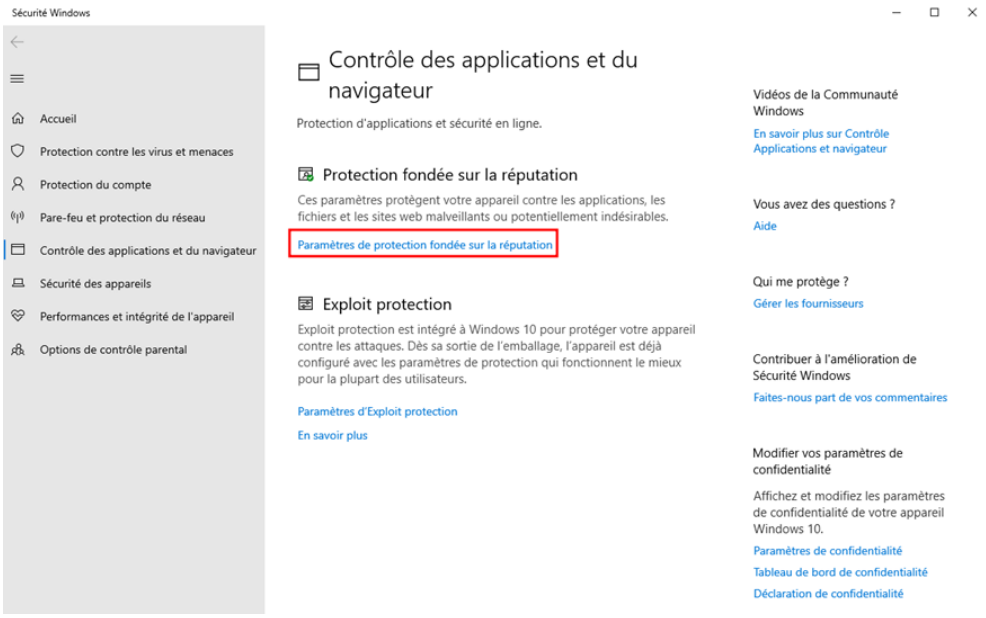
- Configurer SmartScreen via les **paramètres:**
  - Ouvrez **Paramètres Windows** (Win + I) *(1)*.
  - Naviguez vers → **Mise à jour et sécurité** *(2)*.



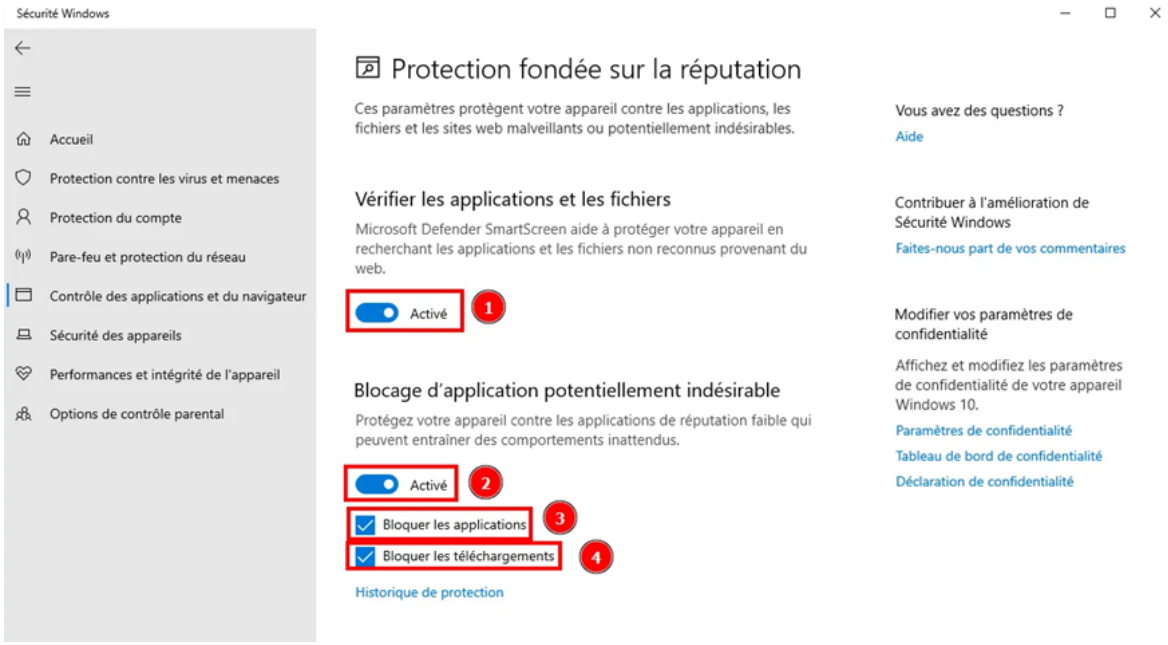
- Puis vers → **Sécurité Windows** *(1)* → **Contrôle des applications et du navigateur** *(2)*.



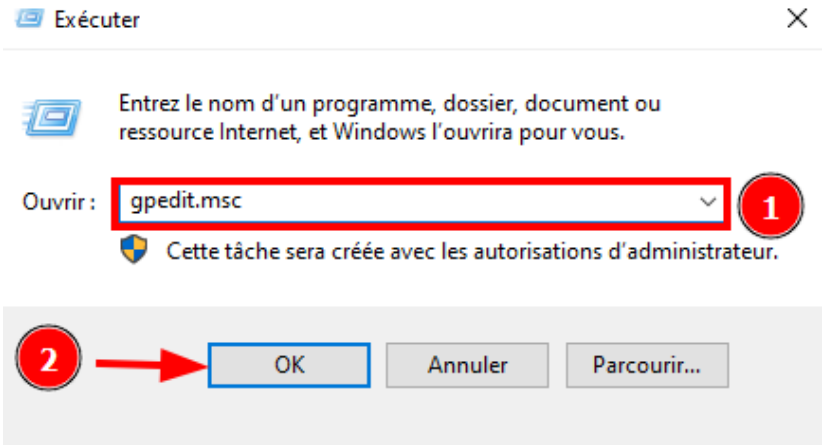
- Enfin dans **Paramètres de protection fondée sur la réputation**.



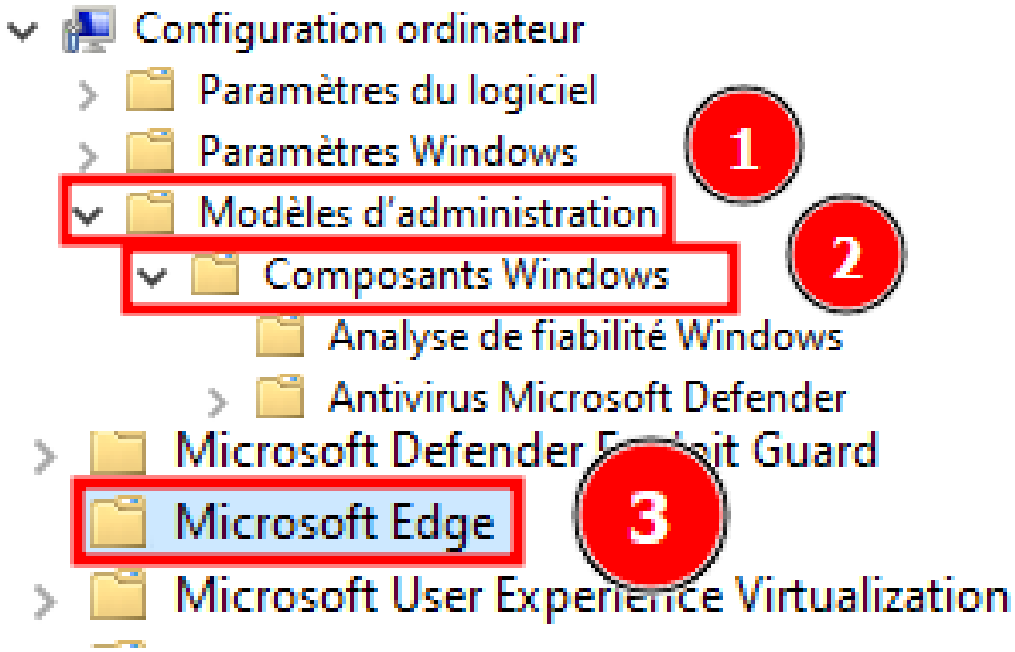
- Sous **SmartScreen**, activez les options suivantes :
  - **Vérifier les applications et les fichiers** : **Activé** *(1)*.
  - **Blocage d'application potentiellement indésirable** : **Activé** *(2)*.
  - **Bloquer les applications** : **Activé** *(3)*.
  - **Bloquer les téléchargements** : **Activé** *(4)*.



- Appuyez sur **Win + R**, tapez **gpedit.msc** *(1)*, et appuyez sur **OK** *(2)*.



- Allez dans **Modèles d'administration** *(1)* → **Composants Windows** *(2)* → **Microsoft Edge** *(3)*.



- Puis activez les stratégies suivantes :
    - Empêcher le contournement des avertissements de Windows Defender SmartScreen pour les sites : **Activé**.
    - Empêcher le contournement des avertissements de Windows Defender SmartScreen pour les fichiers : **Activé**.
    - Configurer Windows Defender SmartScreen : **Activé**.
    - Autoriser les extensions : **Désactivé**.

5. Vérification de la configuration

- Téléchargez un fichier test EICAR depuis un navigateur pris en charge (https://www.eicar.org). SmartScreen devrait bloquer le téléchargement.

6. Pourquoi ces étapes sont importantes ?

- **Signatures SMB/LDAP:** Garantissent l'intégrité des données échangées sur le réseau, réduisant le risque de man-in-the-middle.
- **SmartScreen:** Ajoute une couche de protection utilisateur contre les menaces en ligne et les fichiers infectés.

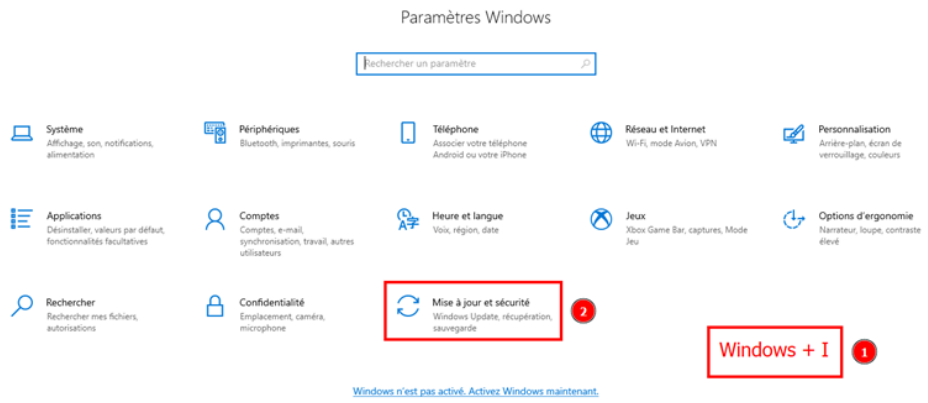
4. Configuration de Windows Defender

1. Introduction

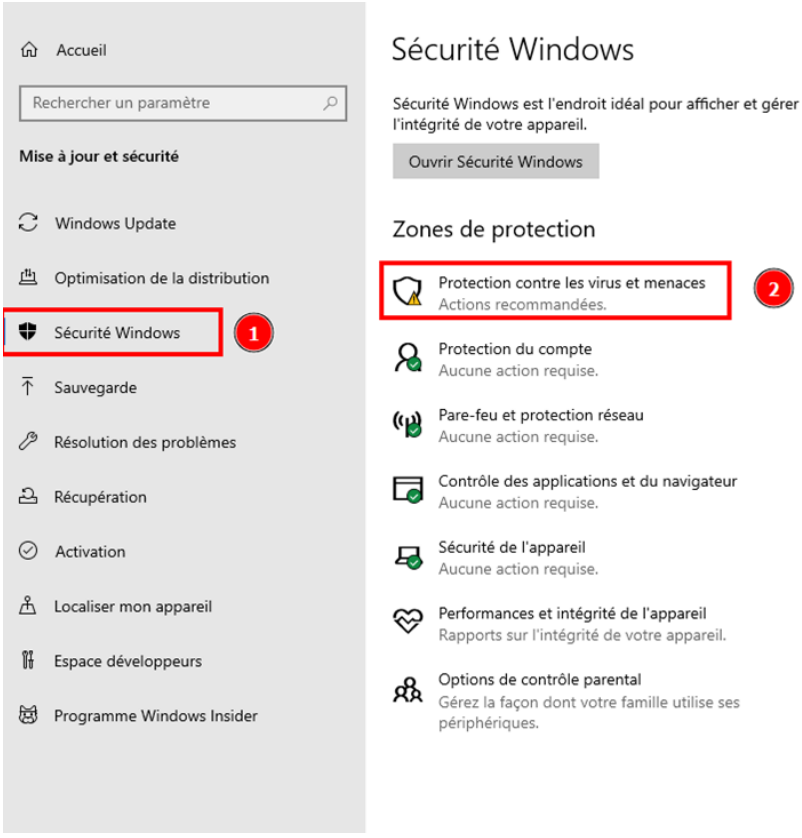
- Dans cette étape, nous allons configurer Windows Defender pour offrir une protection maximale contre les logiciels malveillants, les exploits, et autres menaces en ligne.

2. Activer les protections de base dans Windows Defender

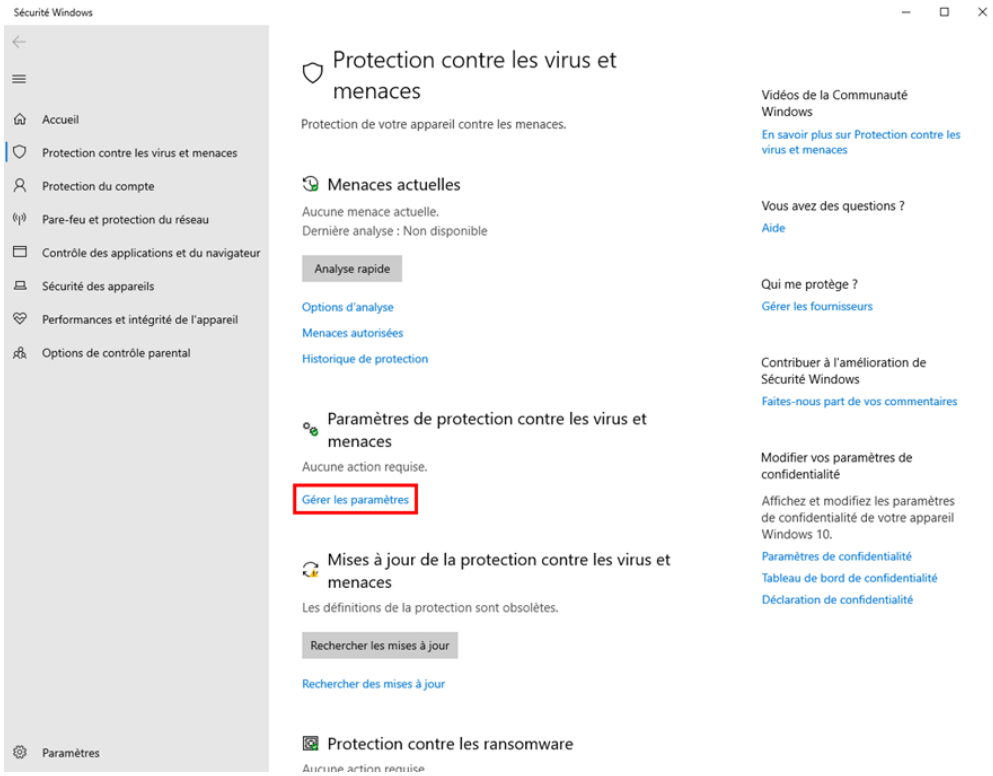
- Accéder aux paramètres de **Windows Defender:**
  - Appuyez sur **Win + I** *(1)* pour ouvrir les **Paramètres Windows**.
  - Naviguez vers **Mise à jour et sécurité** *(2)*.



- Puis vers → **Sécurité Windows** *(1)* → **Protection contre les virus et menaces** *(2)*.



- **Activer les protections :**
  - Cliquez sur **Gérer les paramètres** sous **Paramètres de protection contre les virus et menaces**.



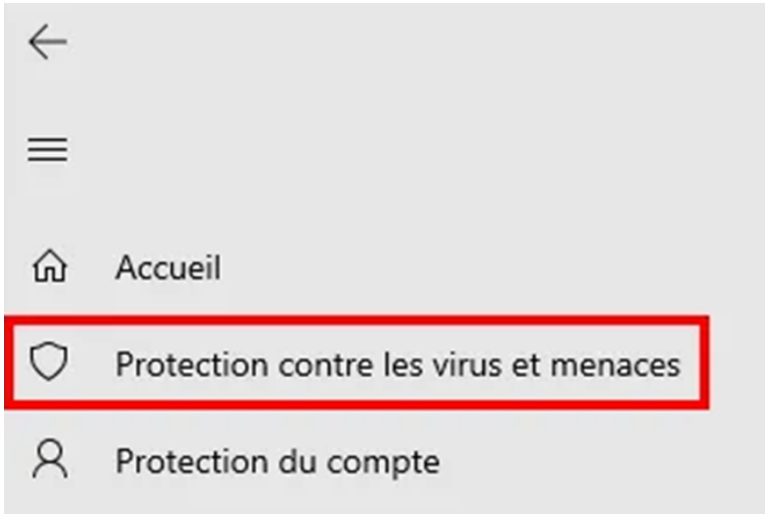
- Vérifiez que les options suivantes sont activées :
  - Protection en temps réel : **Activé** *(1)*.
  - Protection dans le cloud : **Activé** *(2)*.
  - Envoi automatique d'un échantillons : **Activé** *(3)*.
  - Protection contre les falsifications : **Activé** *(4)*.


Paramètres de protection contre les virus et menaces
Consultez et mettez à jour les paramètres de protection contre les virus et menaces de l'antivirus Microsoft Defender.
Protection en temps réel
Ce paramètre permet d'identifier et d'empêcher l'installation ou l'exécution de programmes malveillants sur votre appareil. Vous pouvez le désactiver temporairement, mais nous le réactiverons automatiquement.
Activé
1
Protection dans le cloud
Offre une protection renforcée et plus rapide grâce à l'accès aux données de protection les plus récentes dans le cloud. Fonctionne de manière optimale une fois la soumission automatique d'échantillons activée.
Activé
2
Envoi automatique d'un échantillon
Envoyez des échantillons de fichier à Microsoft pour vous protéger et protéger les autres utilisateurs contre d'éventuelles menaces. Nous vous informerons si le fichier dont nous avons besoin est susceptible de contenir des informations personnelles.
Activé
3
Envoyer un échantillon manuellement
Protection contre les falsifications
Empêche d'autres utilisateurs de falsifier des fonctionnalités de sécurité importantes.
Activé
4
En savoir plus

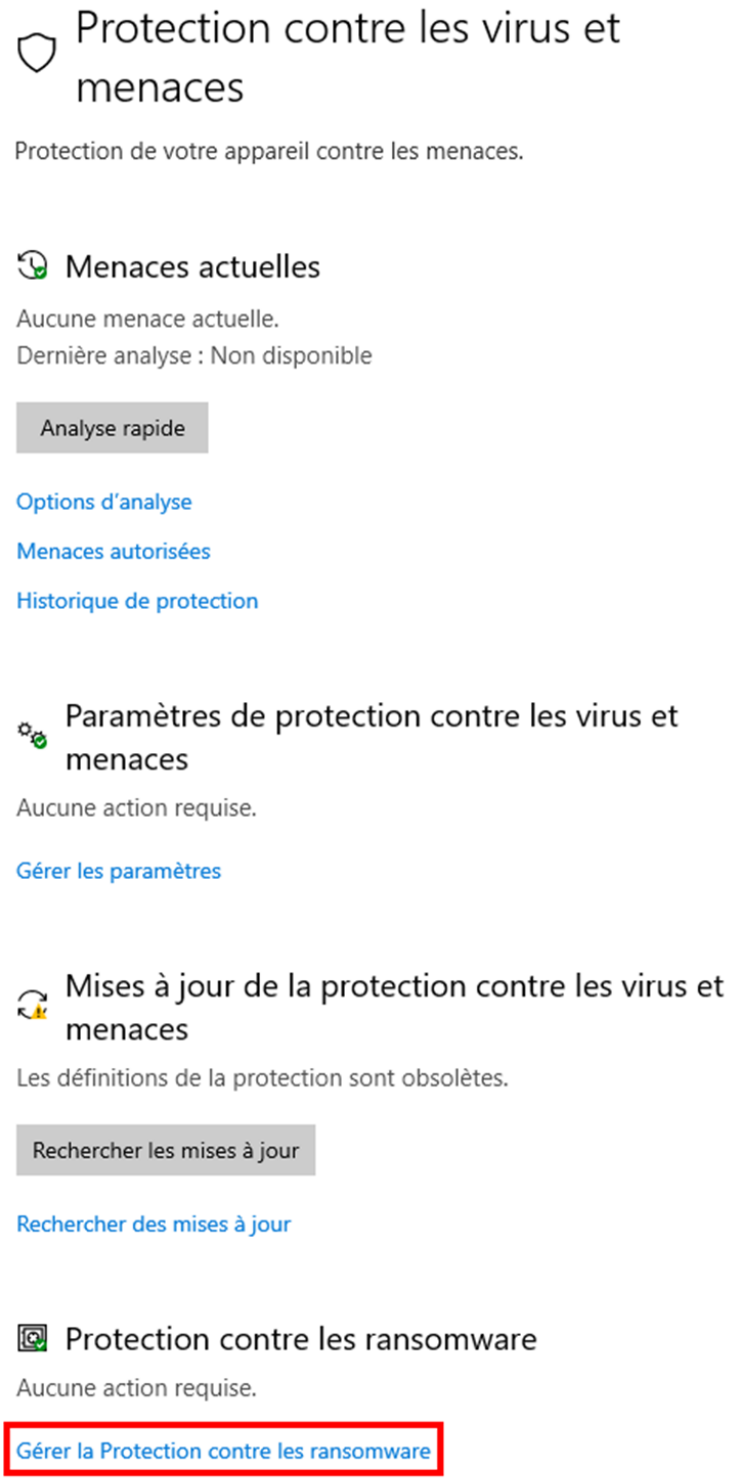
3. Configurer les protections avancées

- Ces paramètres permettent de renforcer la sécurité contre des menaces avancées.

- **Configurer l'accès contrôlé aux dossiers :**
  - Toujours dans **Protection contre les virus et menaces**.



- Sous **Protection contre les ransomwares**, cliquez sur **Gérez la Protection contre les ransomware**.

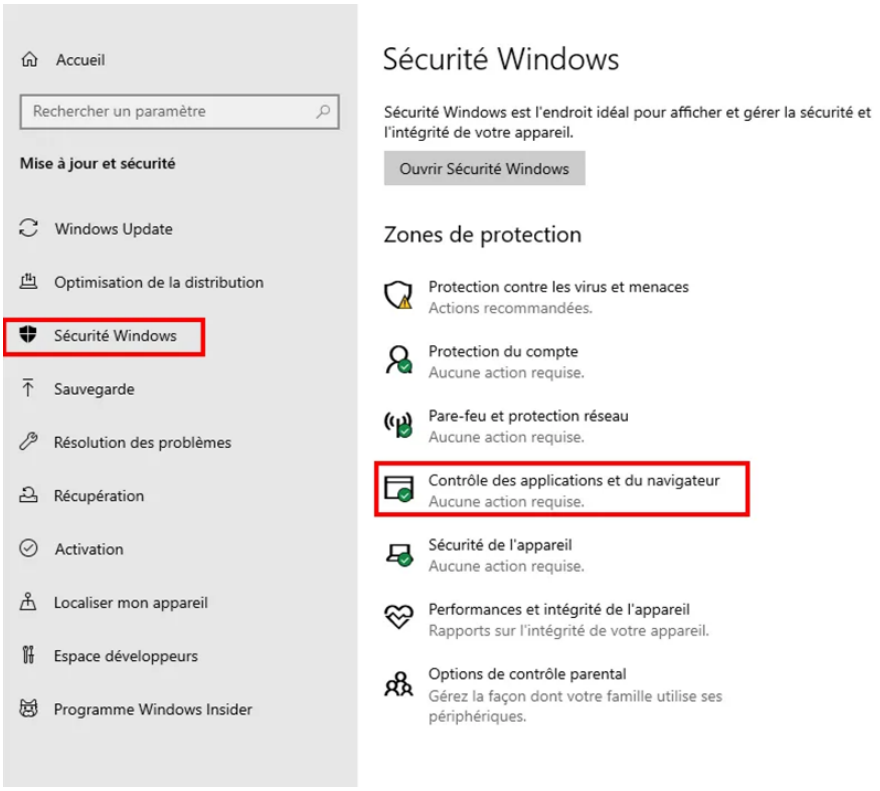

Protection contre les virus et menaces
Protection de votre appareil contre les menaces.
Menaces actuelles
Aucune menace actuelle.
Dernière analyse : Non disponible
Analyse rapide
Options d'analyse
Menaces autorisées
Historique de protection
Paramètres de protection contre les virus et menaces
Aucune action requise.
Gérer les paramètres
Mises à jour de la protection contre les virus et menaces
Les définitions de la protection sont obsolètes.
Rechercher les mises à jour
Rechercher des mises à jour
Protection contre les ransomware
Aucune action requise.
Gérer la Protection contre les ransomware

- Puis dans **Dispositif d'accès contrôlé aux dossiers : Activé.**

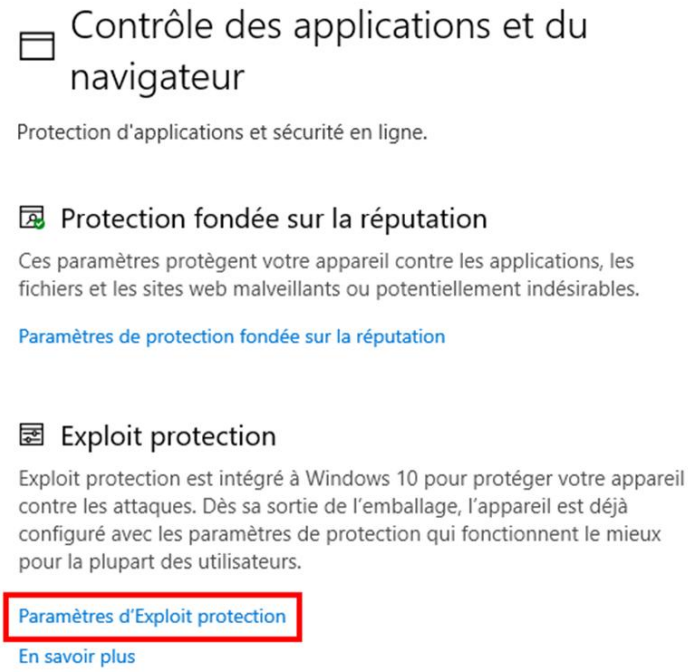
- (Ajoutez les applications autorisées si nécessaire en cliquant sur **Autoriser une application via l'accès contrôlé aux dossiers**.)

4. Activer la protection contre les exploits

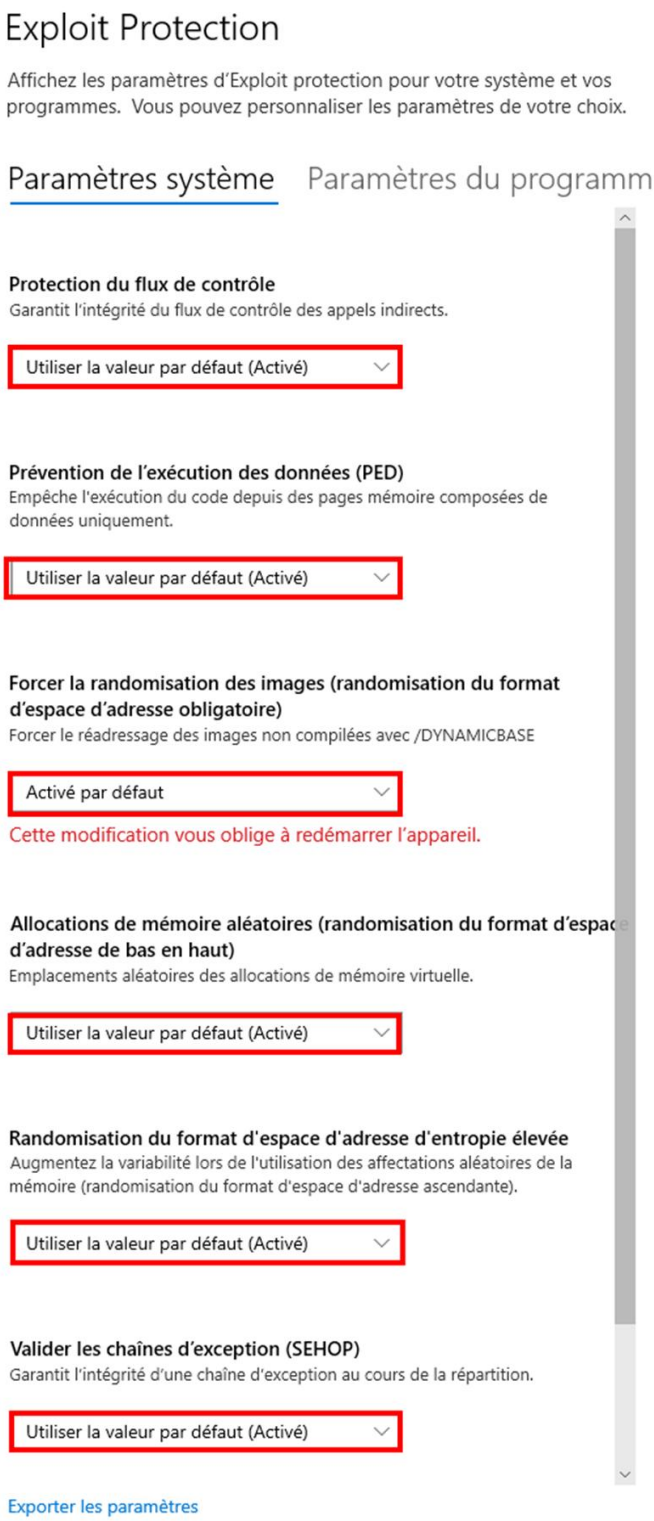
- Revenez à l'écran principal de **Sécurité Windows** et sélectionnez **Contrôle des applications et du navigateur**.

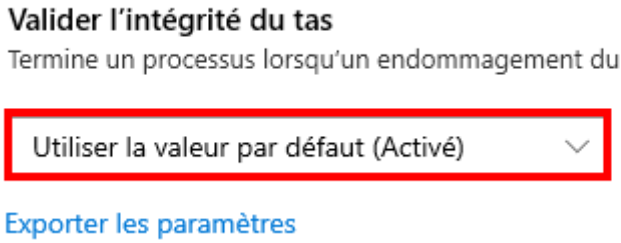


- Cliquez sur **Paramètres d'Exploit protection.**



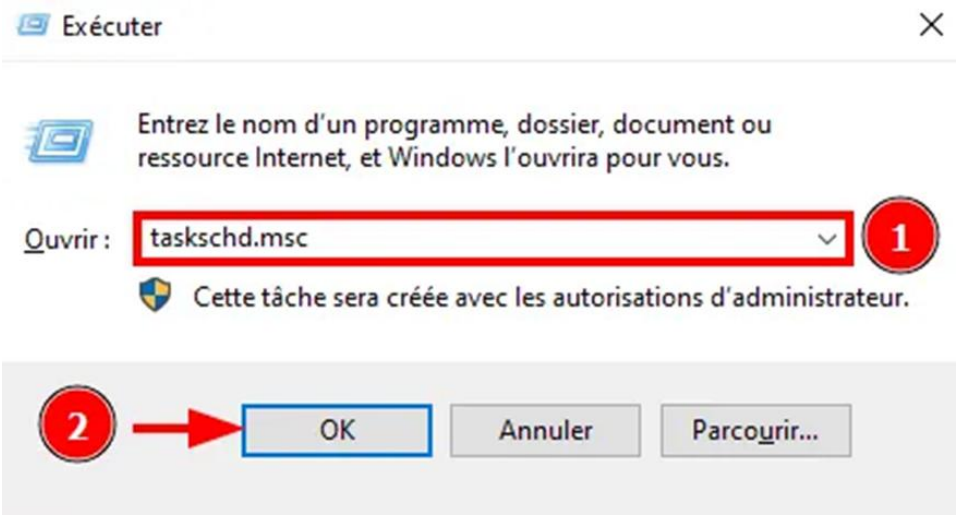
- Vérifiez que toutes les options sous la section **Paramètres système** soit activées par défaut.





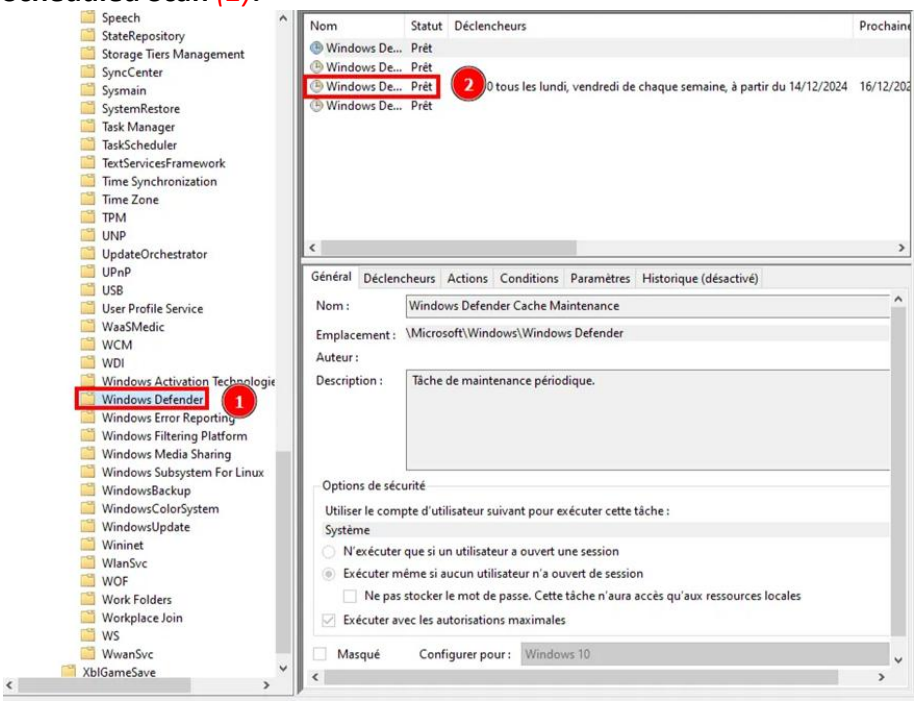
5. Configurer les options de vérification automatique

- Planification des analyses **Windows Defender:**
  - Appuyez sur **Win + R**, tapez **taskschd.msc** *(1)*, et appuyez sur **OK** *(2)* pour ouvrir le Planificateur de tâches.

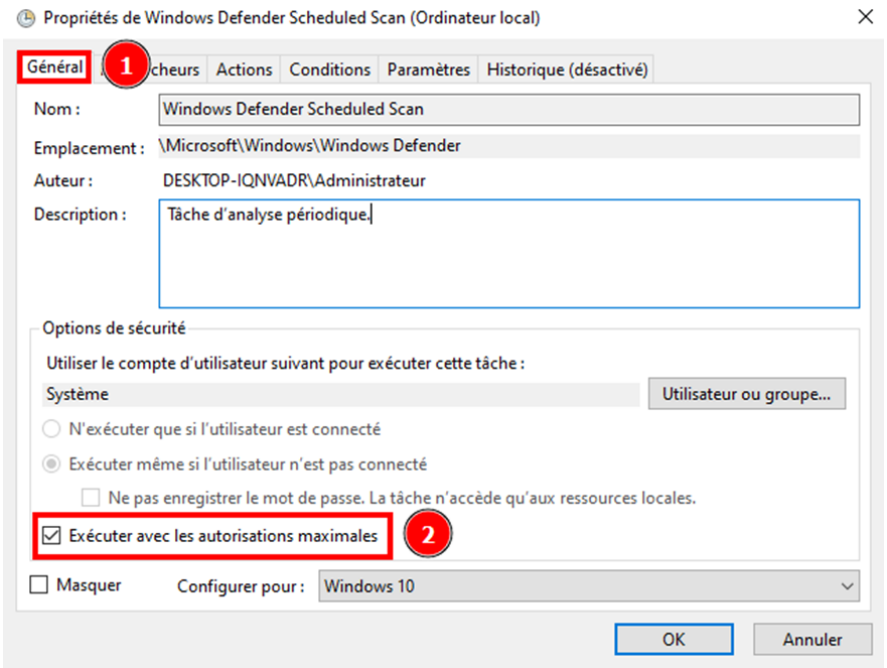


- Naviguez vers → **Bibliothèque du planificateur de tâches → Microsoft** *(1)* **→ Windows** *(2)***.**

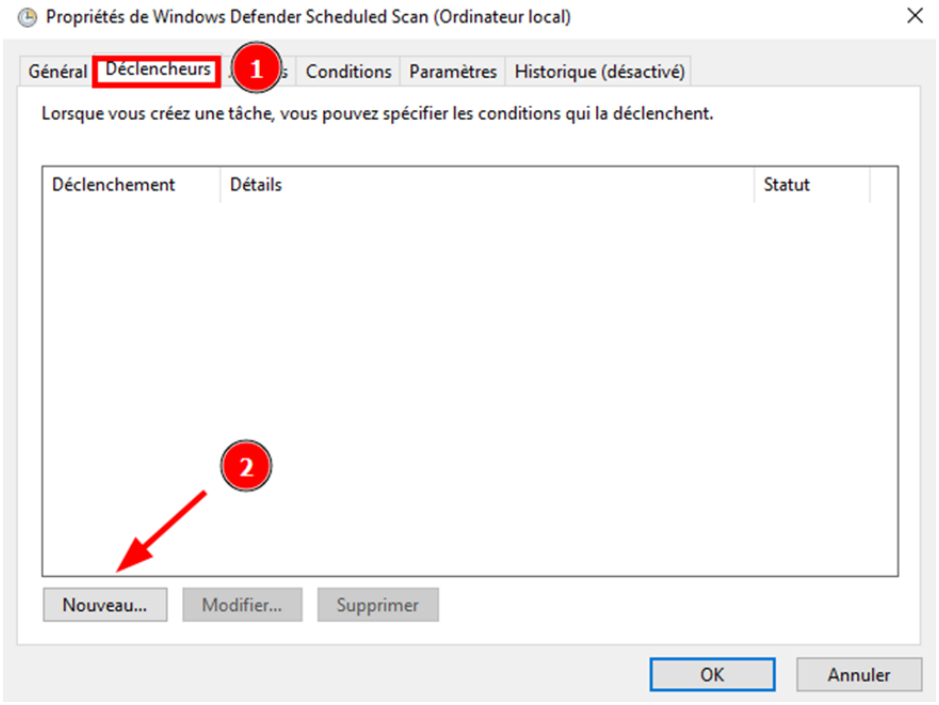
- Puis dans **Windows Defender** *(1)* → Double-cliquez sur **Windows Defender Scheduled Scan** *(2)*.



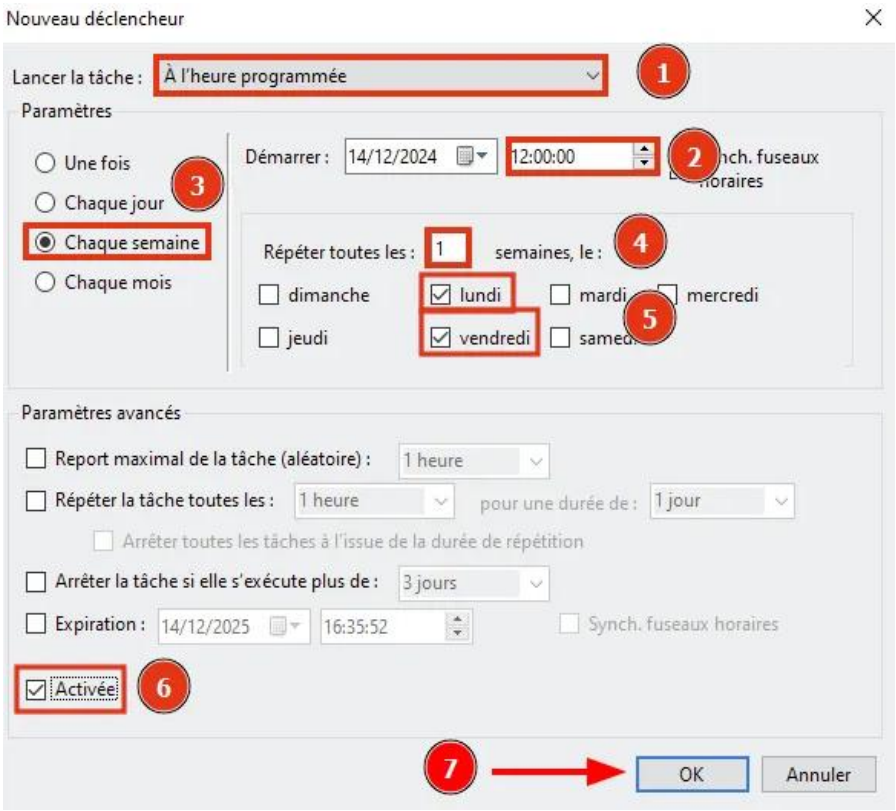
- Allez dans **Général** *(1)*, puis cochez la case **Exécuter avec les autorisations maximales** *(2)*.



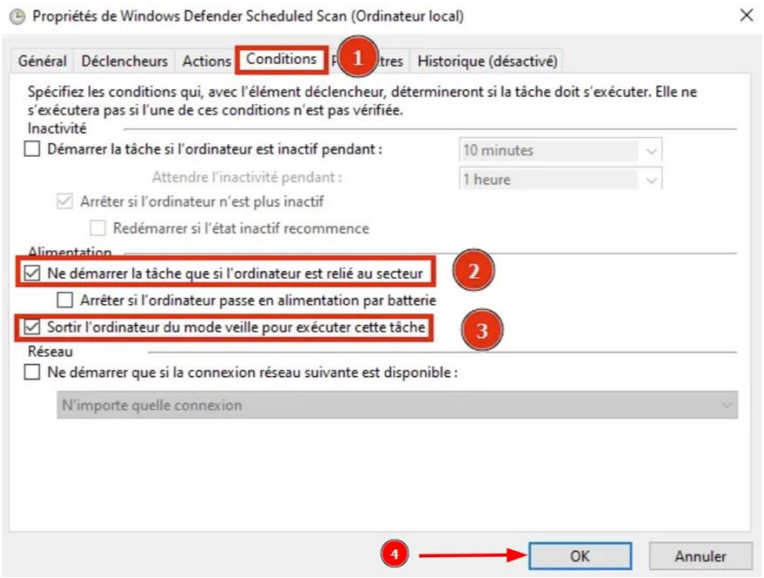
- Allez ensuite dans **Déclencheurs** *(1)*, puis cliquez sur **Nouveau…** *(2)*.



- Dans Nouveau déclencheur :
  - **Lancer la tâche : A l'heure programmée** *(1)*.
  - **Démarrer : 12:00:00** *(2)*.
  - **Pour l'intervalle : Chaque semaine** *(3)*.
  - **Répéter toutes les : 1** *(4)*.
  - **Pour les jours sélectionnez : lundi et vendredi** *(5)*.
  - **Cliquez tout en bas sur : Activée** *(6)*.
  - **Puis faite : OK** *(7)*.

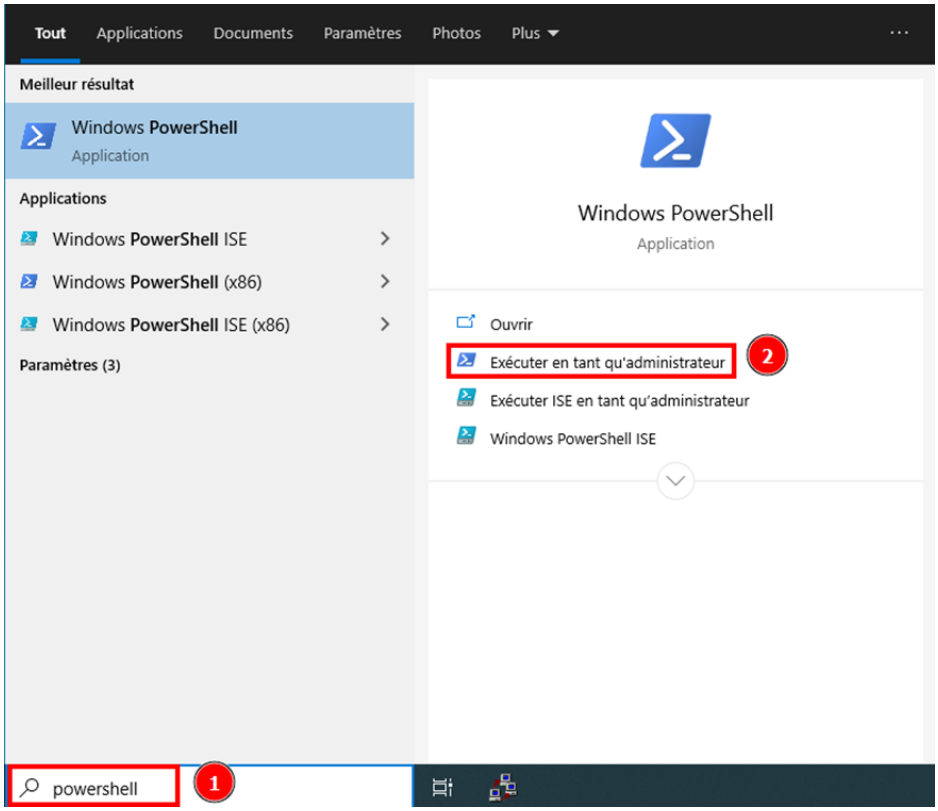


- Allez dans **Conditions** *(1)*, puis Activer:
  - **Ne démarrer la tâche que si l'ordinateur est relié au secteur** *(2)*.
  - **Sortir l'ordinateur du mode veille pour exécuter cette tâche** *(3)***.**
  - Puis cliquez sur : **OK** *(4)*.



6. Utiliser PowerShell pour valider les paramètres

- Exécuter un **diagnostic de configuration:**
  - Ouvrez **PowerShell** *(1)* en tant **qu'administrateur** *(2)*.



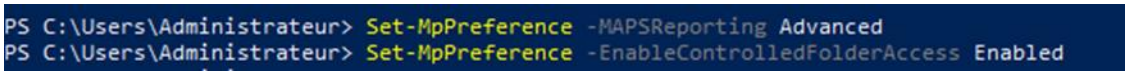
- Exécutez les commandes suivantes pour vérifier la configuration actuelle :
  - `Get-MpPreference`

```
PS C:\Users\Administrateur> Get-MpPreference
```

  - Cette commande affiche les paramètres actuels de Windows Defender.

7. Activer les paramètres avancés via PowerShell

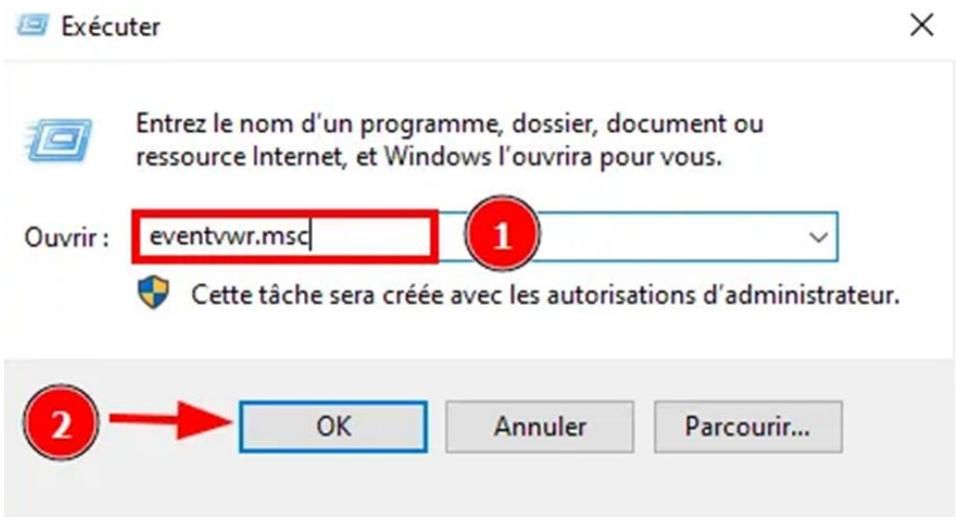
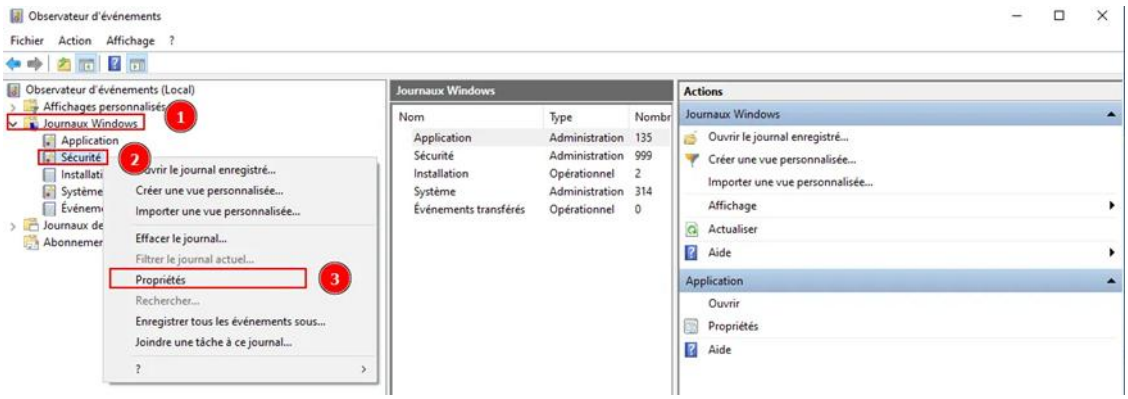
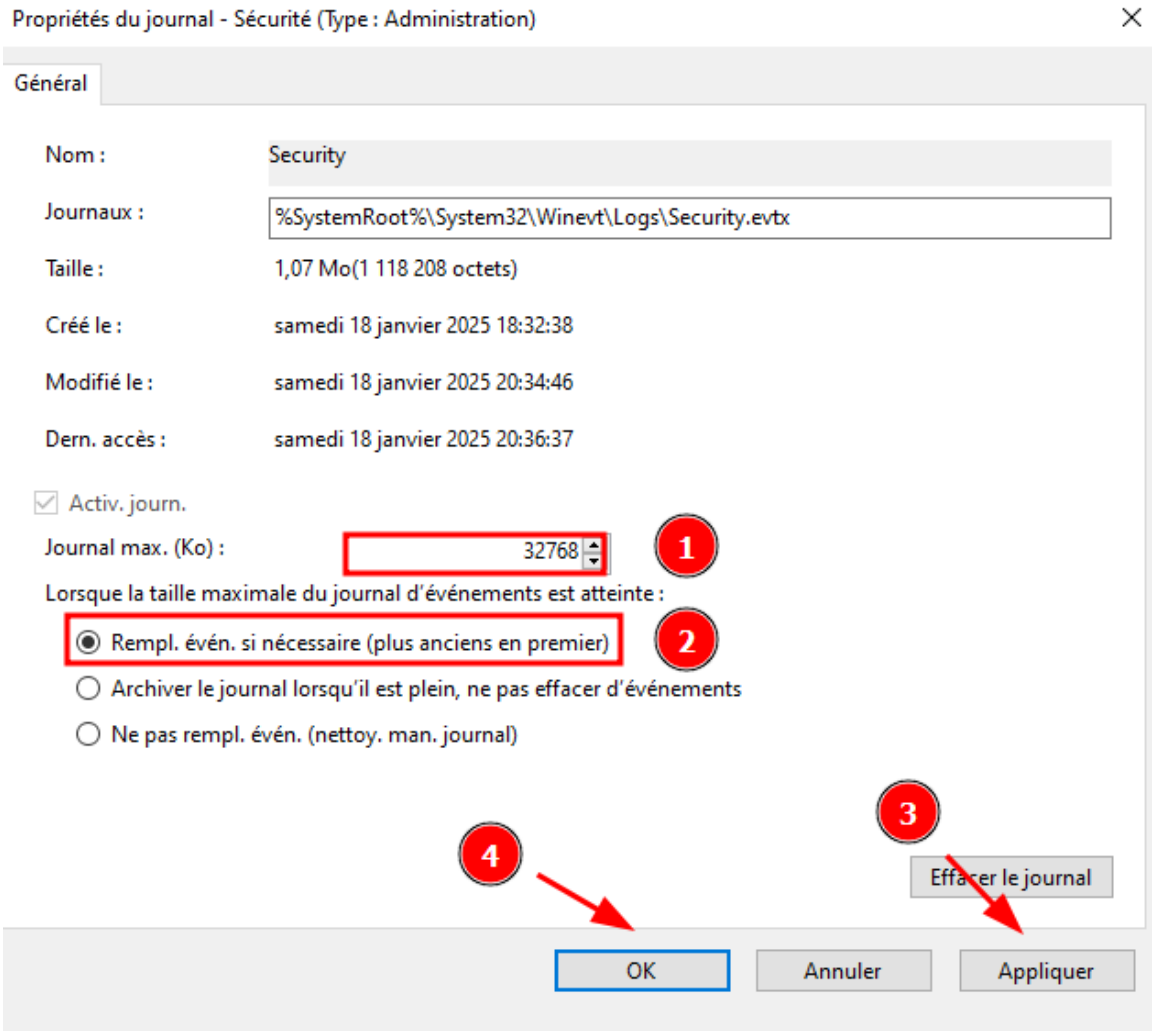
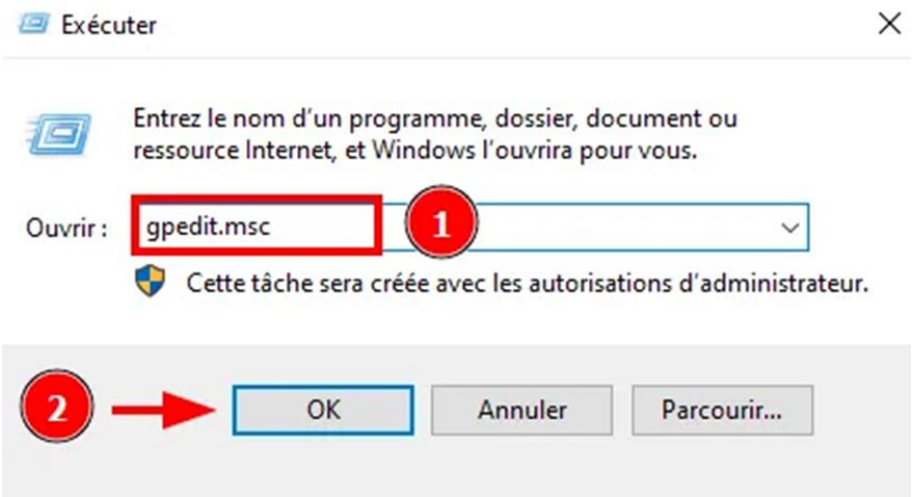
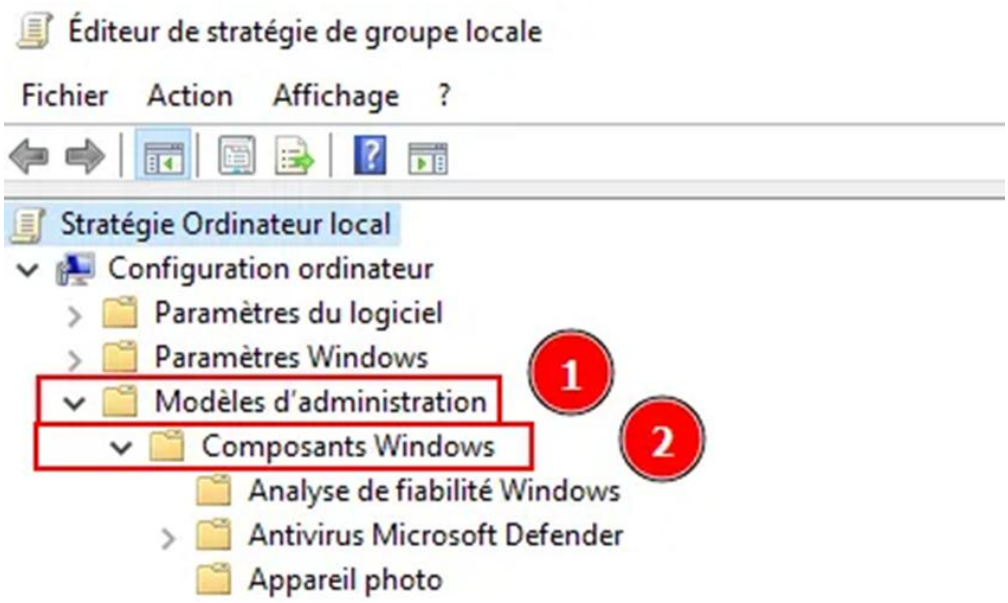
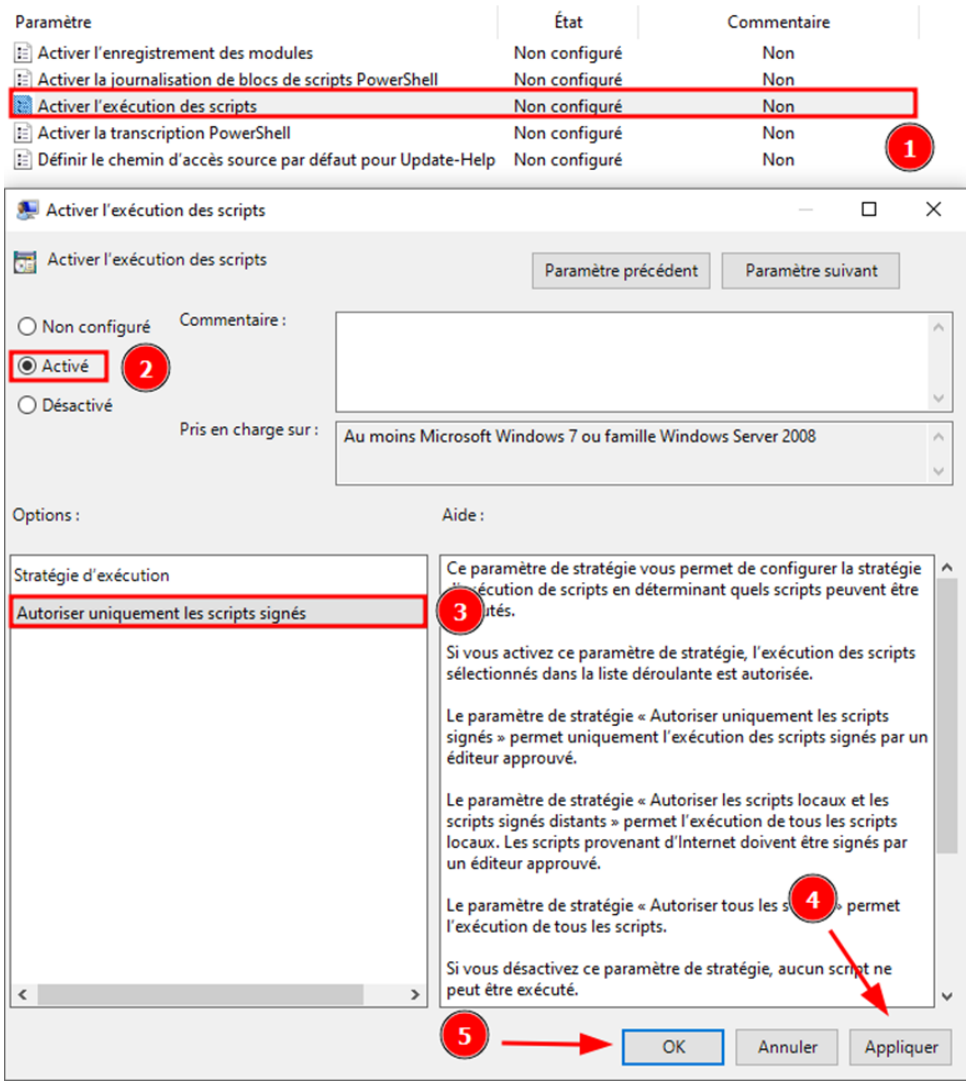
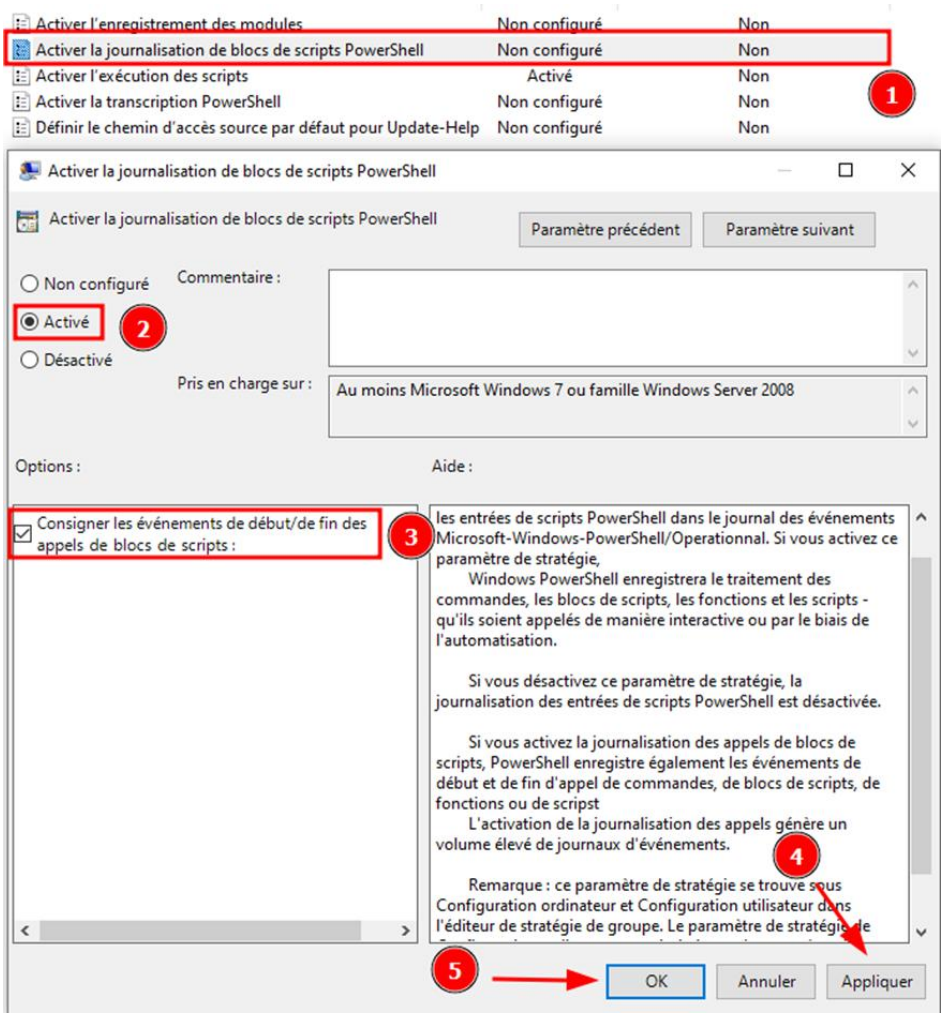
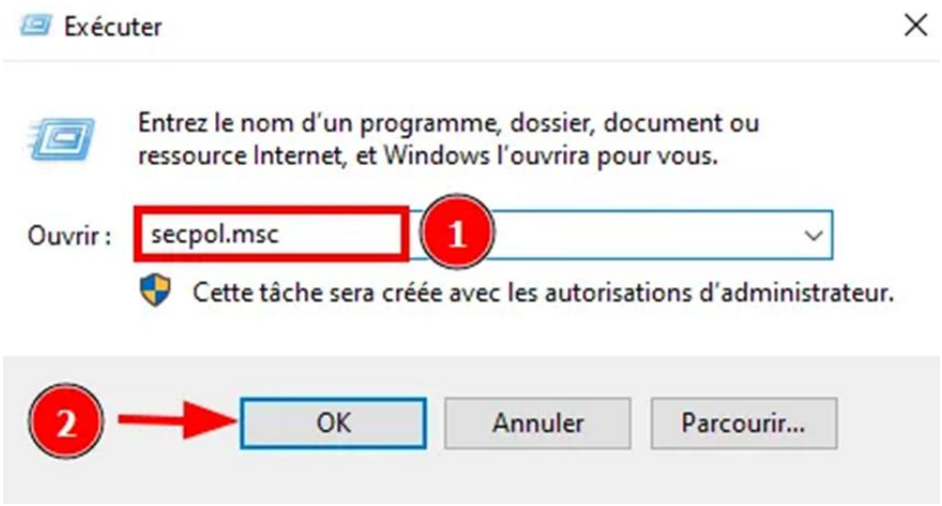
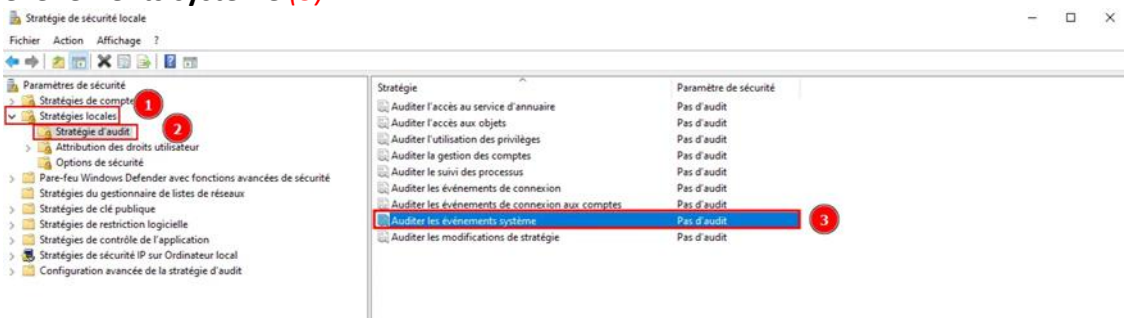
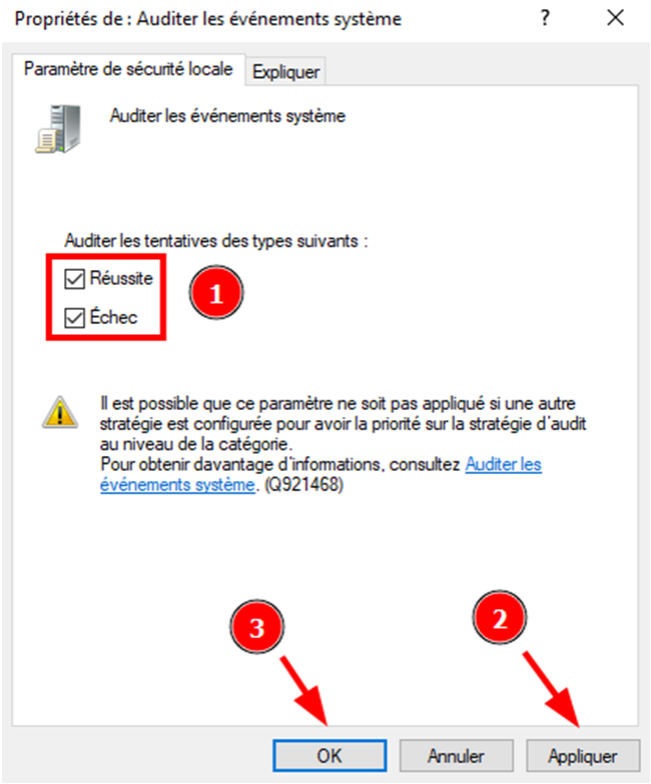
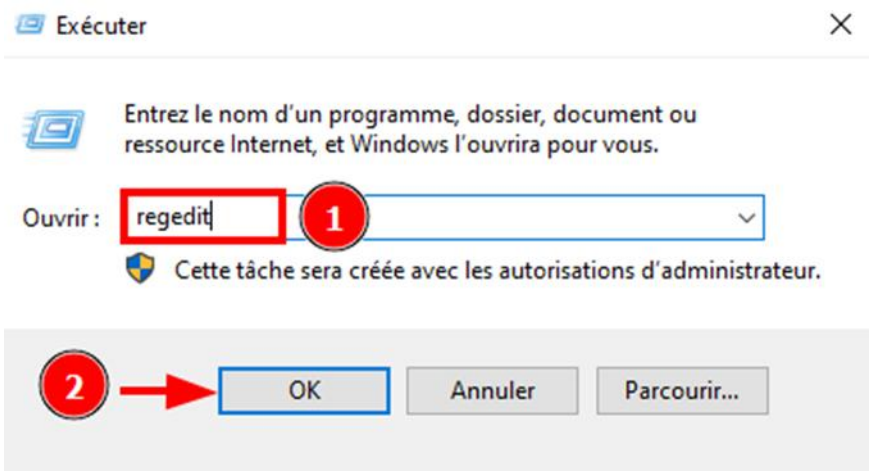
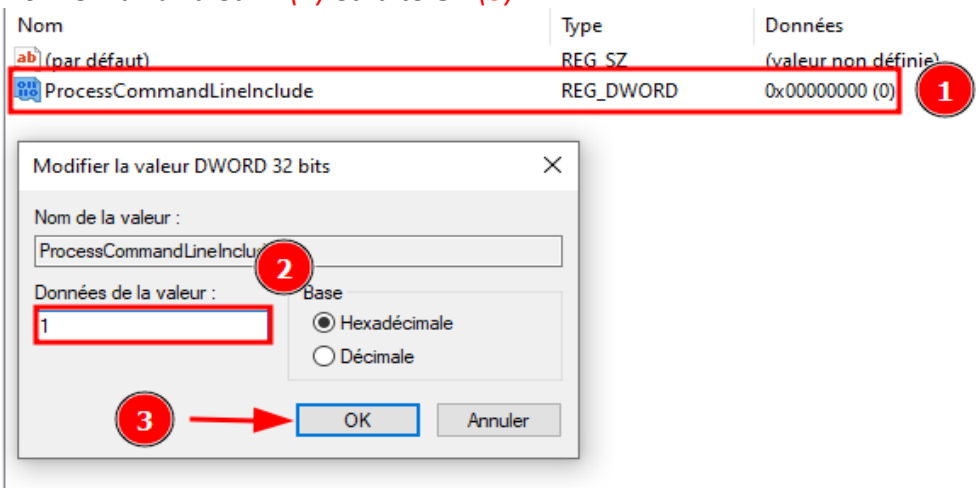
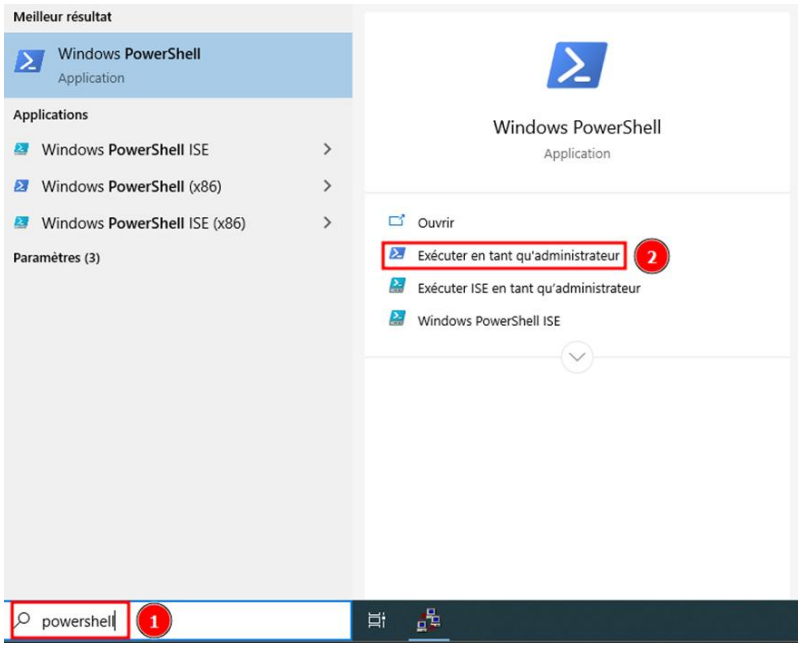
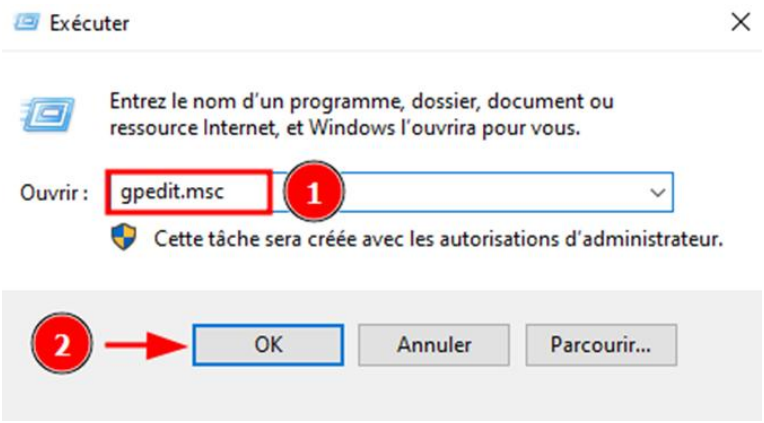
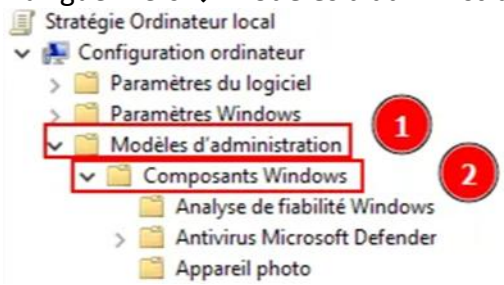
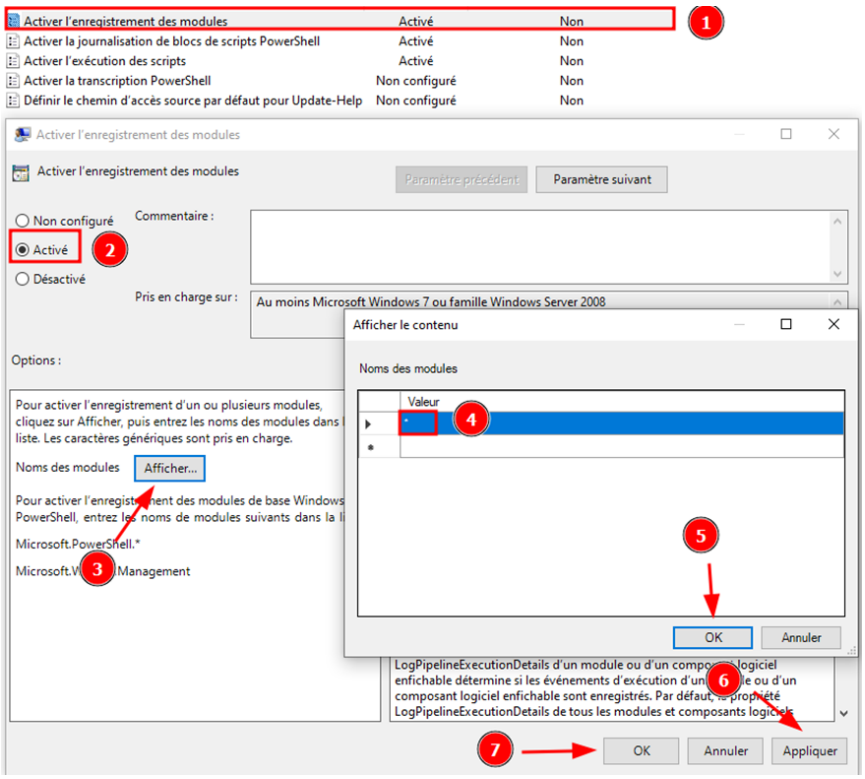
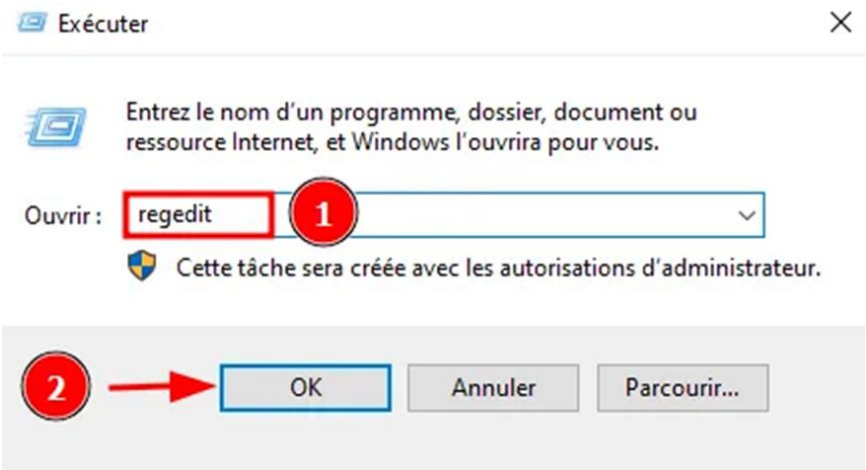
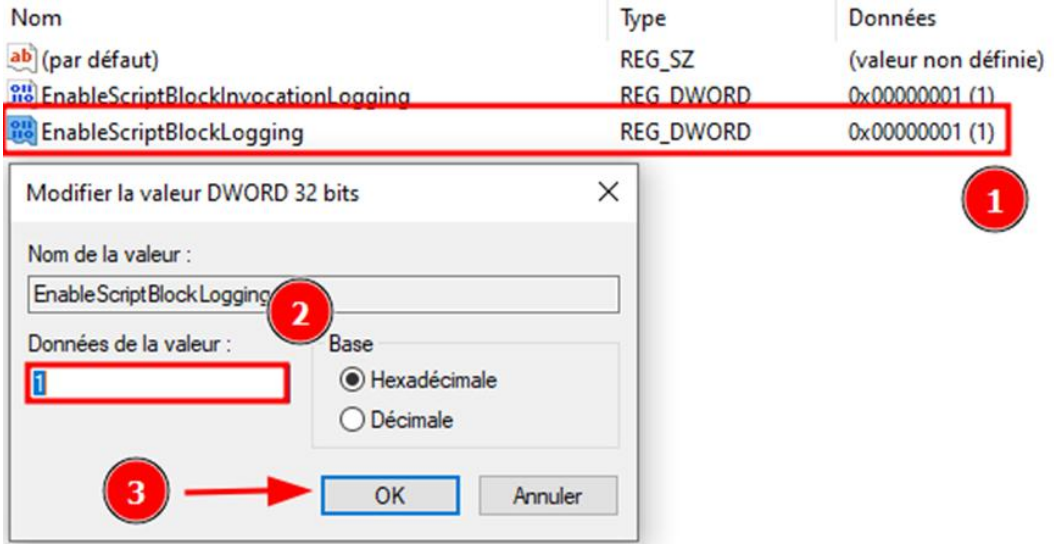
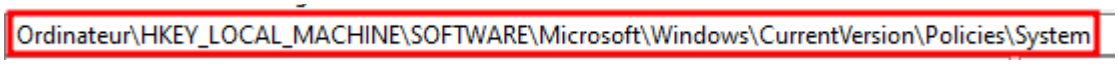
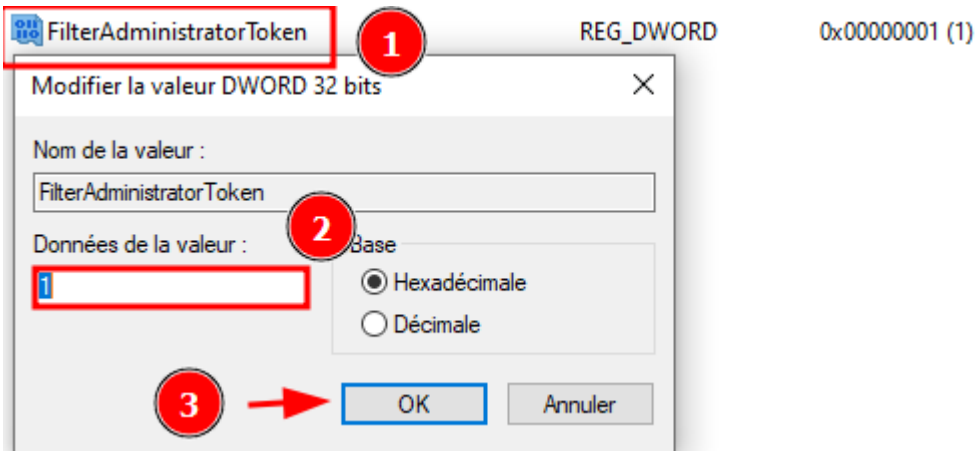
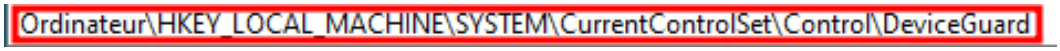
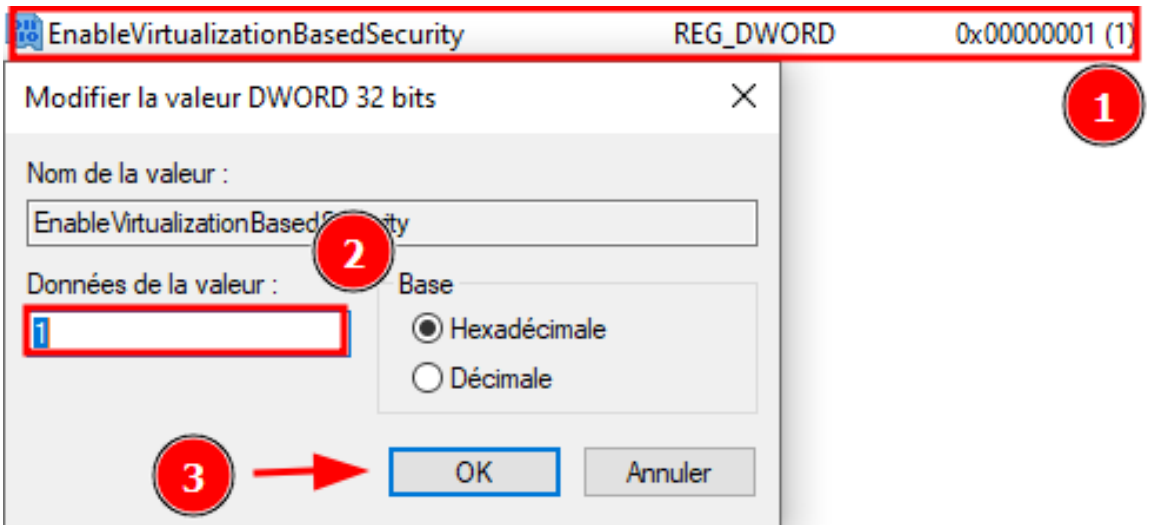
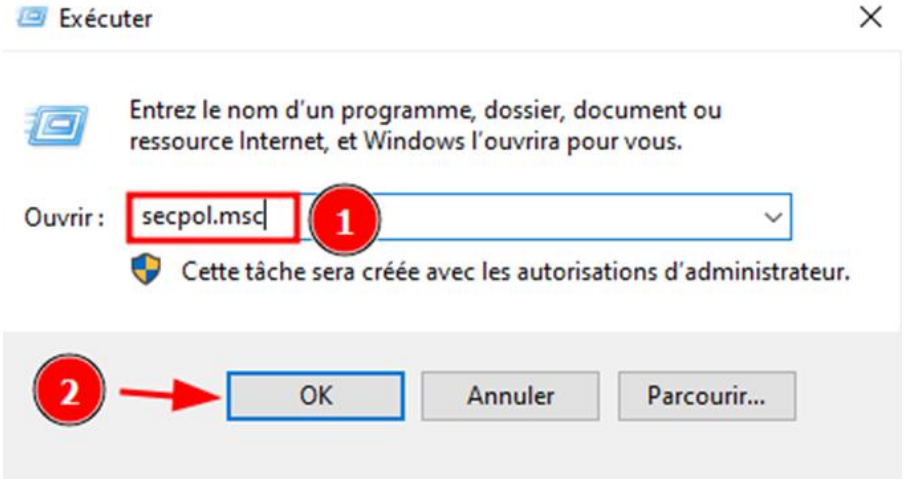
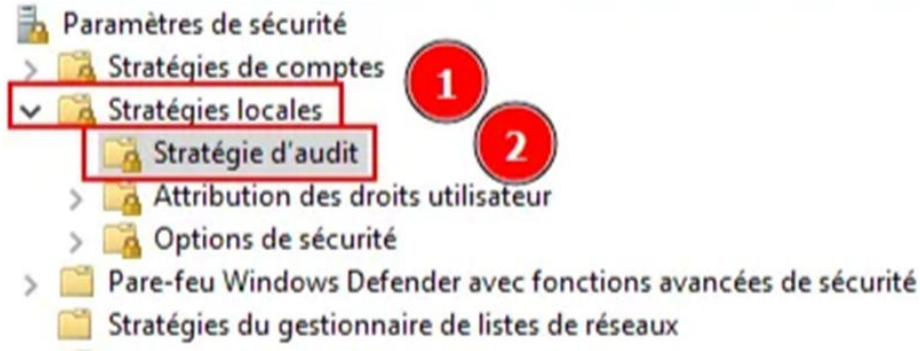
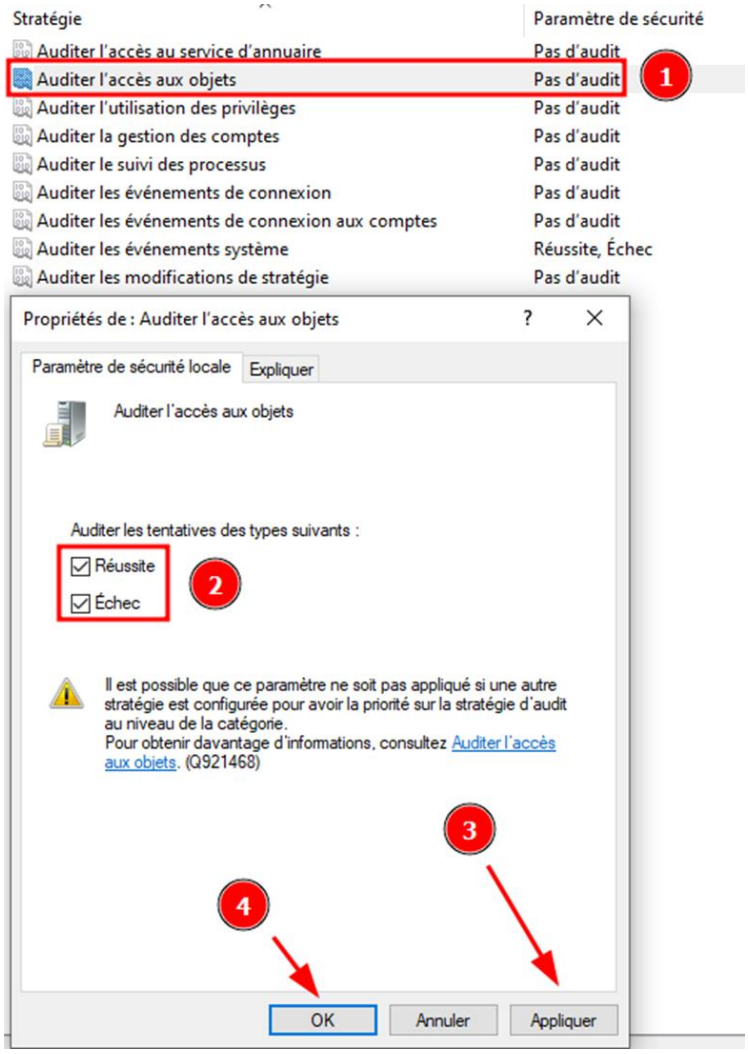
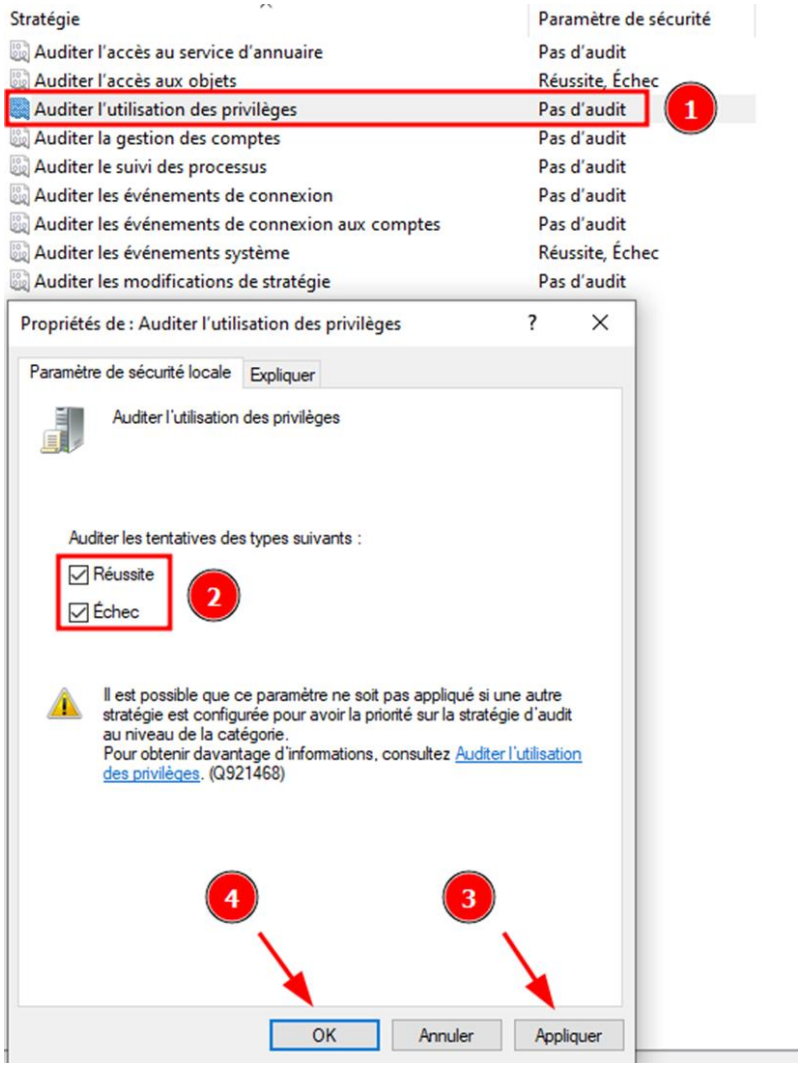
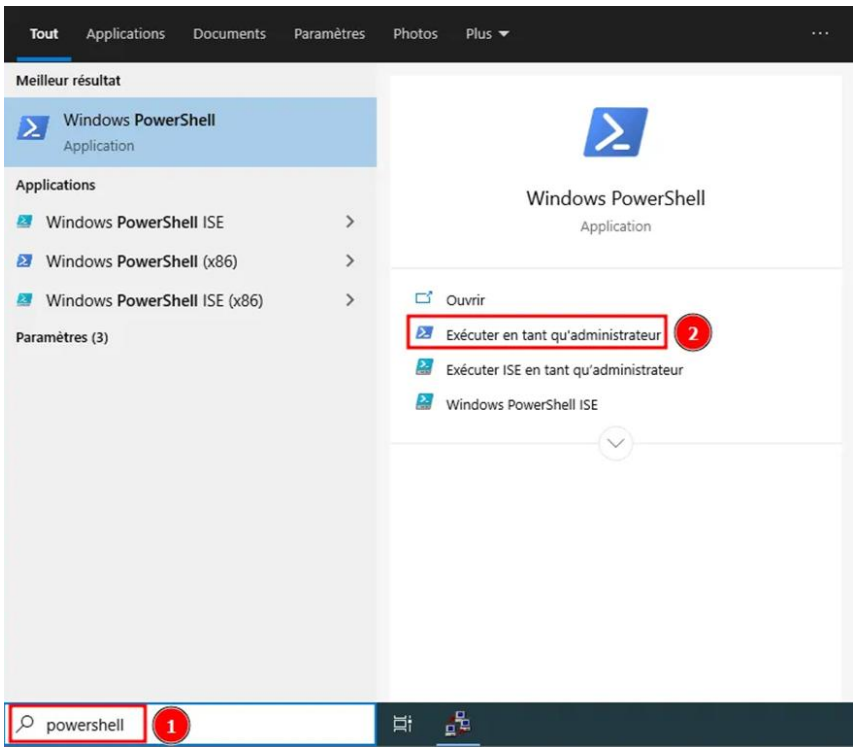
- Activez les protections supplémentaires avec ces commandes :
    - ```
      Set-MpPreference -MAPSReporting Advanced
      Set-MpPreference -EnableControlledFolderAccess Enabled
      ```

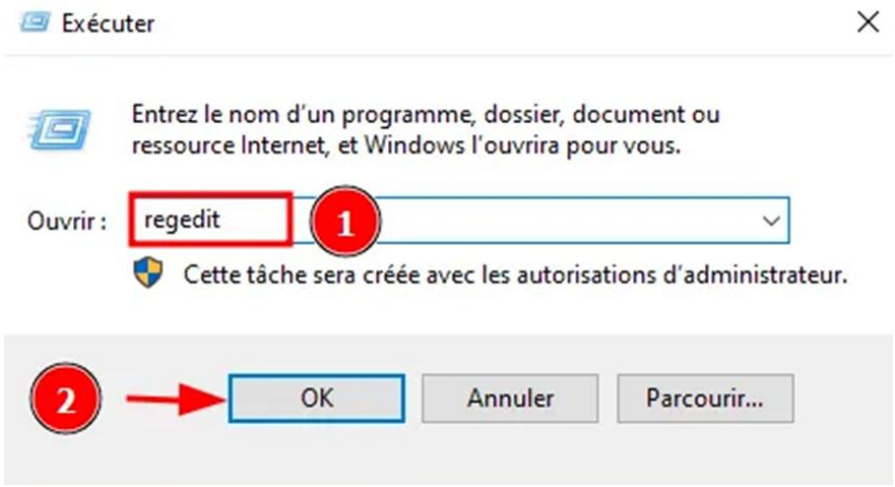
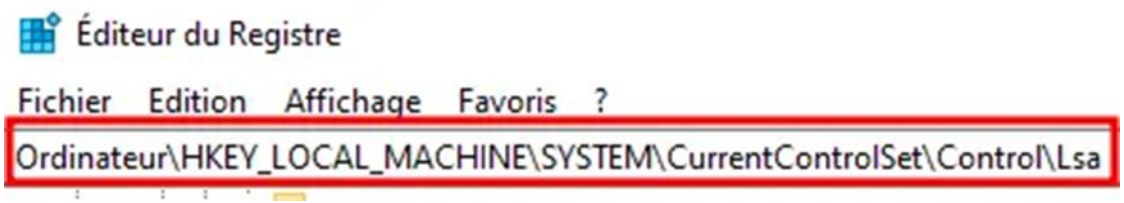
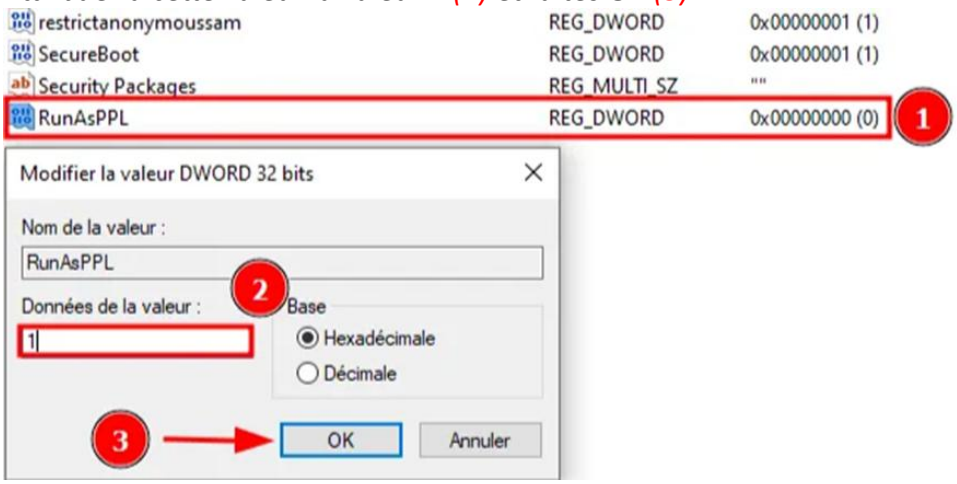
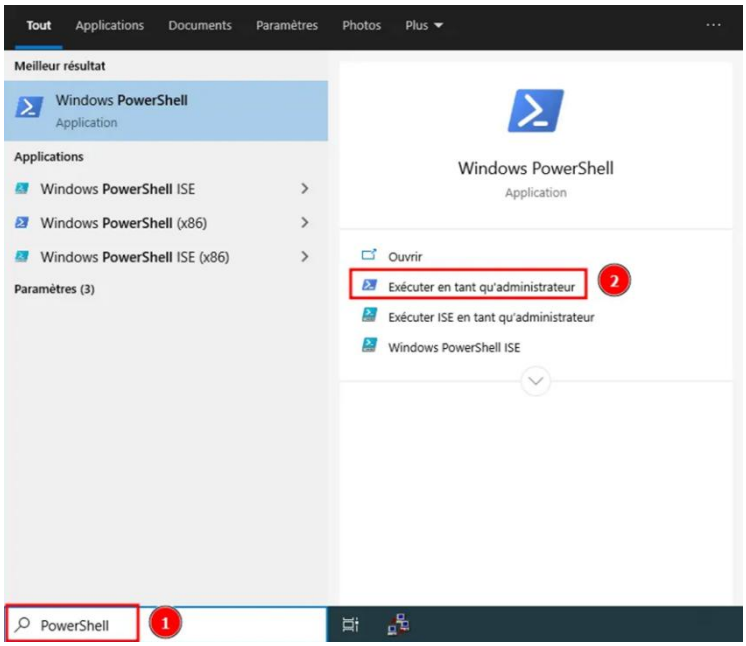
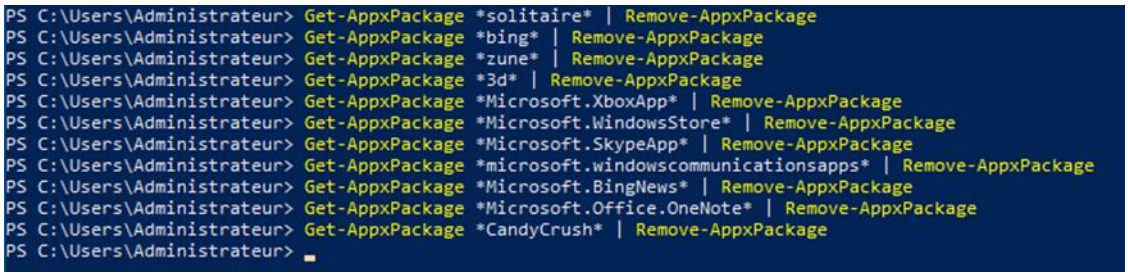
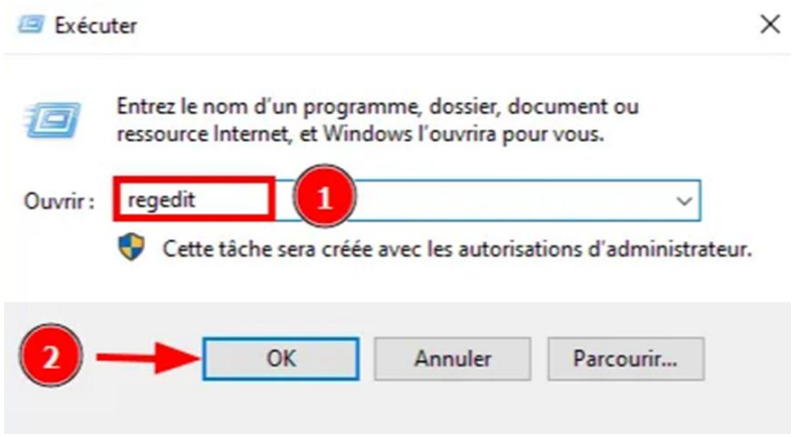


8. Tester les protections

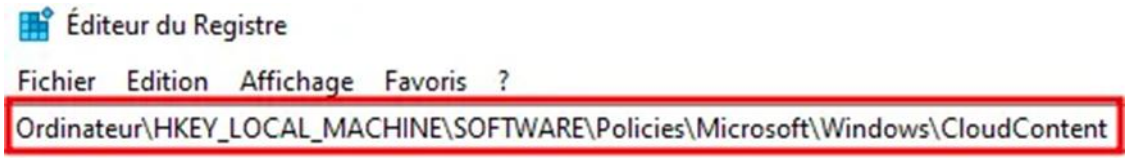
- **Télécharger un fichier de test (EICAR) :**
    - Rendez-vous sur le site https://www.eicar.org et tentez de télécharger un fichier de test.
    - Windows Defender devrait bloquer le téléchargement et afficher une alerte.

9. Pourquoi ces étapes sont importantes ?

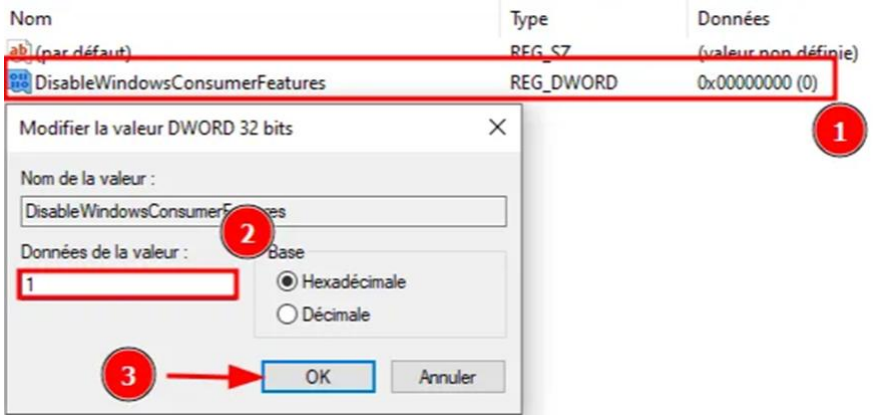
- **Protection en temps réel:** Bloque les logiciels malveillants dès qu'ils sont détectés.
- **Accès contrôlé aux dossiers:** Protège les données critiques contre les ransomwares.
- **Protection contre les exploits:** Empêche l'utilisation de vulnérabilités connues pour compromettre le système.
- **Planification des analyses:** Maintient la sécurité grâce à des analyses régulières.
      ```

5. Journalisation des événements Windows

1. Introduction

- La journalisation des événements est essentielle pour surveiller les activités du système, détecter les comportements suspects, et conserver des preuves en cas d'incident de sécurité.

2. Accéder au Visualiseur d'événements:

- Appuyez sur **Win + R**, tapez **eventvwr.msc** *(1)*, et appuyez sur **OK** *(2)*.



- Modifier la taille du **journal de sécurité:**
  - Dans le volet de gauche, développez **Journaux Windows** *(1)*, puis cliquez droit sur **Sécurité** *(2)* et sélectionnez **Propriétés** *(3)*.



- Sous **Taille maximale du journal (Ko)**, entrez une taille plus grande, par exemple **32 768 Ko** *(1)*.
- Cochez **Rempl.évén. si nécessaire (plus anciens en premier)** *(2)* pour éviter la suppression automatique.
- Cliquez sur **Appliquer** *(3)* et **OK** *(4)*.



- Répétez l'opération pour les journaux suivants :
  - Application
  - Système
- De même dans le volet de gauche, développez **Journaux des applications et des services** puis faites **:**
  - **Internet Explorer**
  - **Service de gestion de clés**
  - **Windows PowerShell**
  - **Evénements matériels**

3. Activer la journalisation des commandes PowerShell

- Cette fonction permet de tracer toutes les commandes exécutées, ce qui est utile pour détecter des attaques ou des scripts malveillants.

- Configurer la **journalisation des scripts PowerShell:**
  - Appuyez sur **Win + R**, tapez **gpedit.msc** *(1)*, puis appuyez sur **OK** *(2)*.



- Naviguez vers → **Modèles d'administration** *(1)* → **Composants Windows** *(2)*.



- Puis allez dans → **Windows PowerShell** *(3)*.

- Activez les options suivantes :
    - **Activer l'exécution des scripts** *(1)*:
        - Choisir l'option: **Activé** *(2)*.
        - Stratégie d'exécution: **Autoriser uniquement les scripts signés** *(3)*.
        - **Appliquer** les modifications *(4)*.
        - Puis cliquez sur: **OK** *(5)*.



- **Activer la journalisation de blocs de script PowerShell** *(1)*:
  - Choisir l'option: **Activé** *(2)*.
  - Puis cochez la case: **Consigner les événements de début/de fin des appels de blocs de scripts** *(3)*.
  - **Appliquer** les modifications *(4)*.
  - Puis cliquez sur: **OK** *(5)*.



4. Activer la journalisation des lignes de commande

- Cette configuration permet de capturer les commandes exécutées dans des terminaux ou scripts.

- Configurer via les **stratégies locales:**
  - Appuyez sur **Win + R**, tapez **secpol.msc** *(1)*, puis appuyez sur **OK** *(2)*.



- Allez dans → **Stratégies locales** *(1)* → **Stratégies d'audit** *(2)* → **Auditer les événements système** *(3)*.



- Activez **Réussite** *(1)* et **Echec** *(1)*.
- **Appliquez** *(2)* puis cliquer sur **et** OK *(3)*.



- Modifier le Registre pour **inclure les arguments de commande:**
  - Appuyez sur **Win + R**, tapez **regedit** (1), puis appuyez sur **OK** (2):



- Allez dans le registre suivant :
    - `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit`

- Créez une nouvelle **valeur DWORD (32 bits)** nommée **ProcessCommandLineInclude** *(1)*.
- Donnez-lui la valeur **1** *(2)* et faite **OK** *(3)*.



- Redémarrer pour appliquer les modifications.

5. Tester la configuration

- Générer un **événement test:**
    - Ouvrez un terminal **PowerShell** ou **CMD**, exécutez une commande simple, comme :
        - `Get-Process`
    - Dans le **Visualiseur d'événements**, vérifiez que la commande exécutée apparaît dans le journal **Sécurité** ou **Applications et Services**.

- Analyser les **journaux:**
  - Filtrez les événements pour rechercher les activités suspectes, comme l'exécution de scripts non autorisés.

6. Pourquoi ces étapes sont importantes ?

- **Taille des journaux:** Garantit que les informations critiques ne sont pas perdues en cas d'incidents prolongés.
- **Journalisation PowerShell:** Permet d'identifier l'utilisation abusive de scripts ou commandes malveillantes.
- **Lignes de commande:** Aide à tracer les actions exécutées par des utilisateurs ou logiciels malveillants.

6. Mesures de sécurité avancées

1. Introduction

- Dans cette étape, nous allons appliquer des configurations avancées pour renforcer la sécurité du système, notamment en activant des options supplémentaires pour la journalisation, les politiques d'audit, et la protection des scripts.

2. Activer les paramètres de sécurité avancés

- Ces options ajoutent une couche de protection contre les vulnérabilités exploitables.

- Configurer les politiques de sécurité via **PowerShell:**
  - Ouvrez une fenêtre **PowerShell** *(1)* en tant qu'**Administrateur** *(2)*.



- Exécutez les commandes suivantes :
    - `Set-ProcessMitigation -System -Enable DEP, BottomUp, HighEntropy, ForceRelocateImages, SEHOP`

```
>>
PS C:\Users\Administrateur> Set-ProcessMitigation -System -Enable DEP, BottomUp, HighEntropy, ForceRelocateImages, SEHOP>>
```

3. Activer la journalisation avancée des scripts

- La journalisation avancée permet de capturer les scripts exécutés, y compris les modules de PowerShell.

- Configurer via les **stratégies locales:**
    - Ouvrez **gpedit.msc** *(1)* et faites **OK** *(2)*.



- Naviguez vers → **Modèles d'administration** *(1)* → **Composants Windows** *(2)*.



- Puis dans → **Windows PowerShell** *(3)*.

- Activez l'option suivante :
  - Allez dans **Activer l'enregistrement des modules** *(1)*.
  - Puis **Activez** le module *(2)*.
  - Faites **Afficher** *(3)*.
  - Choisir en valeur "*" *(4)* puis faite **OK** *(5)*.
  - **Appliquer** *(6)* et faite encore **OK** *(7)*.



- Activer la journalisation des scripts via **le Registre:**
  - Ouvrez **regedit** *(1)* puis faites **OK** *(2)*.



- Naviguez vers la clé suivante :
    - `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging`
- Si la clé **ScriptBlockLogging** n'existe pas, créez-la.

- Ajoutez une valeur **DWORD (32 bits)** nommée **EnableScriptBlockLogging** *(1)* et donnez-lui la valeur 1 *(2)* et faites OK *(3)*.



- Naviguez vers la clé suivante:
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System



- Ajoutez une valeur **DWORD (32 bits)** nommée **FilterAdministratorToken** *(1)* et donnez-lui la valeur **1** *(2)* et faites **OK** *(3)*.



- Naviguez vers la clé suivante:
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceGuard



- Ajoutez une valeur **DWORD (32 bits)** nommée **EnableVirtualizationBasedSecurity** *(1)* et donnez-lui la valeur **1** *(2)* et faites **OK** *(3)*.



4. Configurer les politiques d'audit

- Ces politiques assurent une surveillance renforcée des activités système.

- Configurer via **secpol.msc** *(1)* et faites **OK** *(2)*.



- Accédez à → **Stratégies locales** *(1)* → **Stratégies d'audit** *(2)*.



- Modifiez les paramètres suivants :
  - Allez dans **Auditer l'accès aux objets** *(1)*.
  - Activez **Réussite/Echec** *(2)*.
  - Puis faites **Appliquer** *(3)* et **OK** *(4)*.



- Allez dans **Auditer l'utilisation des privilèges** *(1)*.
- Activez **Réussite/Echec** *(2)*.
- Puis faites **Appliquer** *(3)* et **OK** *(4)*.



- Vérifier les paramètres **d'audit :**
    - Dans une fenêtre PowerShell, exécutez la commande suivante pour afficher les politiques d'audit configurées :
        - `AuditPol /get /category:*`

5. Renforcer la configuration des scripts PowerShell

- Les scripts malveillants constituent une menace importante. Protéger leur exécution est essentiel.

- Activer la **politique d'exécution:**
  - Exécutez **PowerShell** *(1)* en mode **Administrateur** *(2)* :



- Puis entrez la commande suivante :
  - `Set-ExecutionPolicy AllSigned`

```
PS C:\Users\Administrateur> Set-ExecutionPolicy AllSigned

Modification de la stratégie d'exécution
La stratégie d'exécution permet de vous prémunir contre les scripts que vous jugez non fiables. En modifiant la
stratégie d'exécution, vous vous exposez aux risques de sécurité décrits dans la rubrique d'aide
about_Execution_Policies à l'adresse https://go.microsoft.com/fwlink/?LinkID=135170. Voulez-vous modifier la stratégie
d'exécution ?
[O] Oui  [T] Oui pour tout  [N] Non  [U] Non pour tout  [S] Suspendre  [?] Aide (la valeur par défaut est « N ») : T
PS C:\Users\Administrateur>
```

- Cette configuration exige que tous les scripts PowerShell soient signés numériquement avant exécution.

- Vérifier la **politique d'exécution** en executant**:**
  - `Get-ExecutionPolicy -List`
  - Assurez-vous que les sorties indique **AllSigned**.

6. Tester les configurations

- Exécuter un script **PowerShell non signé:**
  - Créez un script simple avec l'extension **.ps1**, par exemple :
  - `Write-Host "Test script"`
  - Tentez de l'exécuter. Vous devriez recevoir un message d'erreur bloquant l'exécution.

- Vérifier les **journaux:**
  - Ouvrez le **Visualiseur d'événements** et recherchez des entrées liées à PowerShell dans le journal **Applications et Services > Microsoft > Windows > PowerShell > Operational**.

7. Pourquoi ces étapes sont importantes ?

- **Paramètres avancés:** Ajoutent une protection contre les attaques mémoire et exploitent les vulnérabilités système.
- **Journalisation PowerShell:** Permet de surveiller et de bloquer les scripts malveillants.
- **Politiques d'audit:** Assurent une traçabilité complète des événements critiques.

7. Sécurisation de Lsass

1. Introduction

- Le processus LSASS (Local Security Authority Subsystem Service) gère l'authentification des utilisateurs et stocke des informations sensibles, telles que les mots de passe. Renforcer sa sécurité est crucial pour empêcher le vol d'identifiants.

2. Activer le mode protégé de LSASS

- Cela empêche les outils malveillants d'accéder aux données en mémoire de LSASS.

- Modifier le **Registre:**
  - Appuyez sur **Win + R**, tapez **regedit** *(1)*, puis appuyez sur **OK** *(2)*.



- Naviguez vers la clé suivante :
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`



- Créez une nouvelle **valeur DWORD (32 bits)** nommée **RunAsPPL** *(1)*.
- Attribuez à cette valeur la valeur **1** *(2)* et faites **OK** *(3)*.



- Les modifications seront appliquées au prochain redémarrage.

3. Tester la configuration

- Vérifier le mode protégé de **LSASS:**
  - Ouvrez une fenêtre **PowerShell** en tant qu'administrateur.
  - Exécutez la commande suivante pour vérifier si LSASS fonctionne en mode protégé :
    - `Get-Process -Name lsass | Select-Object Name, Path`
  - Le chemin du processus LSASS doit être bloqué.

- Analyser les **journaux:**
  - Ouvrez le **Visualiseur d'événements** et recherchez les événements relatifs au processus LSASS pour confirmer qu'il n'y a pas d'erreurs.

- Tester avec **Mimikatz**:
  - Téléchargez l'outil et vérifié si les données n'ont pas été éxtrait par celui-ci.

4. Pourquoi ces étapes sont importantes ?

- **Mode protégé LSASS:** Empêche les outils d'extraction de mots de passe (comme Mimikatz) d'accéder à LSASS.

8. Gestion des applications

1. Introduction

- Cette étape vise à supprimer les applications inutiles ou intégrées indésirables qui peuvent poser des risques de sécurité ou encombrer le système.

2. Supprimer les applications intégrées via PowerShell

- Certaines applications intégrées ne peuvent pas être désinstallées via les Paramètres. Utilisons PowerShell.

- Ouvrir **PowerShell en mode administrateur:**
  - Appuyez sur **Win + S**, tapez **PowerShell** *(1)*, faites un clic droit, et choisissez **Exécuter en tant qu'administrateur** *(2)*.



- Supprimer toutes les **applications inutiles:**
  - Voici les lignes de commande pour tout désinstaller :
  - ```
    Get-AppxPackage *solitaire* | Remove-AppxPackage
    Get-AppxPackage *bing* | Remove-AppxPackage
    Get-AppxPackage *zune* | Remove-AppxPackage
    Get-AppxPackage *3d* | Remove-AppxPackage
    Get-AppxPackage *Microsoft.XboxApp* | Remove-AppxPackage
    Get-AppxPackage *Microsoft.WindowsStore* | Remove-AppxPackage
    Get-AppxPackage *Microsoft.SkypeApp* | Remove-AppxPackage
    Get-AppxPackage *microsoft.windowscommunicationsapps* | Remove-
    AppxPackage
    Get-AppxPackage *Microsoft.BingNews* | Remove-AppxPackage
    Get-AppxPackage *Microsoft.Office.OneNote* | Remove-AppxPackage
    Get-AppxPackage *CandyCrush* | Remove-AppxPackage
    ```



3. Empêcher la reinstallation automatique des applications

- Windows peut réinstaller certaines applications après une mise à jour. Bloquons cela.

- Modifier le **Registre:**
  - Appuyez sur **Win + R**, tapez **regedit** *(1)*, et appuyez sur **OK** *(2)*.


    ```

- Naviguez vers la clé suivante :
    - `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CloudContent`

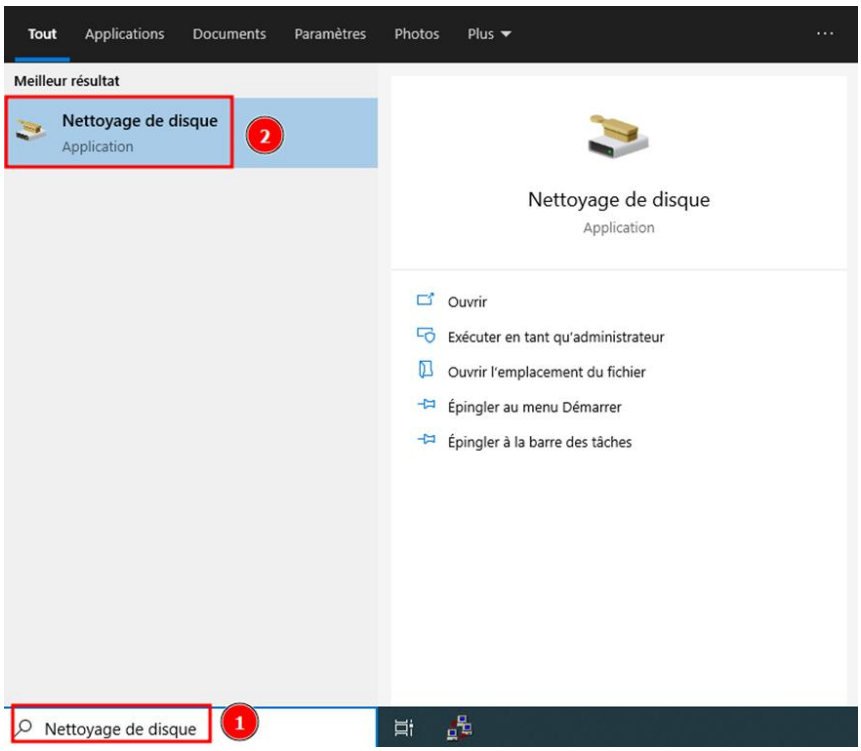


- Si la clé **CloudContent** n'existe pas, créez-la :
    - Faites un clic droit sur **Windows**, choisissez **Nouveau > Clé**, et nommez-la **CloudContent**.
    - Dans **CloudContent**, créez une nouvelle **valeur DWORD (32 bits)** nommée **DisableWindowsConsumerFeatures** *(1)*.
    - Attribuez-lui la valeur **1** *(2)* et faites **OK** *(3)*.

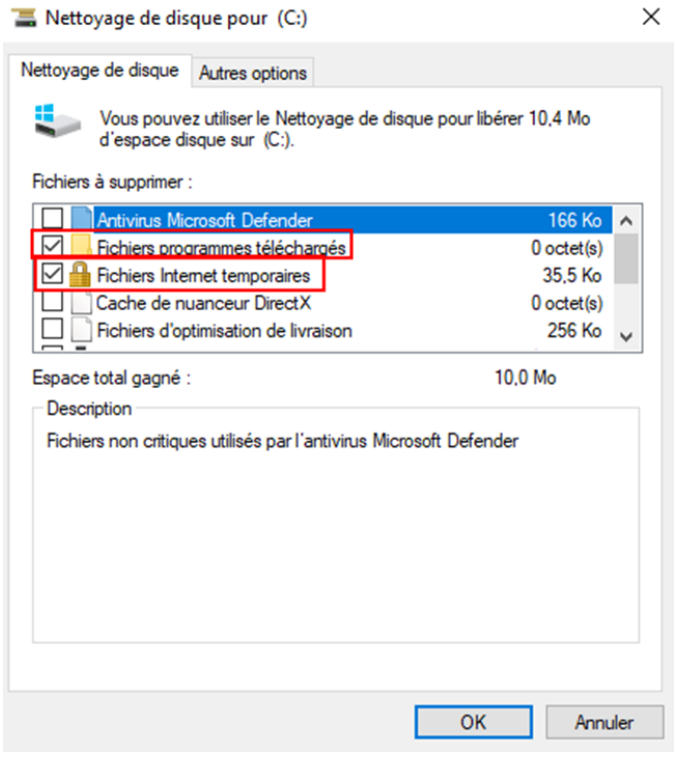


4. Nettoyer les fichiers restants

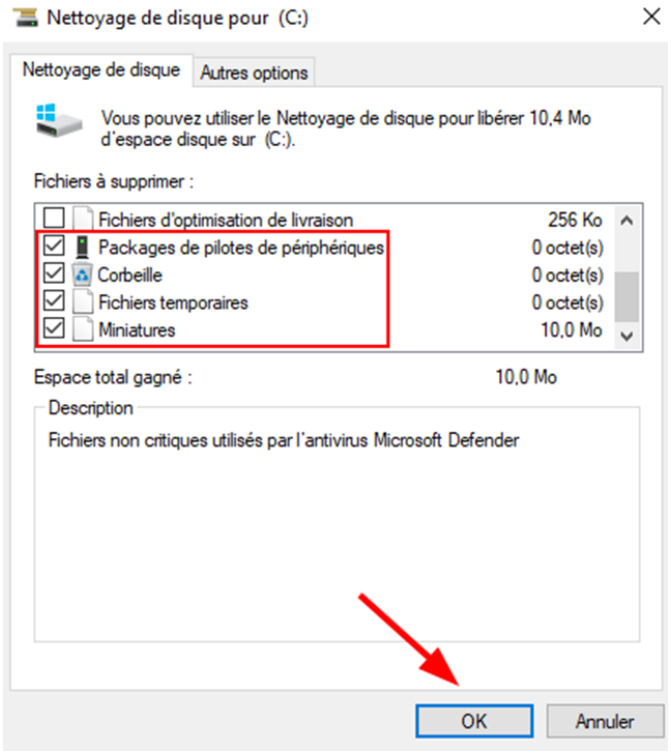
- Utiliser l'outil de **nettoyage de disque:**
    - Appuyez sur **Win + S**, tapez **Nettoyage de disque** *(1)*, et ouvrez l'application *(2)*.



- Sélectionnez le lecteur principal (généralement C:), et cliquez sur **OK**.
- Cochez toutes les options pertinentes, notamment **Fichiers temporaires**, **Fichiers système**, et **Applications inutilisées**.



- Cliquez sur **OK** pour démarrer le nettoyage.



5. Tester et valider

- Vérifier les **applications restantes:**
  - Revenez à **Paramètres > Applications et fonctionnalités** et confirmez que seules les applications nécessaires restent installées.

- Effectuer une analyse **Windows Defender:**
  - Assurez-vous qu'aucune application potentiellement indésirable (PUA) ne persiste en effectuant une analyse complète via **Sécurité Windows**.

6. Pourquoi ces étapes sont importantes

- **Réduction des risques:** Les applications inutiles ou indésirables peuvent présenter des failles de sécurité ou être exploitées par des logiciels malveillants.
- **Performances optimisées:** Supprimer les applications superflues libère des ressources système.

- **Prévention:** Empêcher la réinstallation automatique évite de perdre du temps à répéter ces étapes.

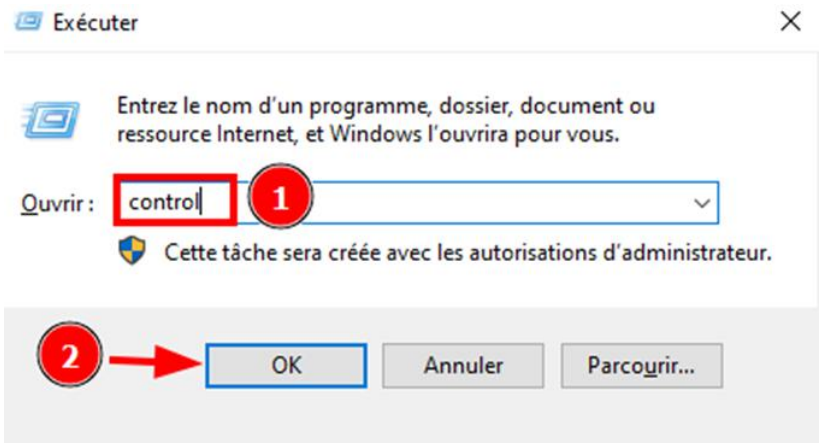
9. Pare-feu et blocage des connexions

1. Introduction

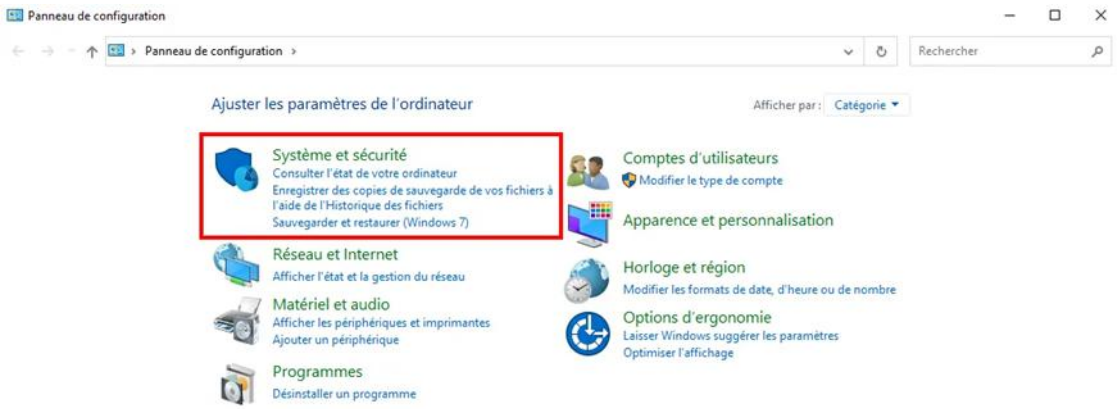
- Dans cette étape, nous allons configurer le pare-feu Windows pour renforcer la sécurité réseau en bloquant les connexions non autorisées, y compris les binaires spécifiques (LOLBins).

2. Activer et configure le Pare-feu Windows

- Accéder aux paramètres du **Pare-feu Windows:**
  - Appuyez sur **Win + R**, tapez **control** *(1)*, et appuyez sur **OK** *(2)*.

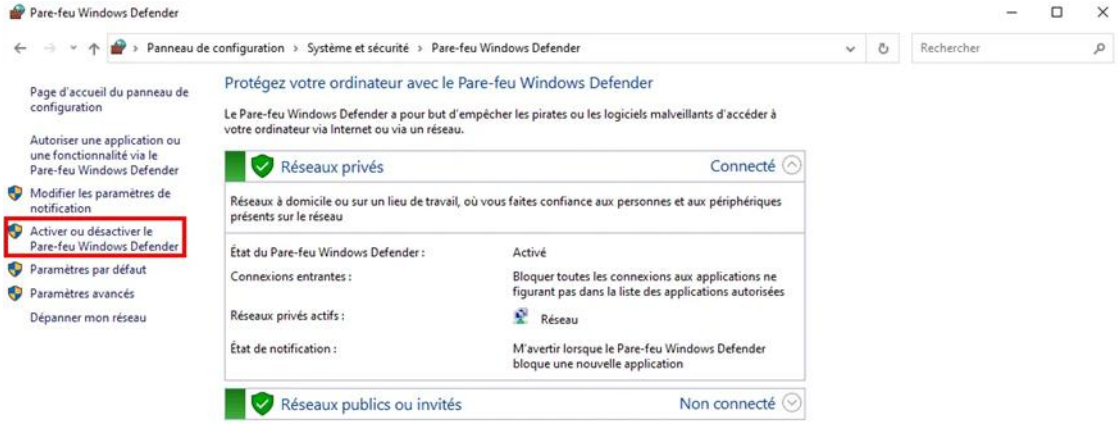


- Allez dans → **Système et sécurité.**

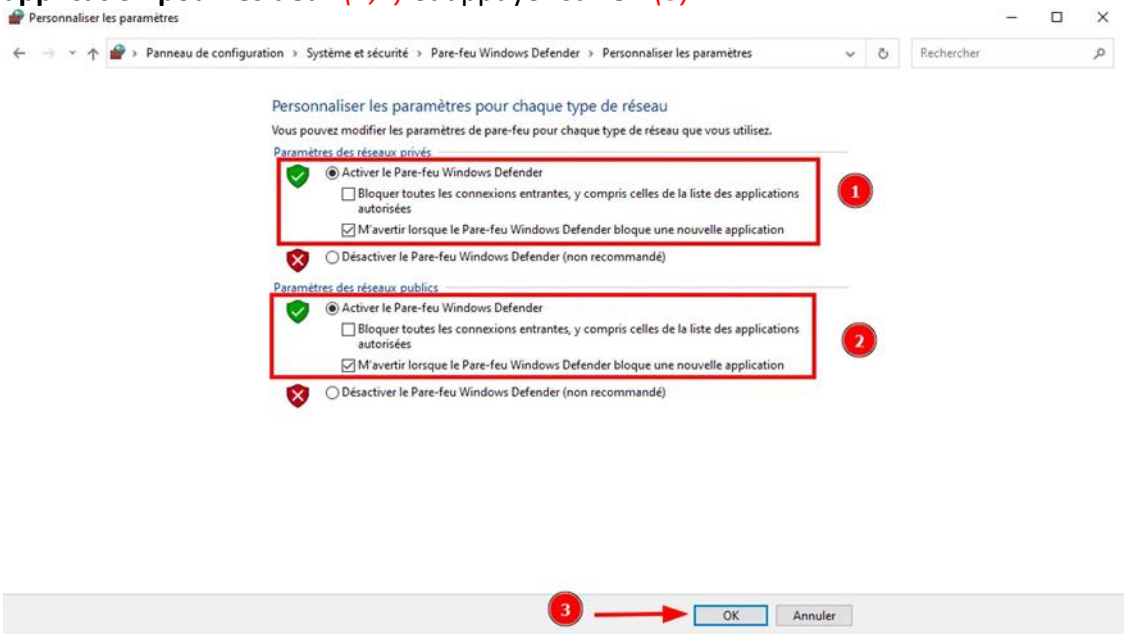


- Puis dans → **Pare-feu Windows Defender**.

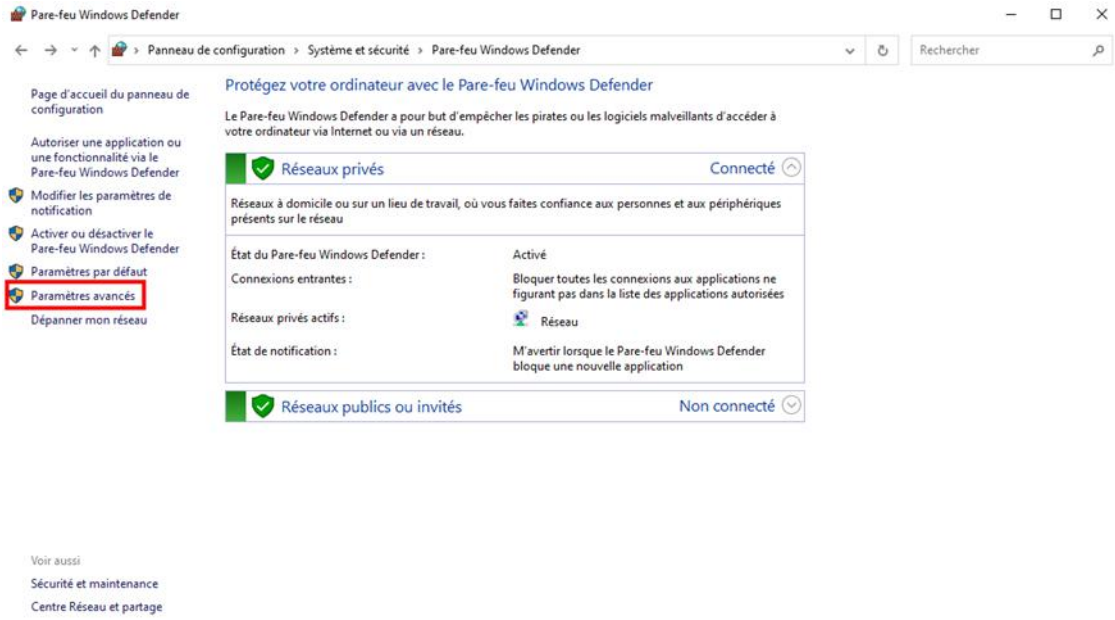
- Cliquez sur **Activer ou désactiver le Pare-feu Windows Defender** dans le menu de gauche.



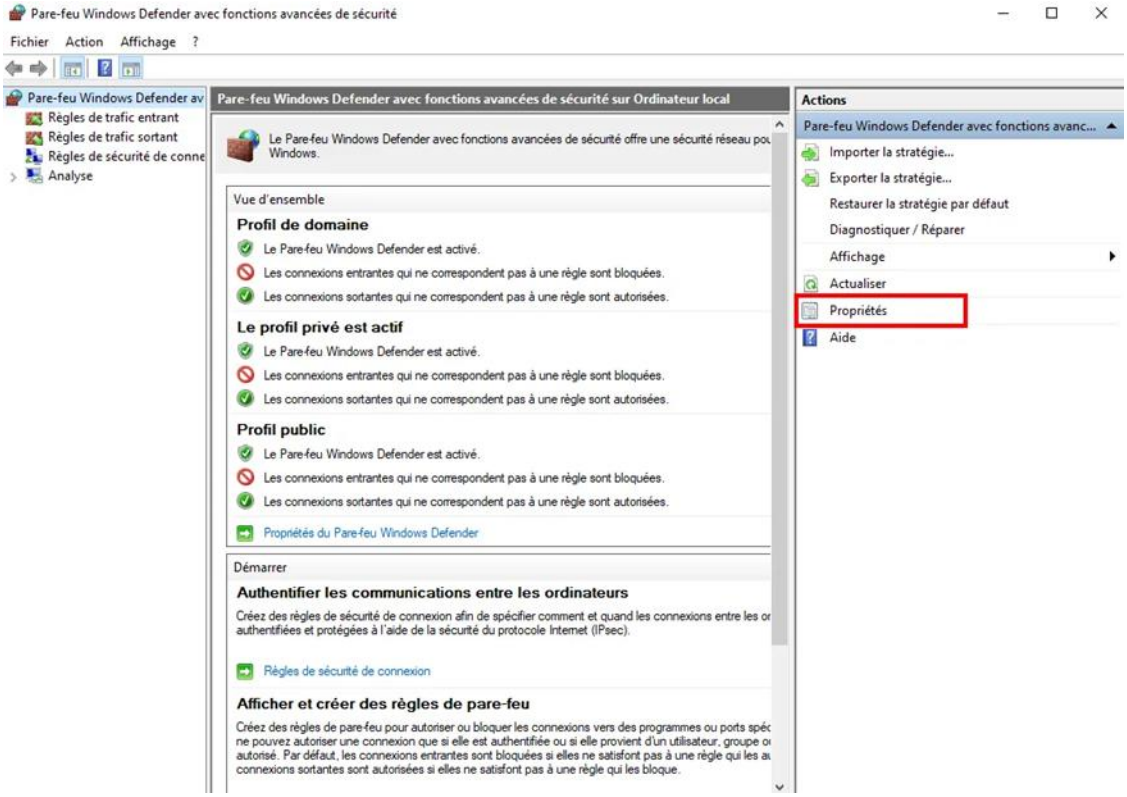
- Assurez-vous que le pare-feu est activé pour les **réseaux privés** *(1)* et **publics** *(2)* puis cochez **M'avertir lorsque le Pare-Feu Windows Defender bloque une nouvelle application pour les deux** *(1,2)* et appuyez sur **OK** *(3)*.



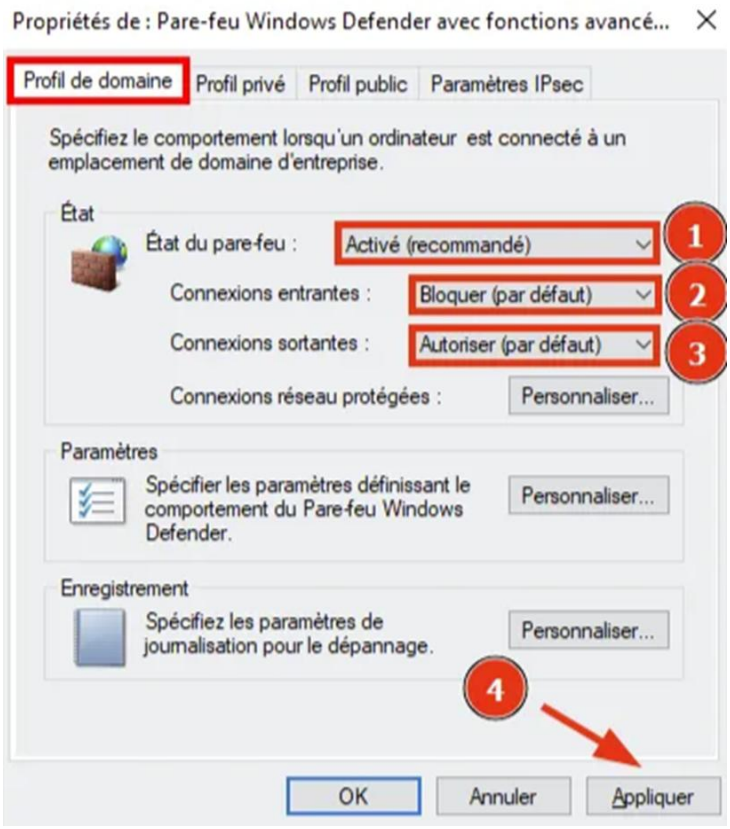
- Configurer les **règles par défaut:**
  - Dans le menu principal, cliquez sur **Paramètres avancés**.



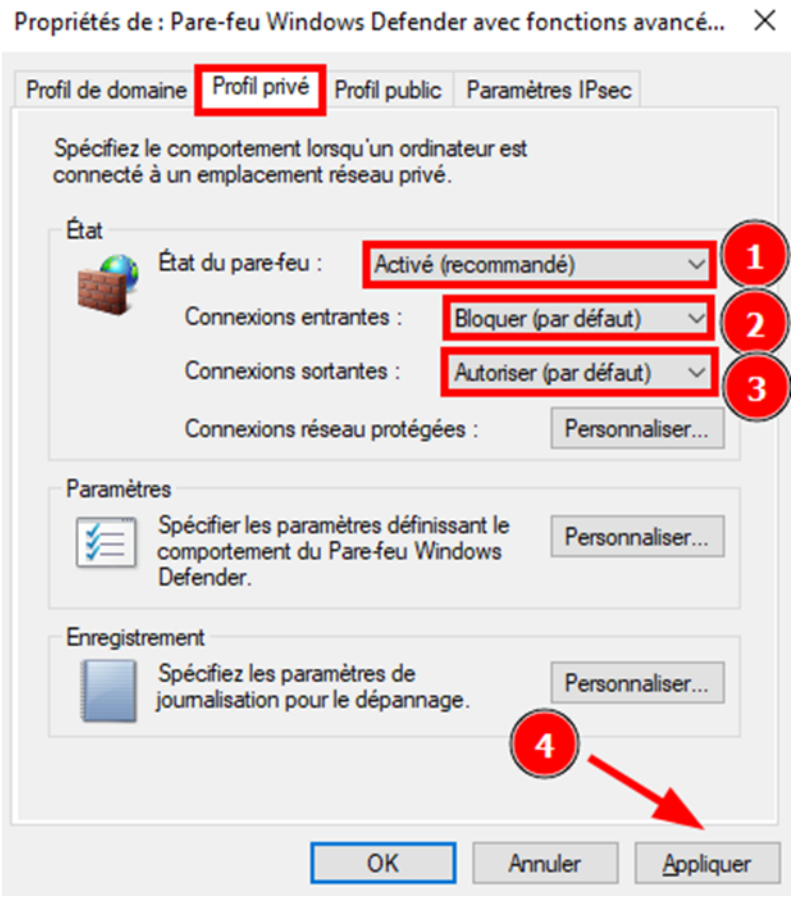
- Accédez à **Propriétés à droite**.



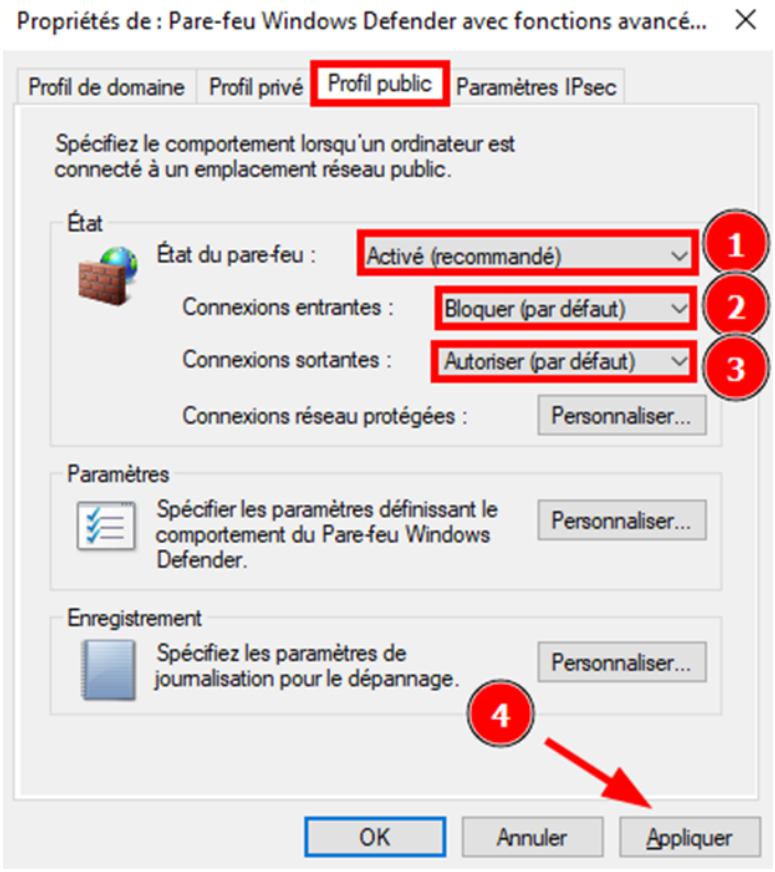
- Sous l'onglet **Paramètres**, assurez-vous que les actions par défaut sont définies comme suit :
    - Dans **Profil de domaine**:
        - **Etat du pare-feu** : **Activé** *(1)*.
        - **Connexions entrantes** : **Bloquer** *(2)*.
        - **Connexions sortantes** : **Autoriser** *(3)*.
        - Puis **Appliquer** *(4)* les modifications.



- Dans **Profil privé**:
  - **Etat du pare-feu : Activé** *(1)*.
  - **Connexions entrantes : Bloquer** *(2)*.
  - **Connexions sortantes : Autoriser** *(3)*.
  - Puis **Appliquer** les modifications *(4)*.



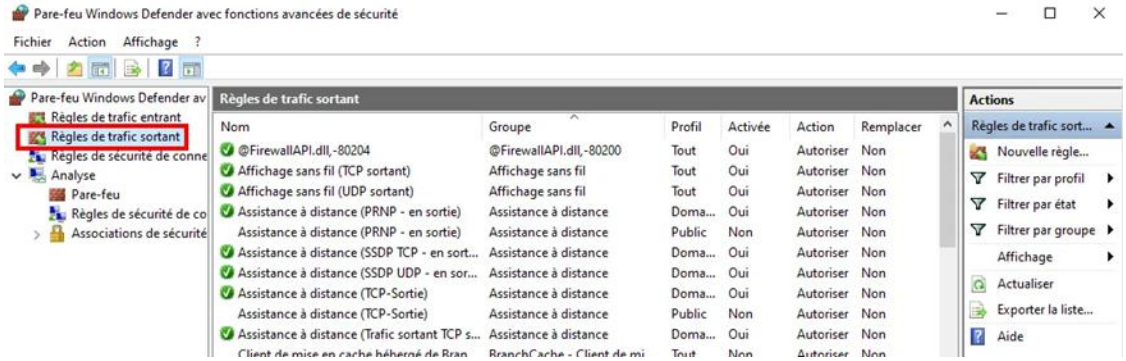
- Dans **Profil public**:
  - **Etat du pare-feu : Activé** *(1)*.
  - **Connexions entrantes : Bloquer** *(2)*.
  - **Connexions sortantes : Autoriser** *(3)*.
  - Puis **Appliquer** les modifications *(4)*.



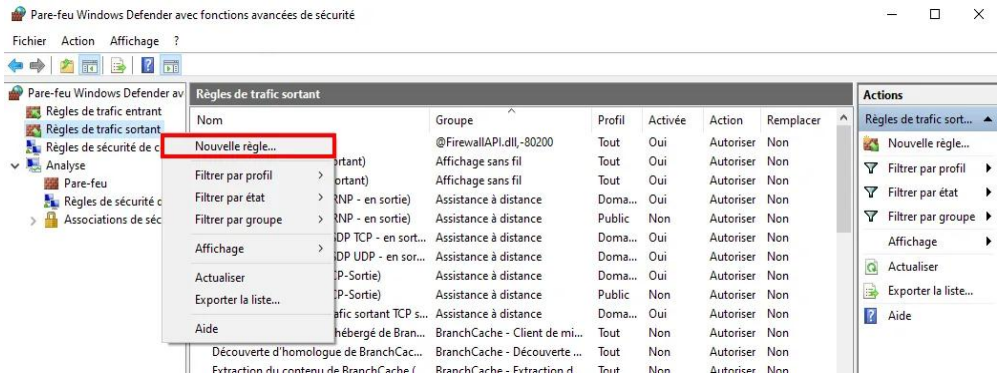
3. Crée des règles pour bloquer des binaires spécifiques (LOLBins)

- Certaines applications légitimes, comme PowerShell, peuvent être exploitées pour des attaques.

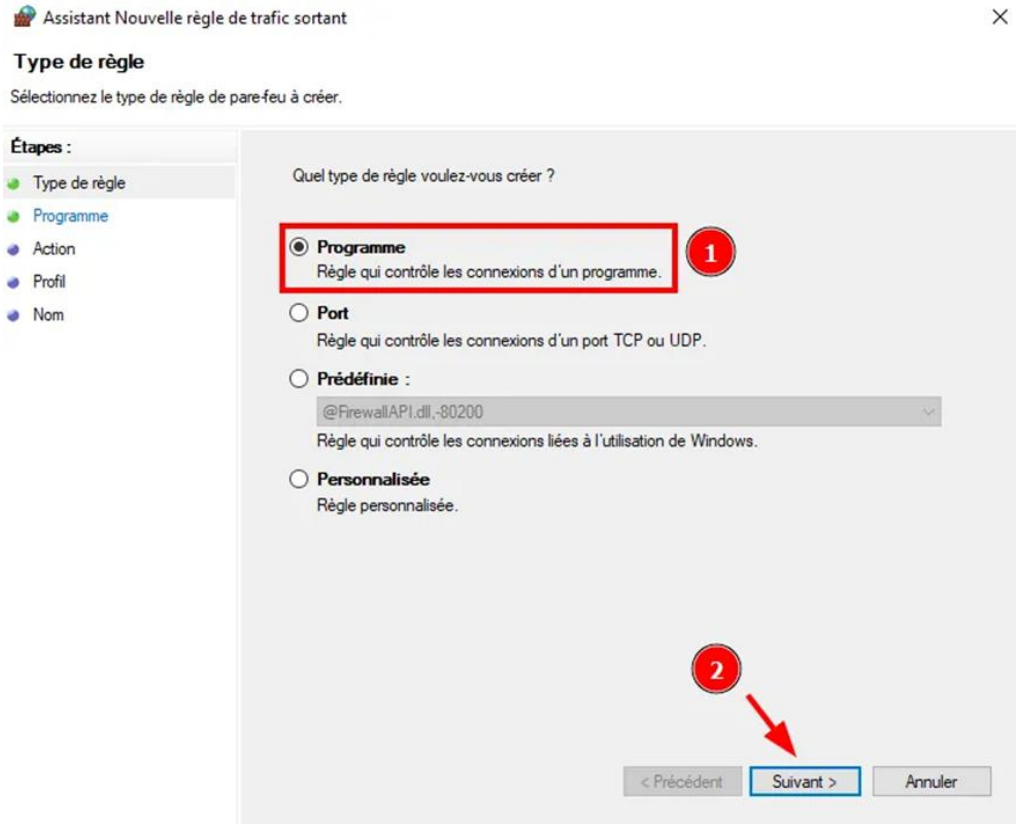
- Accéder aux **règles de sortie:**
  - Dans la fenêtre **Paramètres avancés**, cliquez sur **Règles de trafic sortant**.



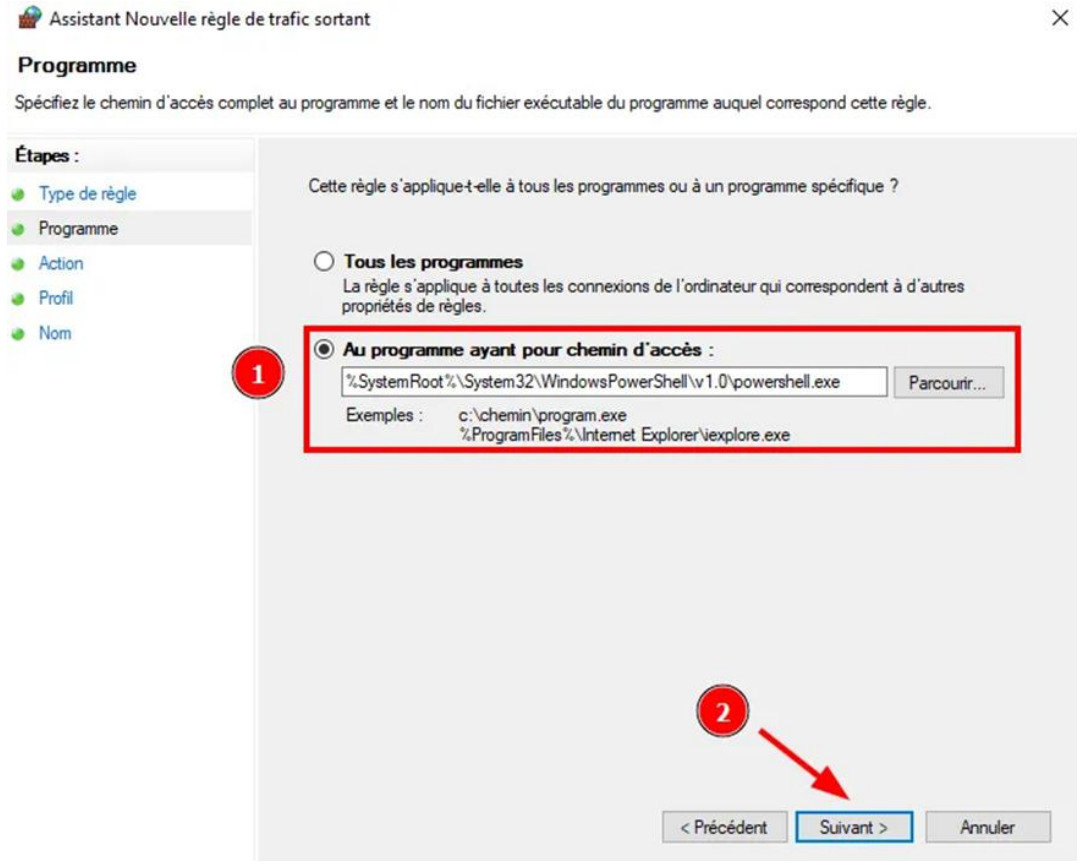
- Créer une **nouvelle règle:**
  - Cliquez sur **Nouvelle règle** dans le volet de droite.



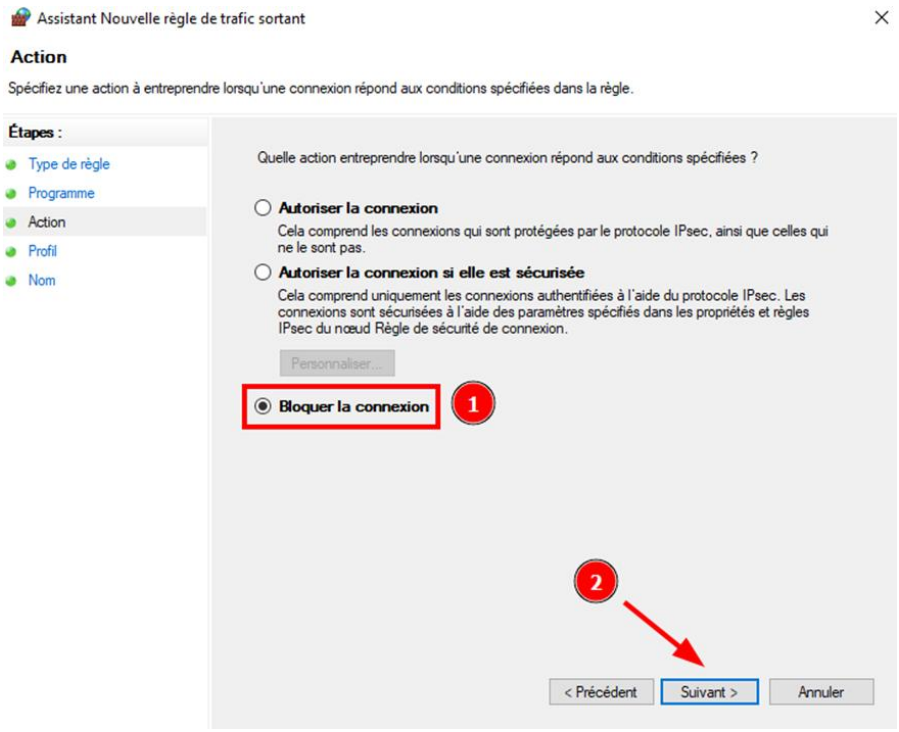
- Sélectionnez **Programme** *(1)*, puis cliquez sur **Suivant** *(2)*.



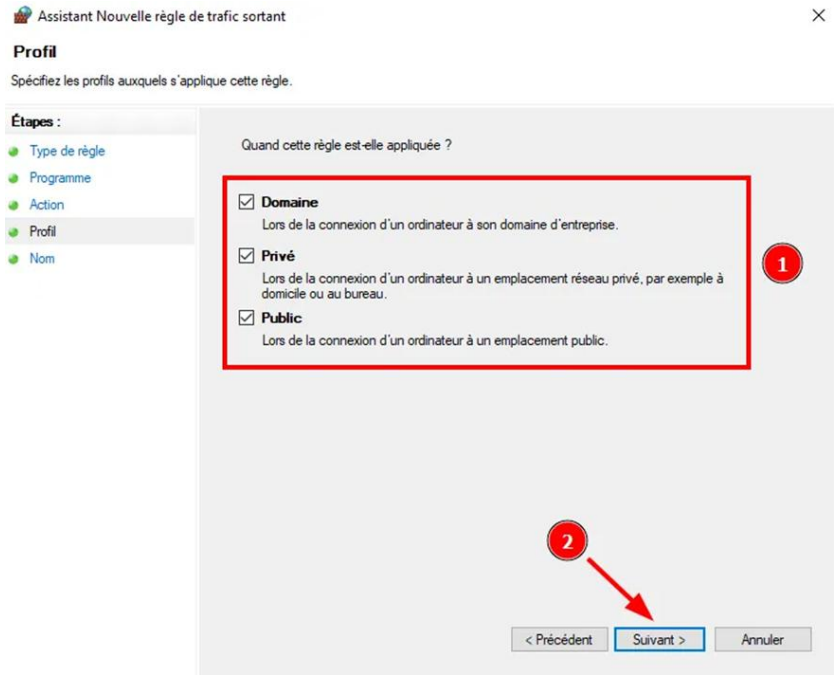
- Naviguez jusqu'au chemin de l'application à bloquer, par exemple *(1)* :
  - `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`
  - Cliquez sur **Suivant** *(2)*.



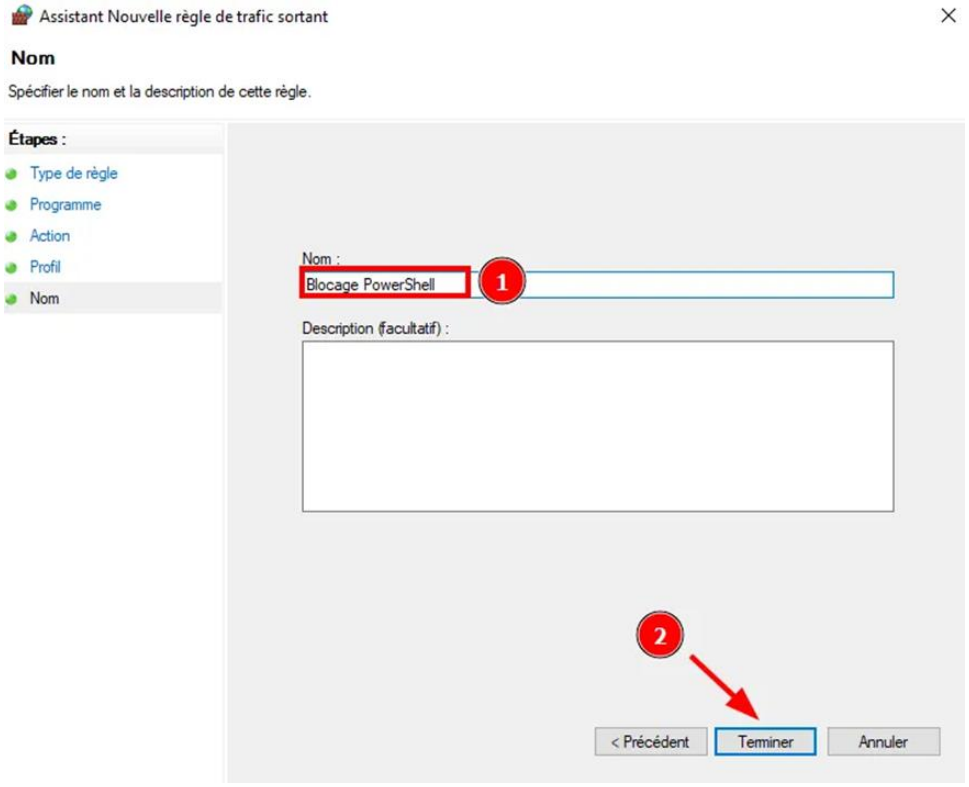
- **S**électionnez **Bloquer la connexion** *(1)* puis **Suivant** *(2)***.**



- Appliquer la **règle:**
  - Choisissez les profils auxquels appliquer la règle (**Domaine, Privé, Public**) *(1)* et faites **Suivant** *(2)*.

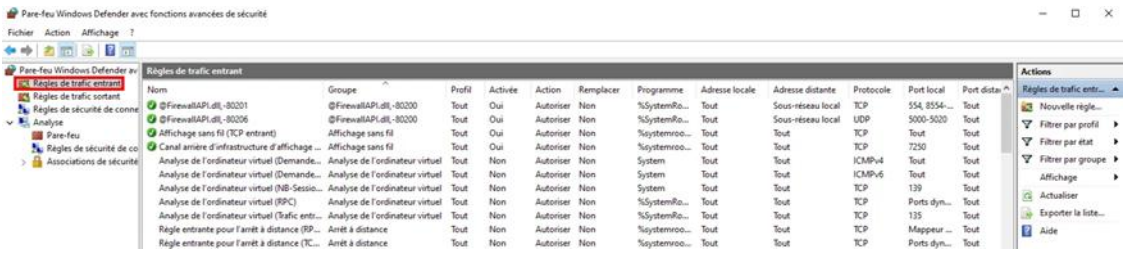


- Donnez-lui un nom explicite, comme **Blocage PowerShell** *(1)* et faites **Terminer** *(2)*.

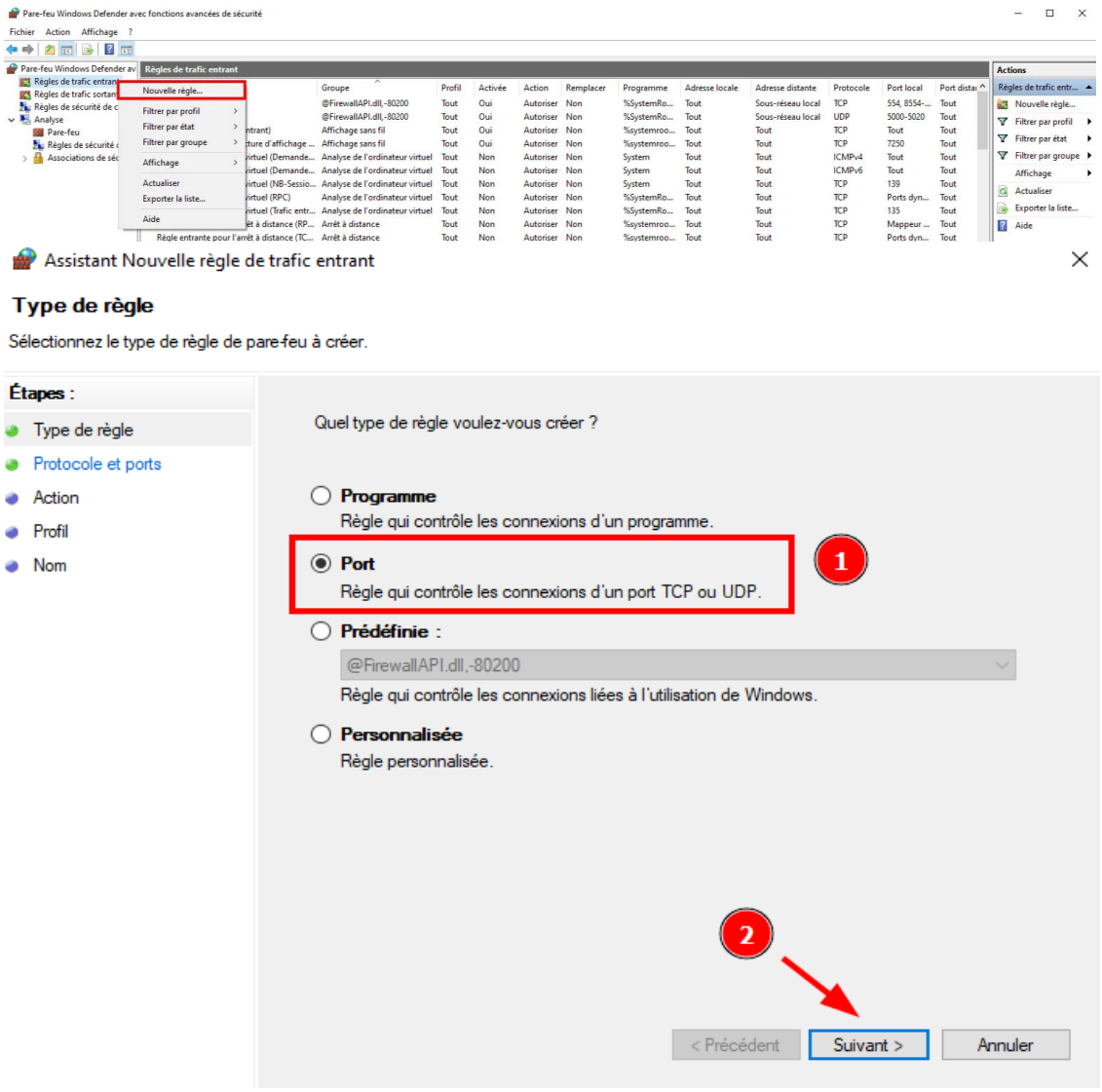


4. Configurer des règles spécifiques pour les ports sensibles

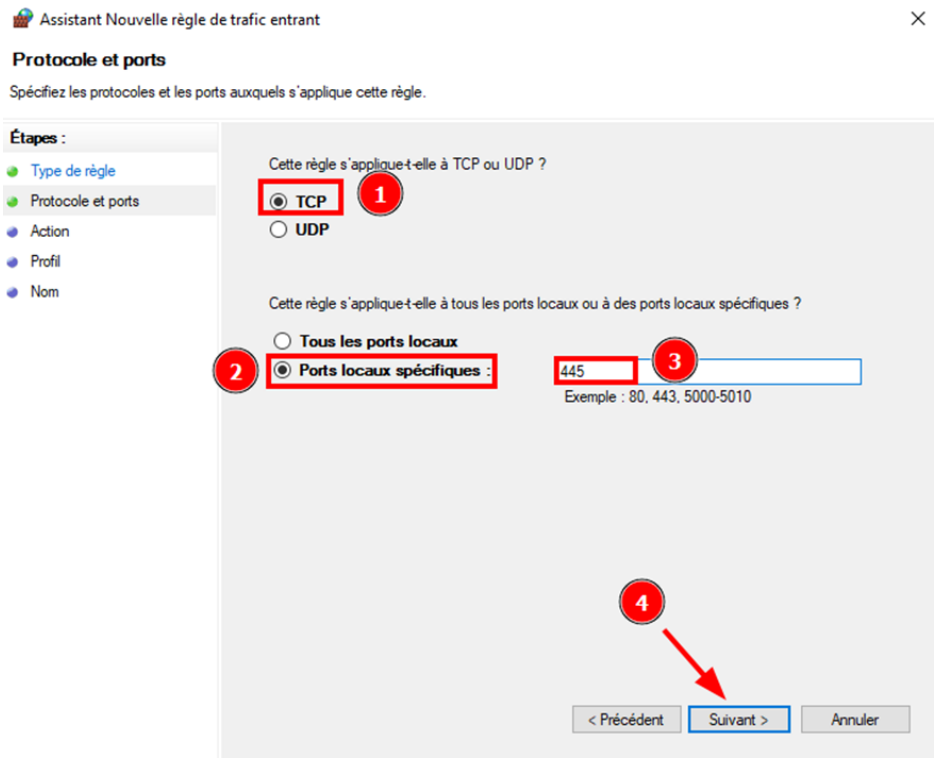
- Bloquer les **ports inutilisés:**
  - Dans **Paramètres avancés**, accédez à **Règles de trafic entrant**



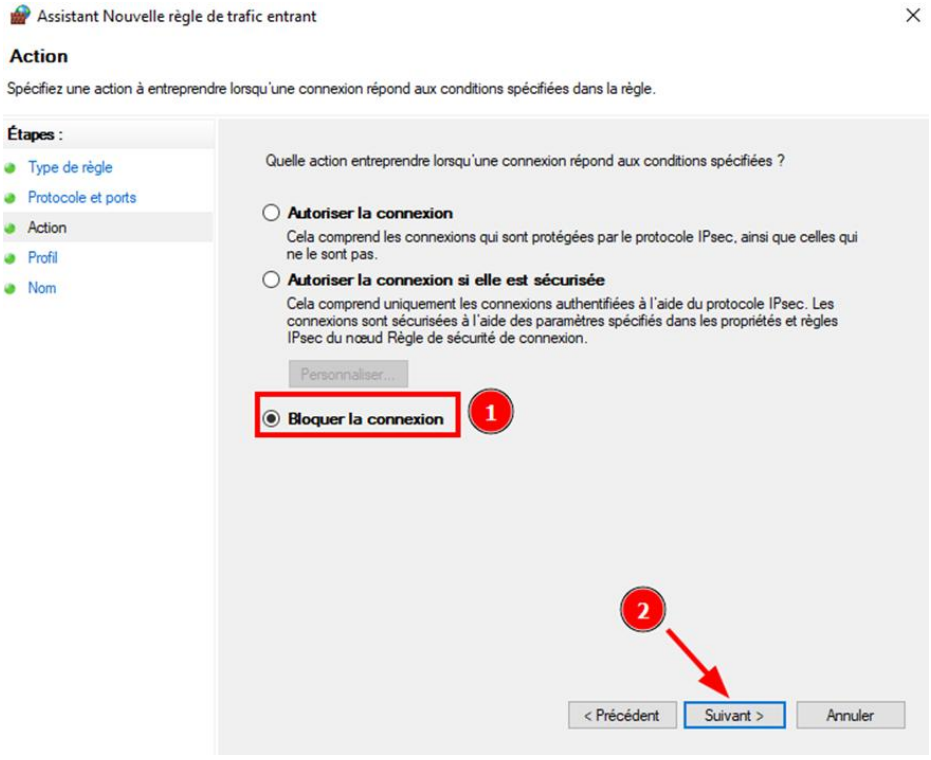
- Créez une nouvelle règle en sélectionnant **Port** *(1)* puis **Suivant** *(2)*.



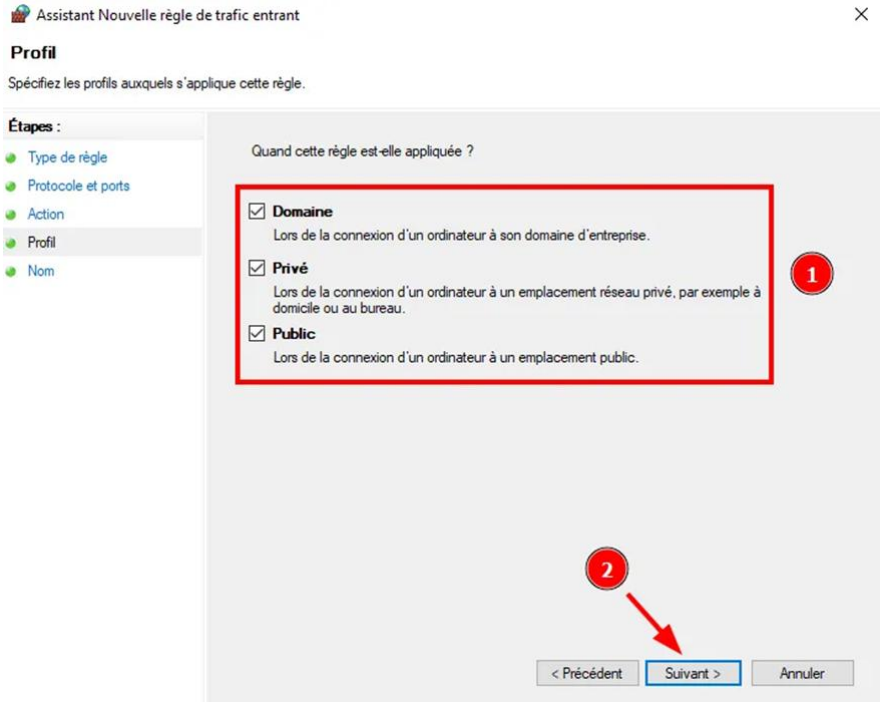
- Spécifiez le **protocol** (TCP ou UDP) *(1)* puis choisissez le **Ports locaux spécifiques** *(2)* et entrez **445** *(3)* comme ports à bloquer (par exemple, 445 pour SMB) puis **Suivant** *(4)*.



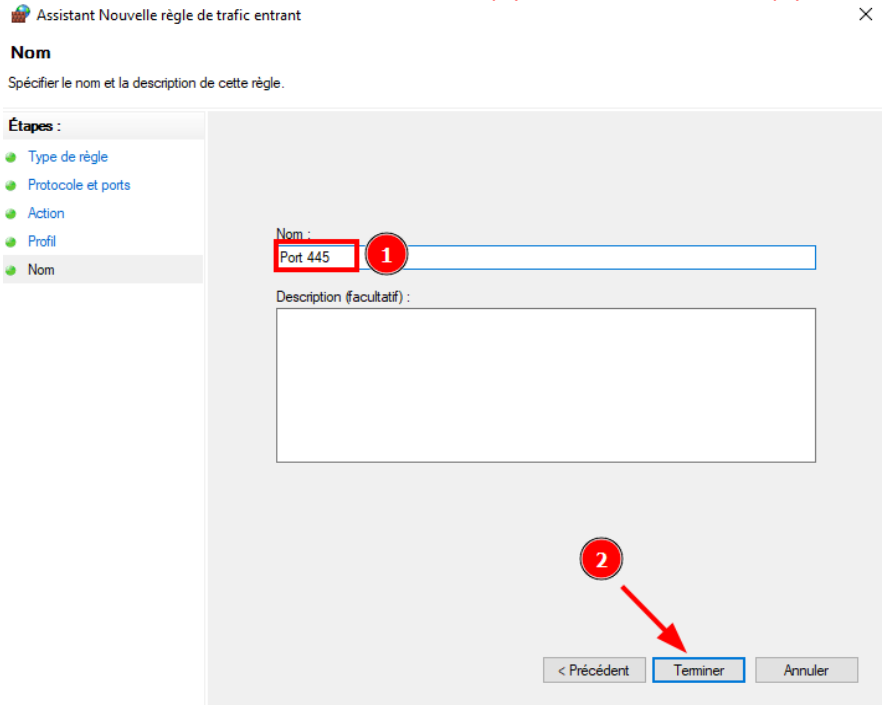
- Sélectionnez **Bloquer la connexion** *(1)* et faite **Suivant** *(2)*.



- Puis cochez **Domaine**, **public** et **privé** *(1)* et faites **Suivant** *(2)*.



- Enfin attribuez comme nom **Port 445** *(1)* et faites **Terminer** *(2)*.



- Suivez le même processus pour ses ports:
  - Autorisez le port 22/tcp (Autorise le SSH)
  - Autorisez le port 443/tcp (Autoriser le HTTPS)
  - Autorisez le port 80/tcp (Autoriser le HTTP)
  - Refusez le port 23/tcp (Refuser Telnet)

5. Tester les configurations

- Simuler une **connexion bloquée:**
  - Essayez d'exécuter PowerShell sur la machine, ou tentez d'accéder à un port bloqué (par exemple, via telnet).
  - Vérifiez que la connexion est bloquée et qu'une notification s'affiche.

- Analyser les **journaux du Pare-feu Windows:**
  - Ouvrez **Visualiseur d'événements > Journaux des applications et des services > Microsoft > Windows > Security-Auditing** pour voir les tentatives bloquées.

6. Pourquoi ces étapes sont importantes ?

- **Pare-feu actif:** Protège contre les connexions non autorisées ou malveillantes.
- **LOLBins:** Bloque les outils souvent utilisés dans des attaques par des pirates.
- **Restrictions des ports:** Réduit la surface d'attaque en limitant les services exposés.

10. Gestion des mises à jour Windows

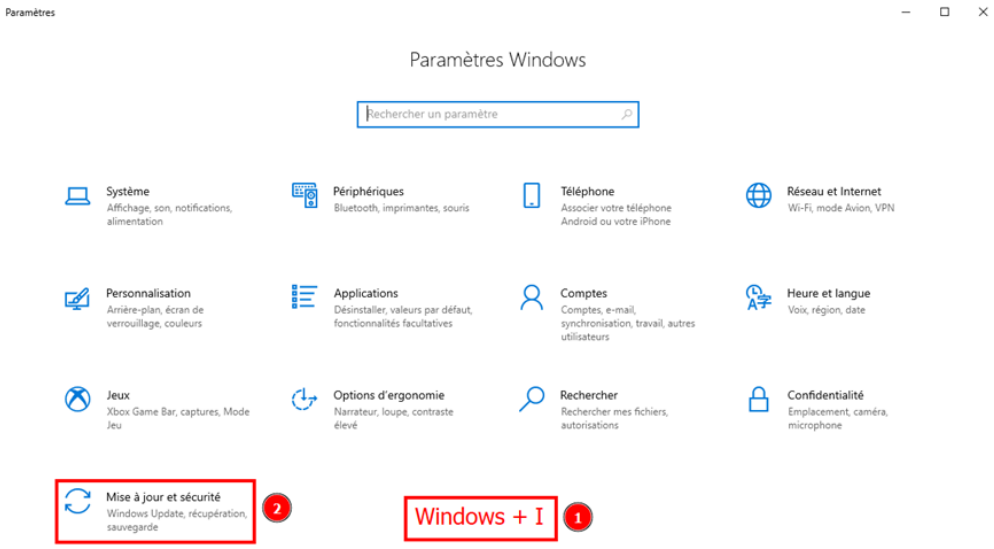
1. Introduction

Dans cette étape, nous allons activer les mises à jour automatiques de Windows pour maintenir le système à jour.

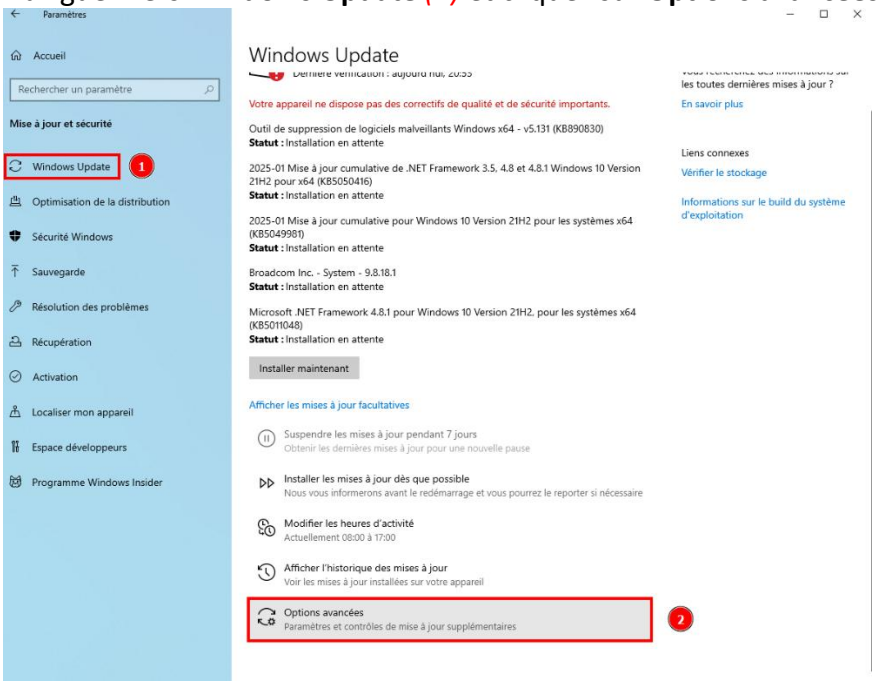
2. Activer les mises à jour automatiques

- Les mises à jour automatiques garantissent que toutes les vulnérabilités connues sont corrigées.

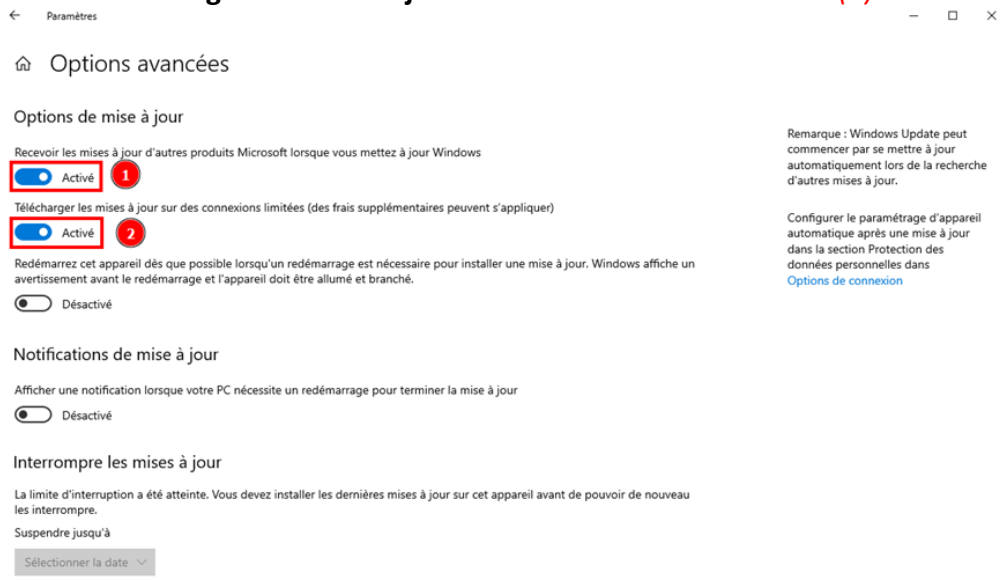
- Configurer via **Paramètres Windows:**
  - Appuyez sur **Win + I** *(1)* pour ouvrir **Mise à jour et sécurité** *(2)*.



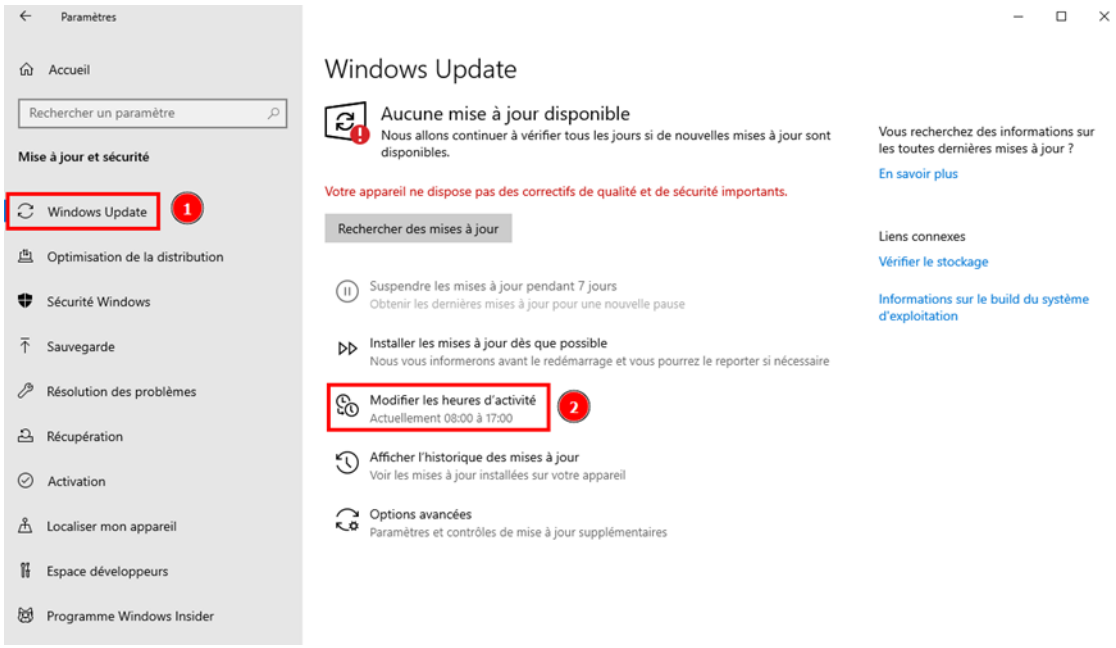
- Naviguez vers **Windows Update** *(1)* et cliquez sur **Options avancées** *(2)*.



- Activez les paramètres suivants :
  - Activez **Recevoir des mises à jour pour d'autres produits Microsoft lors de la mise à jour Windows** *(1)*.
  - Activez **Télécharger les mises à jour sur des connexions limitées** *(2)***.**

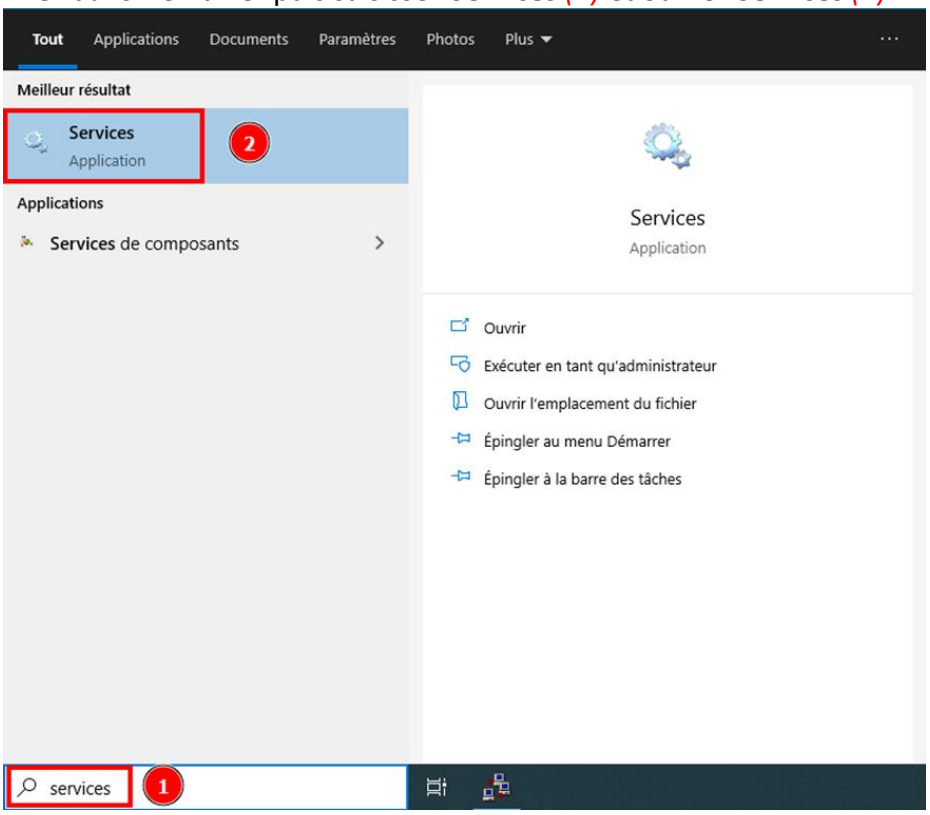


- Configurer les **heures actives:**
  - Allez dans → **Windows Update** *(1)* puis cliquez sur **Modifier les heures d'activités** *(2)*.

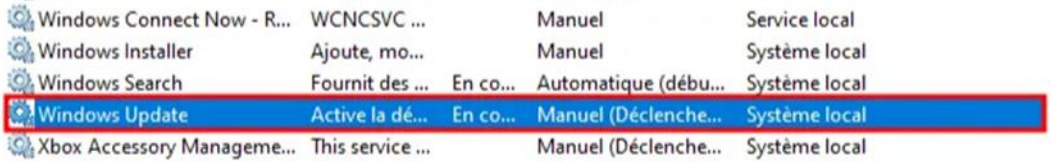


- Définissez une plage horaire pendant laquelle le système ne redémarrera pas automatiquement pour installer des mises à jour.
    - Cliquez sur **Modifier** *(1)*, puis mettez Heure de début **8 Heures** *(2)* et Heure de fin **17 Heures** *(3)*. Enfin cliquez sur **Enregistrer** *(4)*.

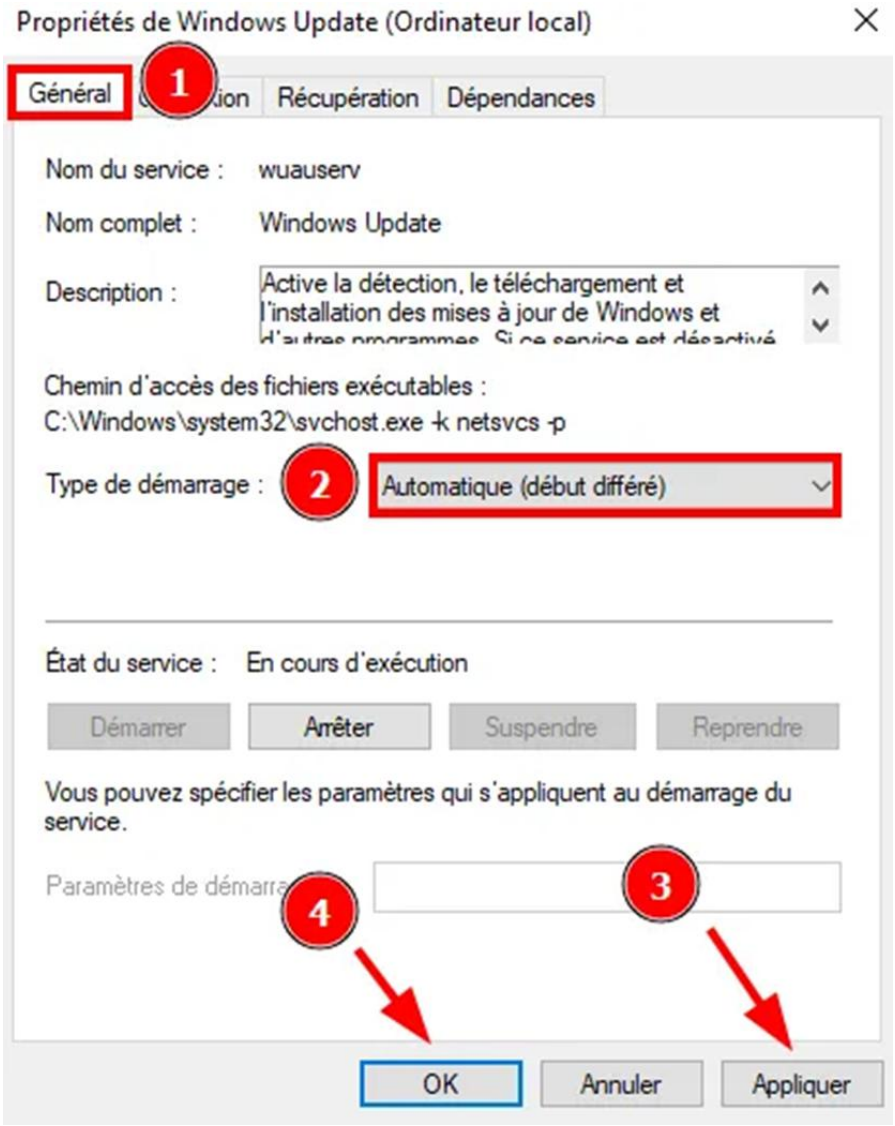
- Allez dans Démarrer puis saisissez **Services** *(1)* et ouvrez **Services** *(2)*.



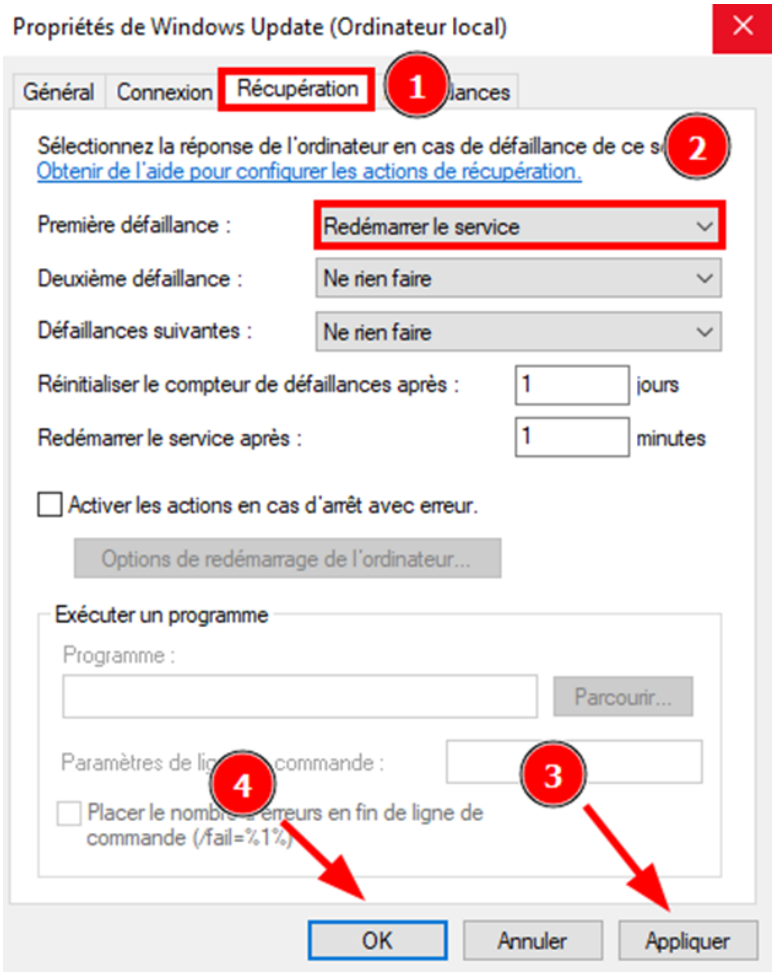
- Double-cliquez sur **Windows Update** dans la fenêtre **Services** qui s'affiche.



- Dans **Général** *(1)*, réglez **Type de démarrage** (Startup type) sur **Automatique** *(2)* (démarrage différé) (Automatic (Delayed Start)), faites **Appliquer** *(3)* et **OK** *(4)*.



- Cliquez sur **Récupération** *(1)* (Recovery), réglez **Premier échec** (First failure) sur **Redémarrer le service** *(2)* (Restart service) faites **Appliquer** *(3)* et **OK** *(4)*.



3. Vérifier les configurations

- Vérifier les **mises à jour Windows:**
  - Revenez à **Paramètres > Mise à jour et sécurité > Windows Update**.
  - Cliquez sur **Rechercher des mises à jour** pour confirmer que les mises à jour automatiques fonctionnent.

4. Pourquoi ces étapes sont importantes ?

- **Mises à jour automatiques:** Garantissent que le système reste protégé contre les nouvelles menaces.

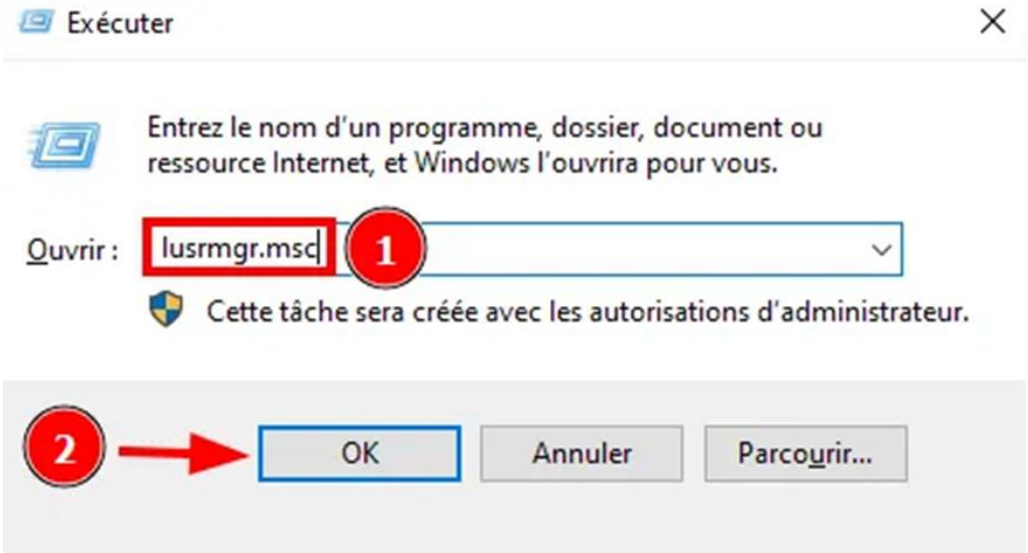
11. Création d'un utilisateur standard pour la mise en production

1. Introduction

- Dans cette étape, nous allons remplacer l'utilisation du compte administrateur par un **compte utilisateur standard**, ce qui réduit les risques de sécurité et suit les **bonnes pratiques de déploiement**.

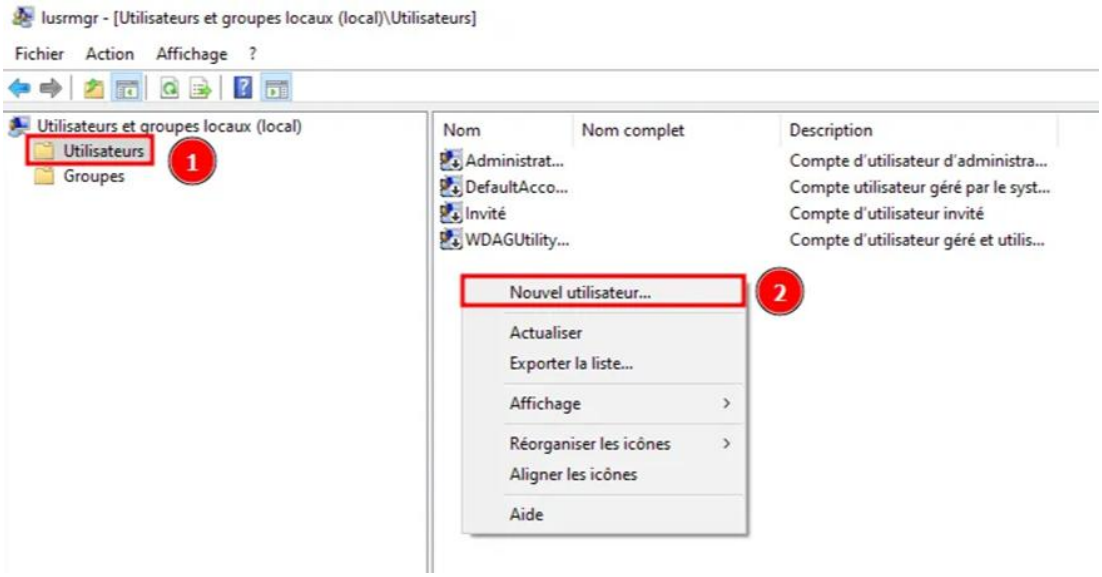
2. Accéder à la gestion des utilisateurs

- Appuyez sur **Win + R**, tapez **lusrmgr.msc** *(1)*, et appuyez sur **OK** *(2)*.

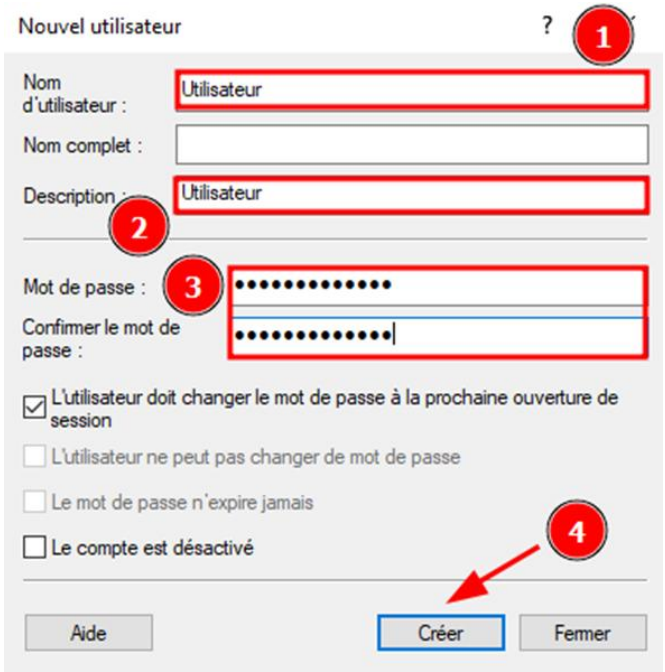


3. Ajouter un nouvel utilisateur standard

- Allez dans → **Utilisateurs** *(1)*, puis faites un clique droit et cliquez sur **Nouvel utilisateur…** *(2)*.

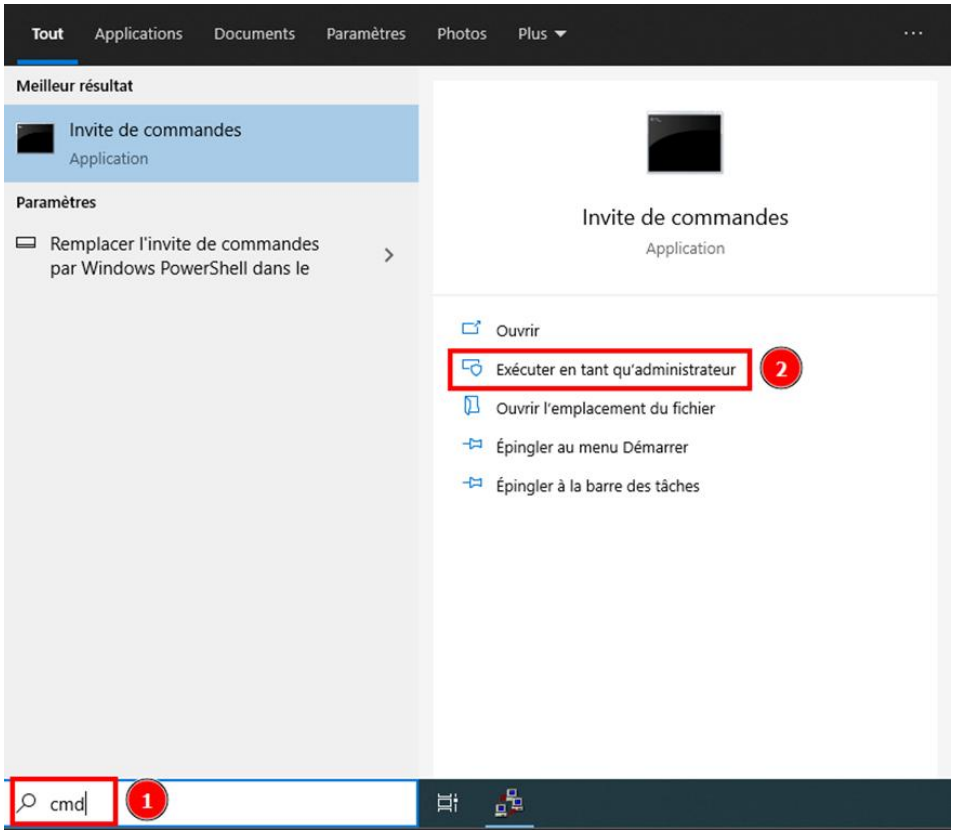


- Dans la fenêtre qui s'ouvre :
  - Choisissez un **Nom d'utilisateur** *(1)*, et mettez une **Description** *(2)* pour détailler l'utilité du compte.
  - Puis choisissez un **Mot de passe** et **Confirmer le mot de passe** *(3)*.
  - Enfin, faites **Créer** *(4)*.



4. Renforcer le mot de passe du compte administrateur

- Sécurisez le compte administrateur existant:
  - Ouvrez une **invite de commande** *(1)* en tant qu'**Administrateur** *(2)*.



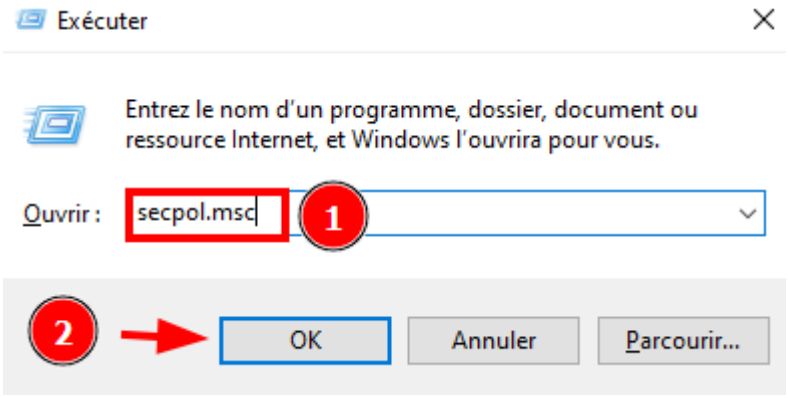
- Tapez la commande suivante pour changer le mot de passe :

```
net user [Nom] NouveauMotDePasseFort
```

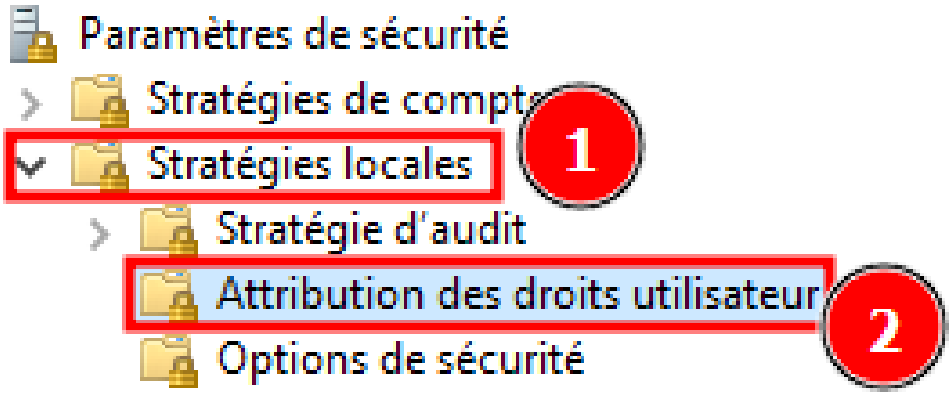
```
PS C:\Windows\system32> net user Windows_AP1 CeciEstUnMotDePasse123!
```

5. Changez les règles des utilisateurs

- Appuyez sur **Win + R**, tapez **secpol.msc** *(1)*, et appuyez sur **OK** *(2)*.

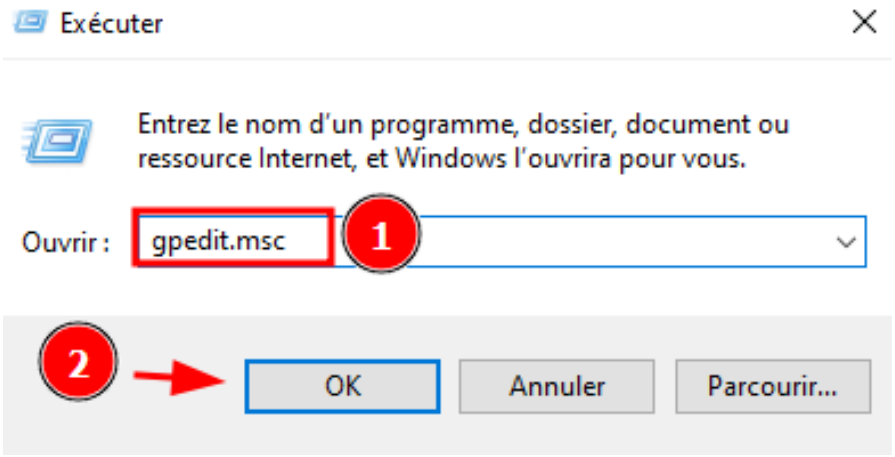


- Allez dans **Stratégies locales** *(1)* → **Attribution des droits utilisateur** *(2)*.

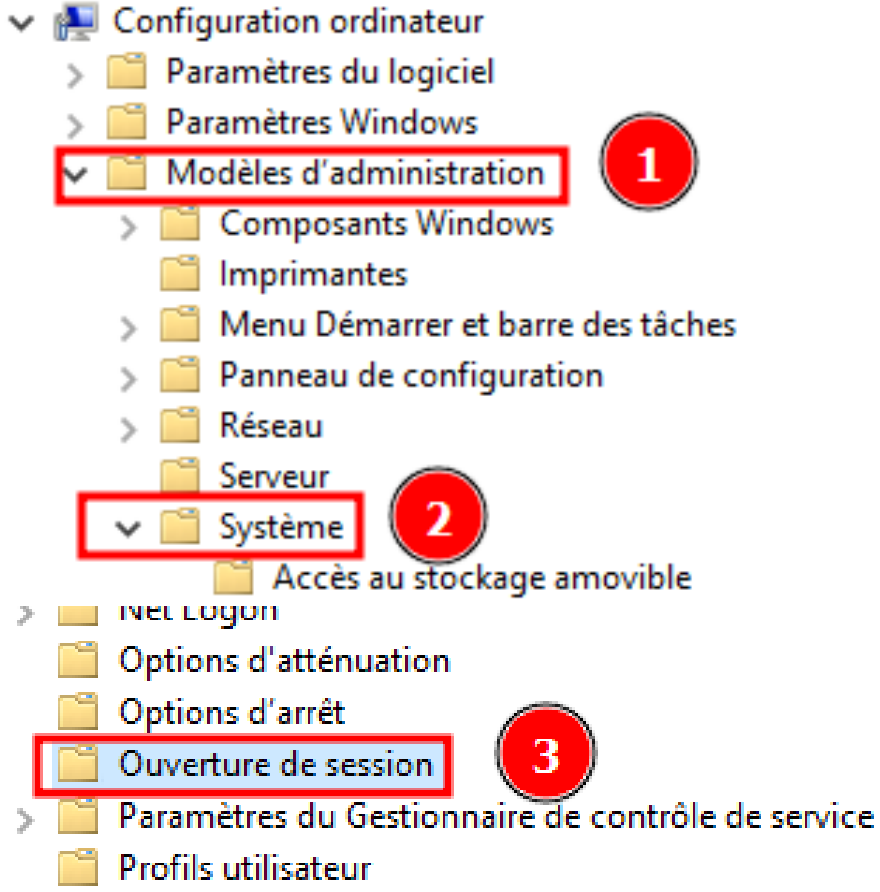


- Changez les paramètres suivants :
    - Accéder à cet ordinateur à partir du réseau : **Administrateurs, Utilisateurs authentifiés**.
    - Créer des liens symboliques : **Administrateurs**.
    - Permettre l'ouverture d'une session locale : **Administrateurs, Utilisateurs authentifiés**.
    - Interdire l'ouverture d'une session locale : **Invité, SERVICE LOCAL.**

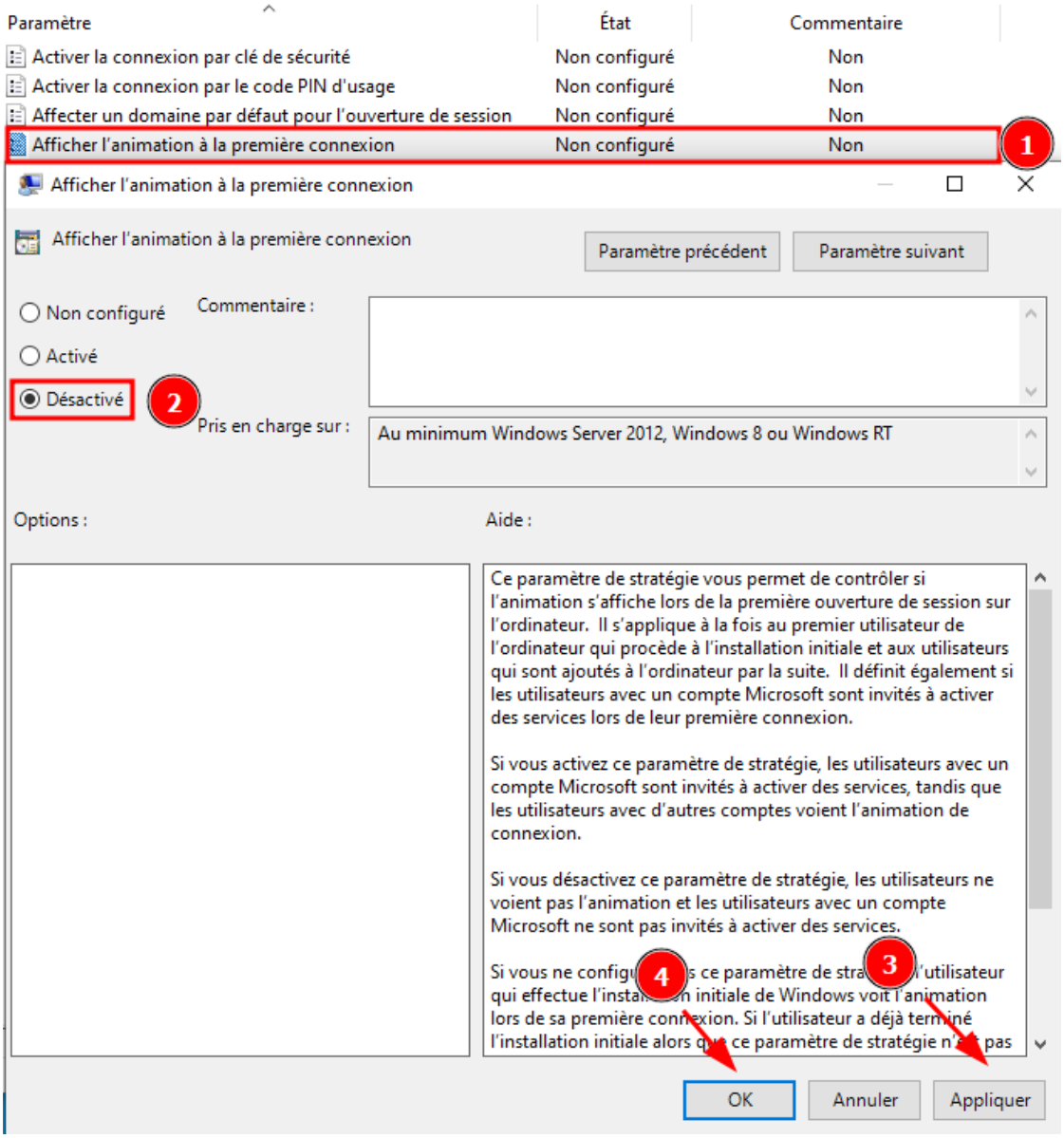
- Appuyez sur **Win + R**, tapez **gpedit.msc** *(1)*, et appuyez sur **OK** *(2)*.



- Allez dans → **Modèles d'administration** *(1)* → **Système** *(2)* → **Ouverture de session** *(3)*.

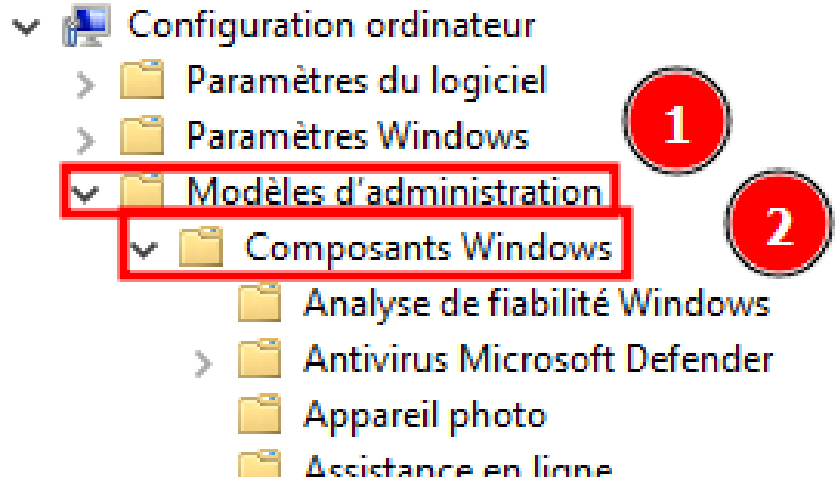


- Puis cliquez sur **Afficher l'animation à la première connexion** *(1)* puis faites **Désactivé** *(2)* enfin **Appliquer** *(3)* et **OK** *(4)*.

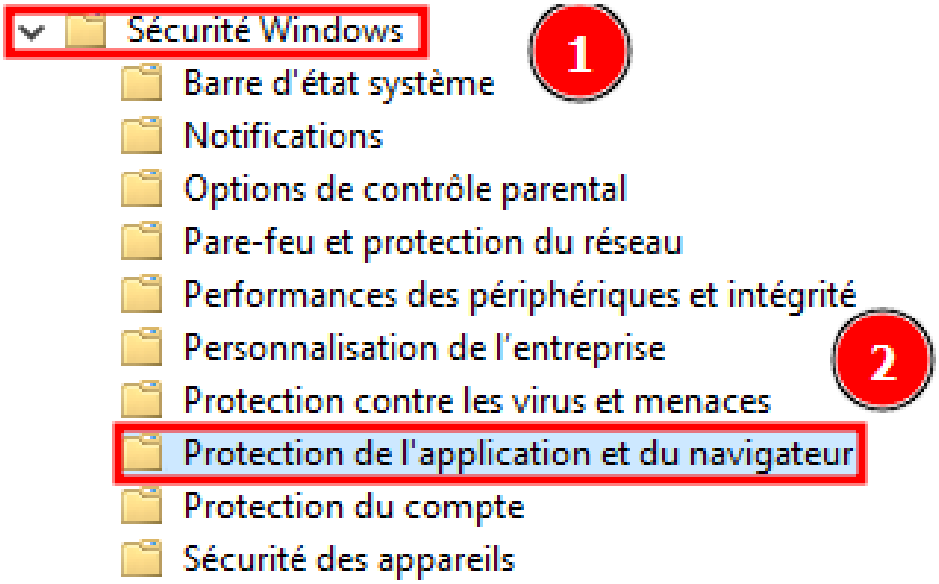


- Faites la même chose pour les **options** suivantes :
  - Afficher l'animation à la première connexion : **Désactivé**.
  - Désactiver le son de démarrage de Windows : **Désactivé**.
  - Désactiver les notifications des applications sur l'écran de verrouillage : **Désactivé**.
  - Afficher un arrière-plan d'ouverture de session clair : **Activé**.
  - Empêcher l'utilisateur d'afficher les détails du compte à la connexion : **Activé**.

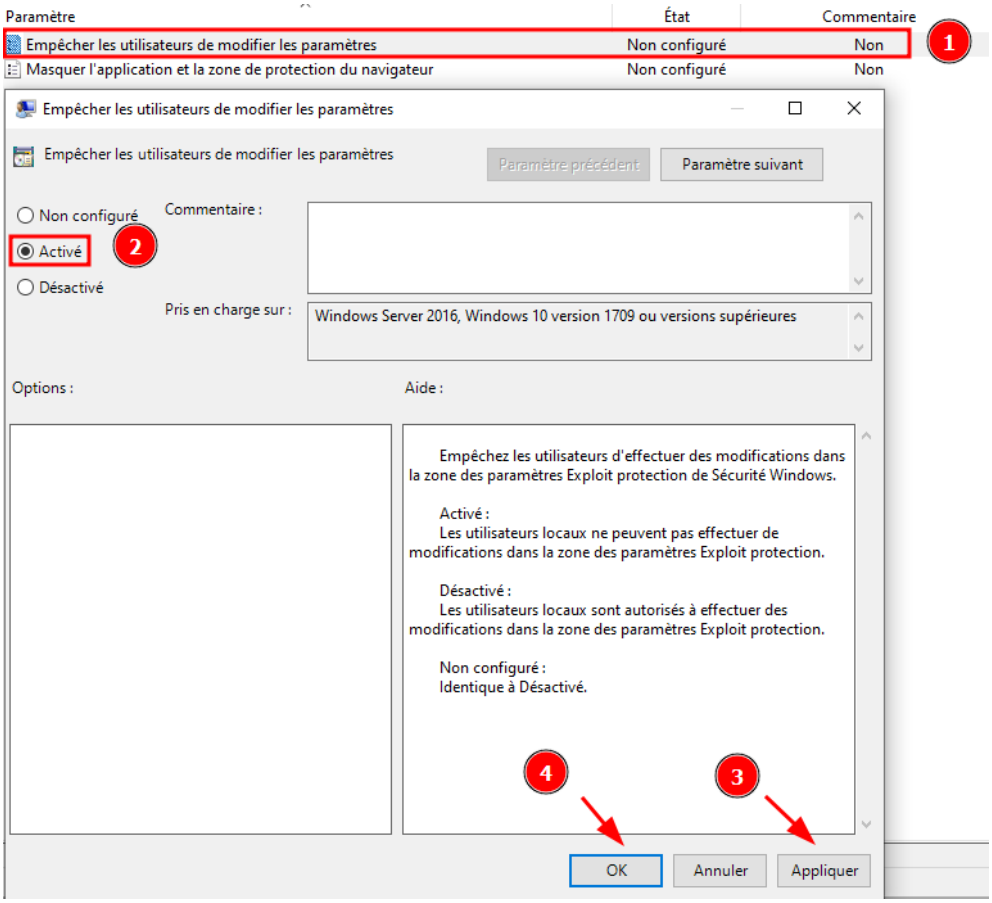
- Toujours dans le **gpedit.msc,** allez dans → **Modèles d'administration** *(1)* → **Composants Windows** *(2)*.



- Puis dans → **Sécurité Windows** *(1)* → **Protection de l'application et du navigateur** *(2)*.



- Puis cliquez sur **Empêcher les utilisateurs de modifier les paramètres** *(1)* puis faites **Activé** *(2)* enfin **Appliquer** *(3)* et **OK** *(4)*.



- Toujours dans le **gpedit.msc,** allez dans → **Modèles d'administration** → **Composants Windows → Contenu cloud,** puis activez les paramètres suivants :
    - Désactiver le contenu optimisé pour le cloud : **Activé**.
    - Désactiver les expériences consommateur de Microsoft : **Activé**.

6. Test du nouvel utilisateur

- Déconnectez-vous du compte administrateur:
    - Appuyez sur **Ctrl + Alt + Suppr** et choisissez **Se déconnecter**.

- Connectez-vous avec le **nouvel utilisateur standard** pour vérifier:
    - Que les configurations appliquées dans les étapes précédentes (pare-feu, Defender, désactivation des services) sont toujours en place.

- Que l'utilisateur n'a **pas de droits administratifs** (par exemple, tentez d'installer une application ou d'accéder aux paramètres système avancés).

7. Pourquoi cette étape est importante ?

- **Sécurité accrue:** Utiliser un compte standard limite les risques liés à des actions malveillantes ou accidentelles.
- **Bonnes pratiques professionnelles:** Les utilisateurs finaux n'ont pas besoin de privilèges administratifs.

12. Installation des logiciels pour Windows 10

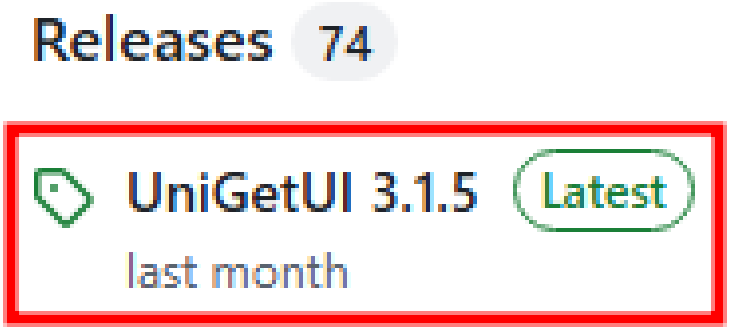
1. Introduction

- Dans cette étape, nous installerons les logiciels nécessaires pour la bureautique ainsi que pour la communication. WingetUI va nous permettre de mettre à jour automatiquement les logiciels que nous installerons plus tard.

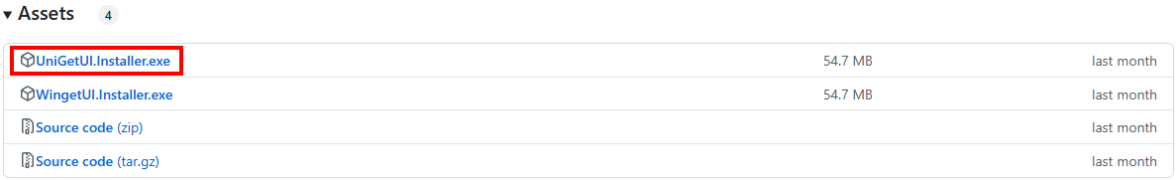
2. Installation de WingetUI

- Allez sur Edge et copié ce lien dans la bar de recherche :
  - https://github.com/marticliment/UnigetUI

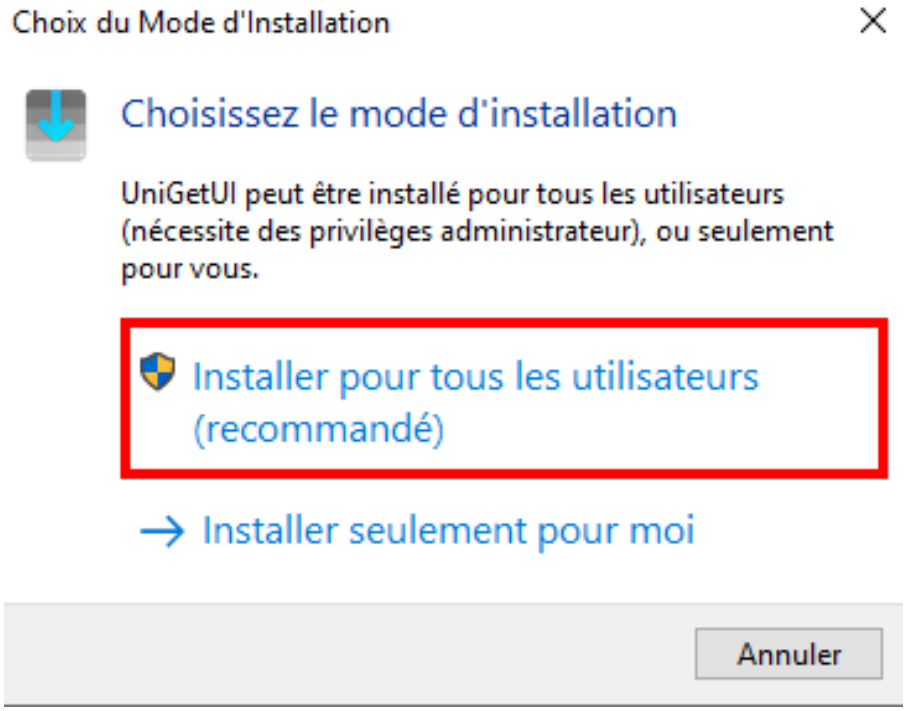
- Descendez jusqu'a que vous ayez à droite **UniGetUI [Version]** et cliquez dessus.



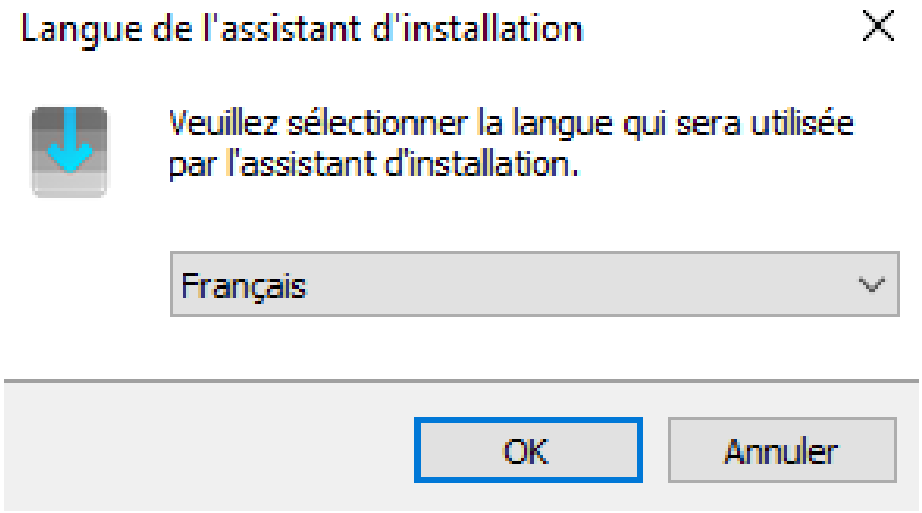
- Ensuite téléchargez le **UniGetUI.Installer.exe.**



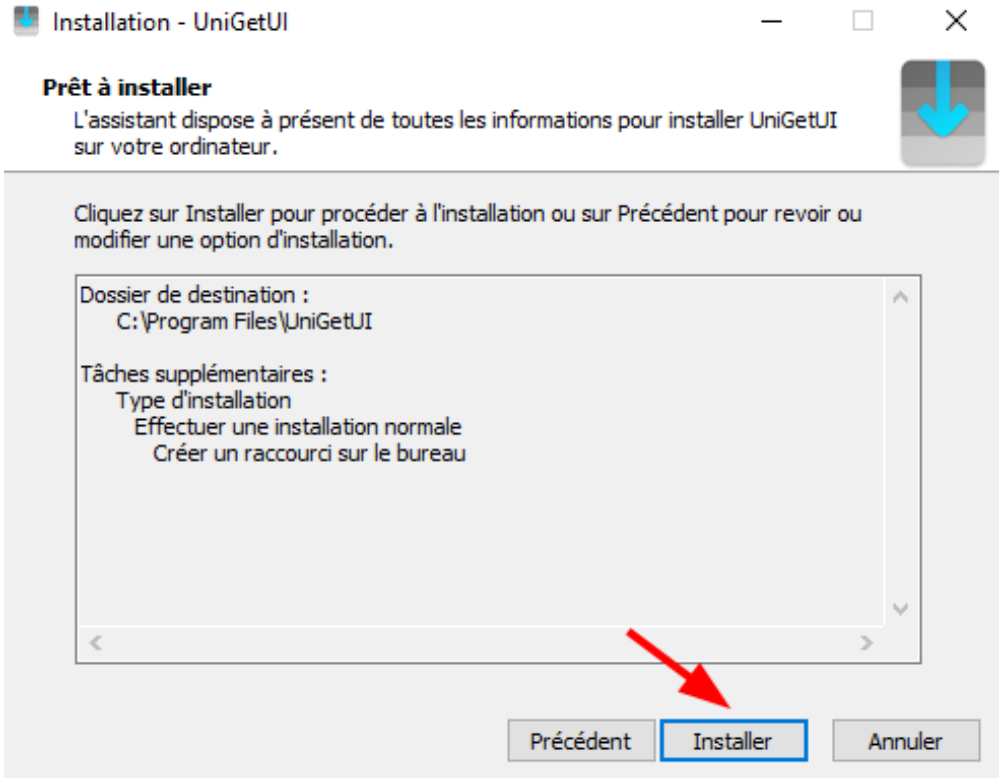
- Et faites **Installer pour tous les utilisateurs (recommandé)**.

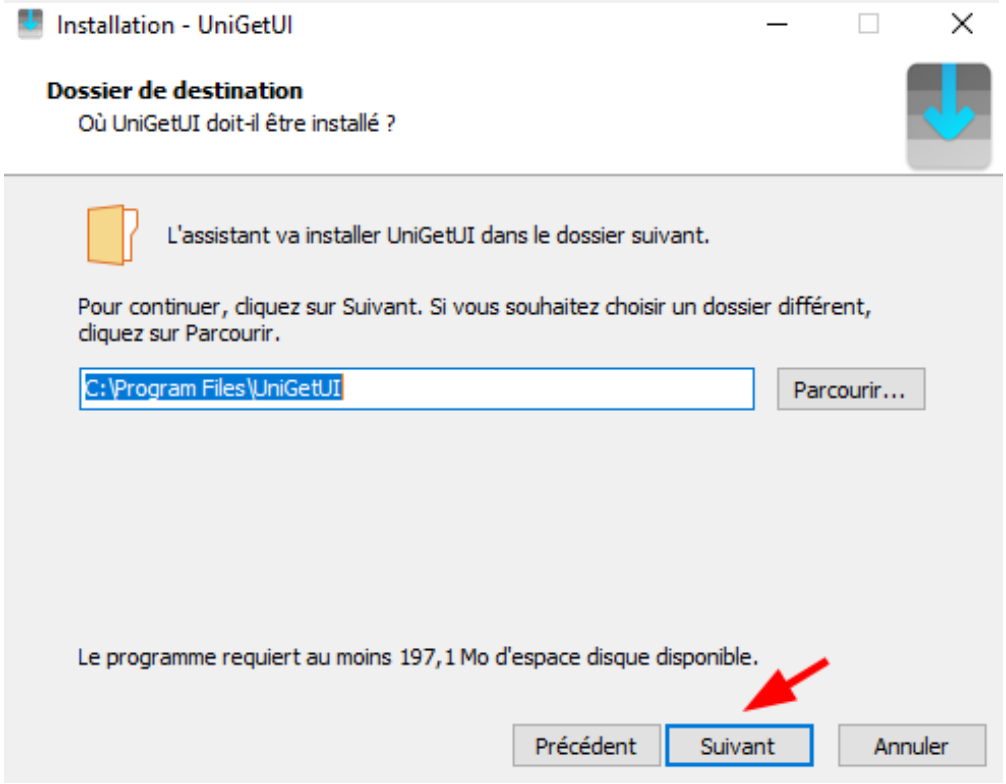


- Choisissez **Français**.

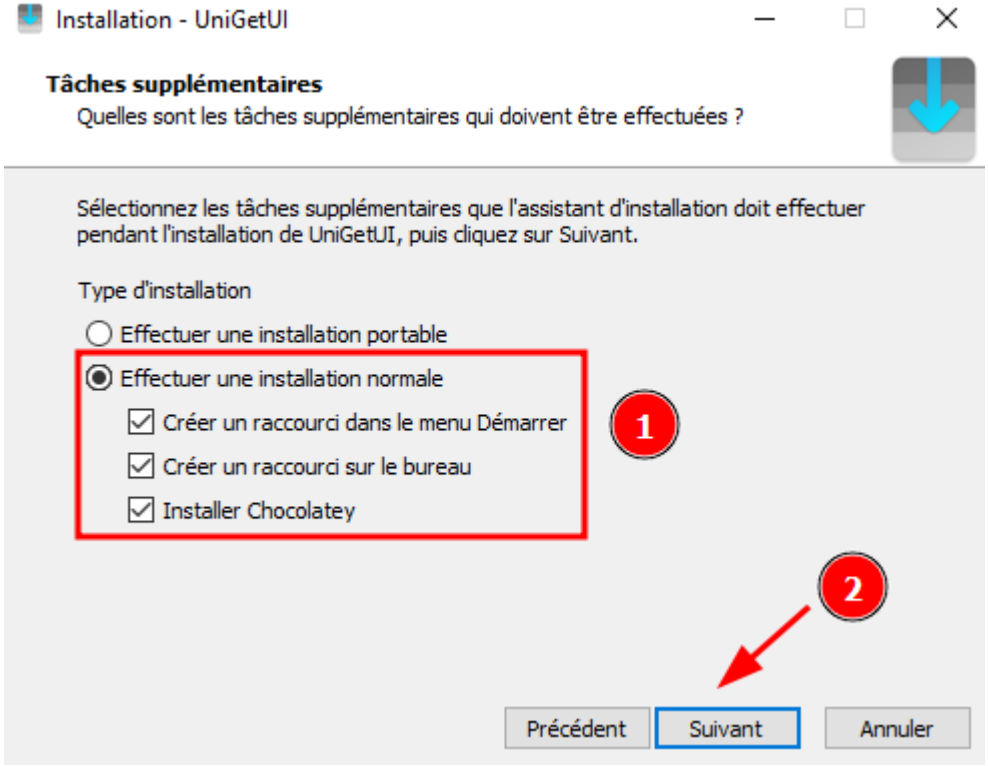


- Puis faites deux fois **Suivant.**





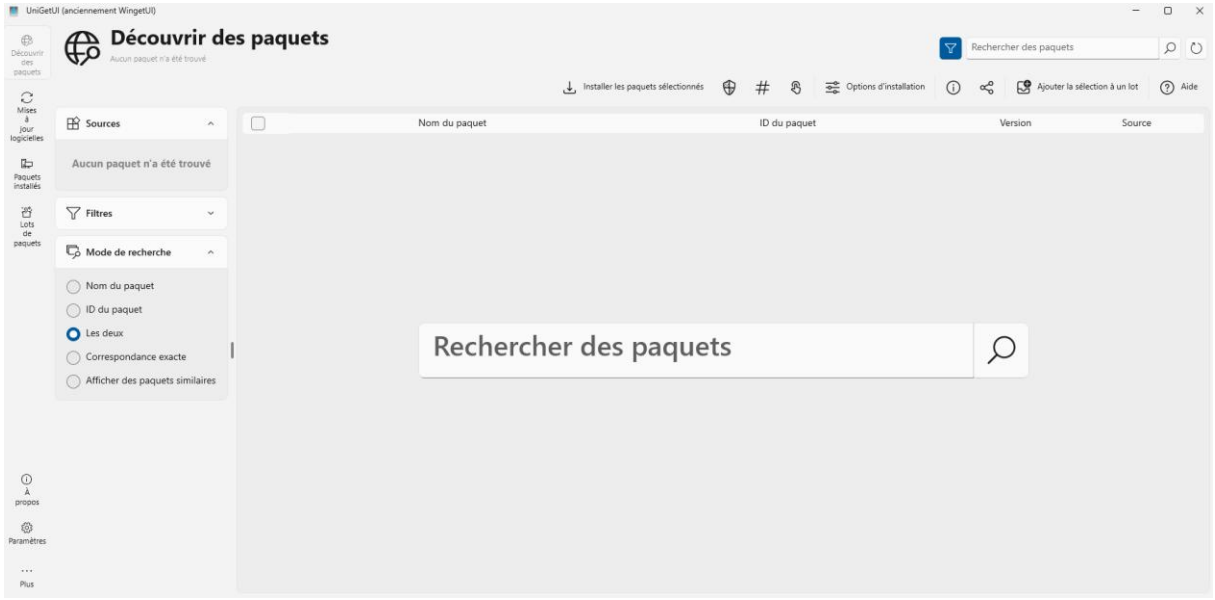
- Arrivez aux **Tâches supplémentaires,** sélectionnés les **cases** *(1)* et faites **Suivant** *(2)*.



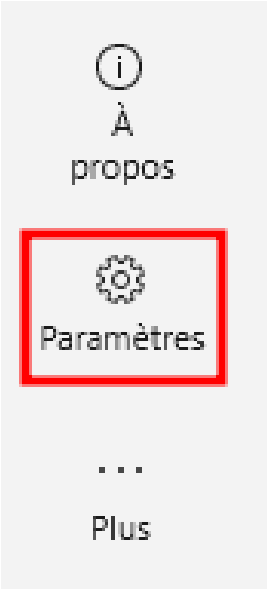
- Puis faites **Terminer.**

3. Activation des mises à jour automatique

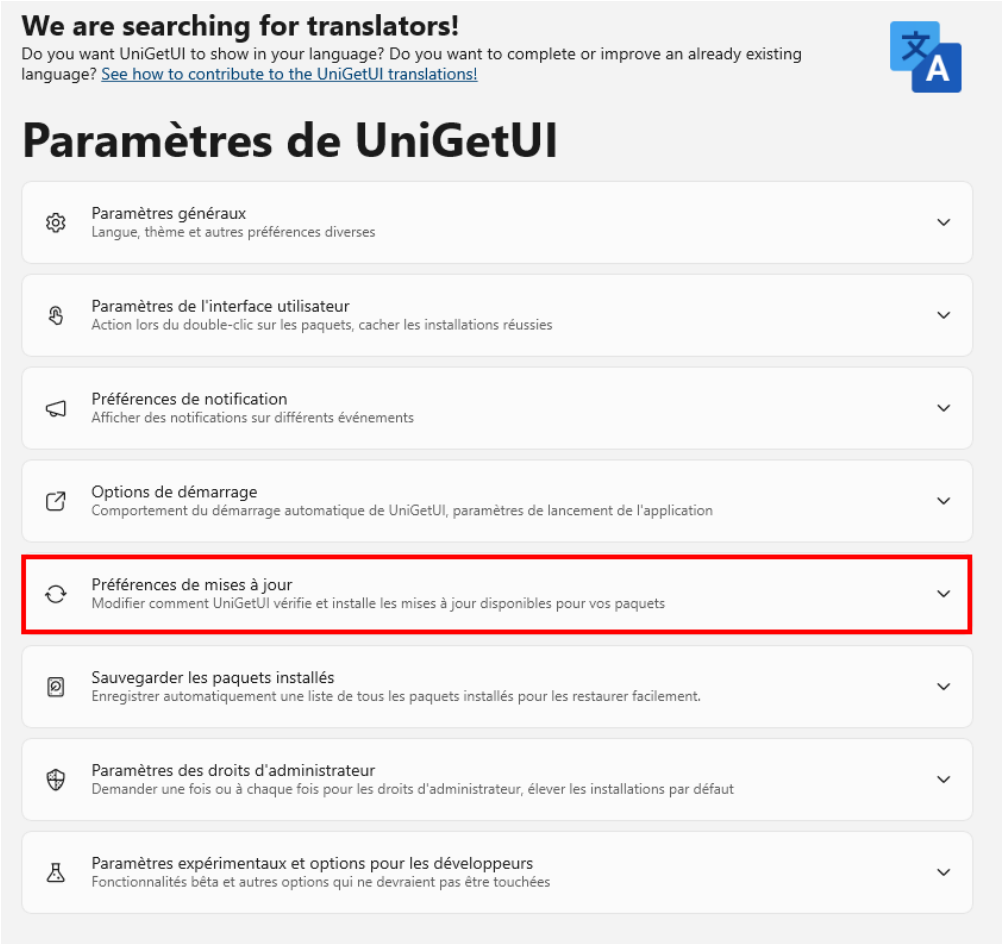
- Bienvenue sur l'interface **UniGetUI,** nous l'utiliserons pour installer et mettre à jour automatiquement les paquets des **logiciels**.



- Allez dans **Paramètres** en bas à gauche.



- Enfin allez dans **Préférences de mise à jour**.



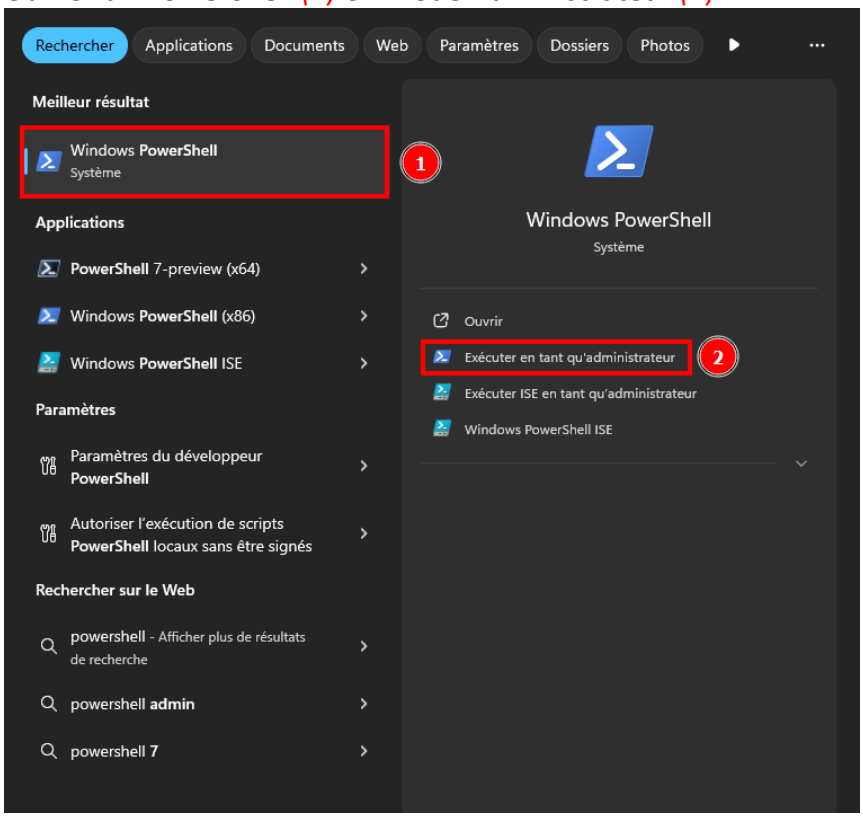
- Cochez les cases suivantes :
  - **Vérifier les mises à jour des paquets périodiquement** *(1)* et mettez **1 jour** *(2)*.
  - **Installer automatiquement les mises à jour disponibles** *(3)*.

4. Installation des logiciels avec Chocolatey

- Pour la partie Bureautique, nous optons pour OnlyOffice, si vous souhaitez télécharger Office 365, il faudra finir cette étape sans télécharger OnlyOffice et regarder la prochaine étape pour celui-ci.

- On va utiliser Chocolatey qui a était installé avec UniGetUI.

- Ouvrez un **PowerShell** *(1)* en **Mode Administrateur** *(2)*.



- Rentrez la commande suivante :

  - choco install OnlyOffice -y
  - choco install VLC -y
  - choco install 7zip -y
  - choco install Okular -y
  - choco install Thunderbird -y

- Ou bien utilisé le script **logiciel_script.ps1.**

5. Pourquoi l'installation de logiciels est importante ?

- **Sécurité renforcée :** Installer des versions à jour et fiables réduit les risques de cyberattaques et garantit la conformité aux normes comme le RGPD.
- **Productivité accrue :** Fournir aux utilisateurs les outils nécessaires optimise leur efficacité pour les tâches professionnelles.
- **Maintenance simplifiée :** Une configuration standardisée facilite les mises à jour et les dépannages en cas de problème.

13. Sécurisation de MS Office

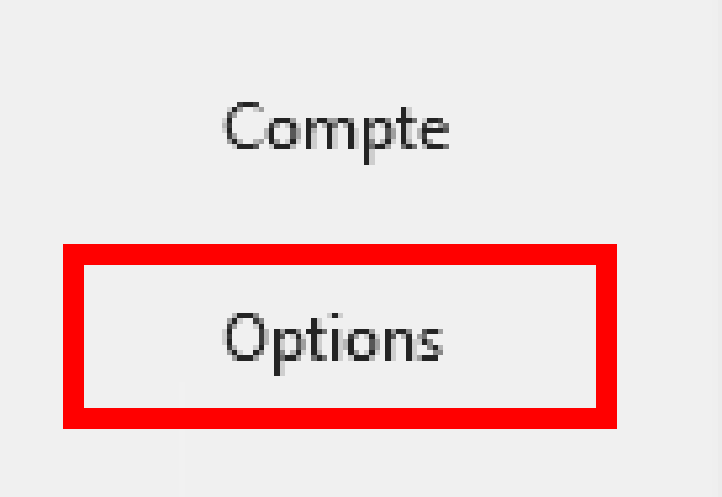
1. Introduction

- Au préalable il faudra télécharger Office 365 avec votre compte Microsoft et installer les applications (Excel, Word, PowerPoint). Puis nous allons configurer Microsoft Office pour protéger les utilisateurs contre les attaques de type malspam (phishing et fichiers malveillants).

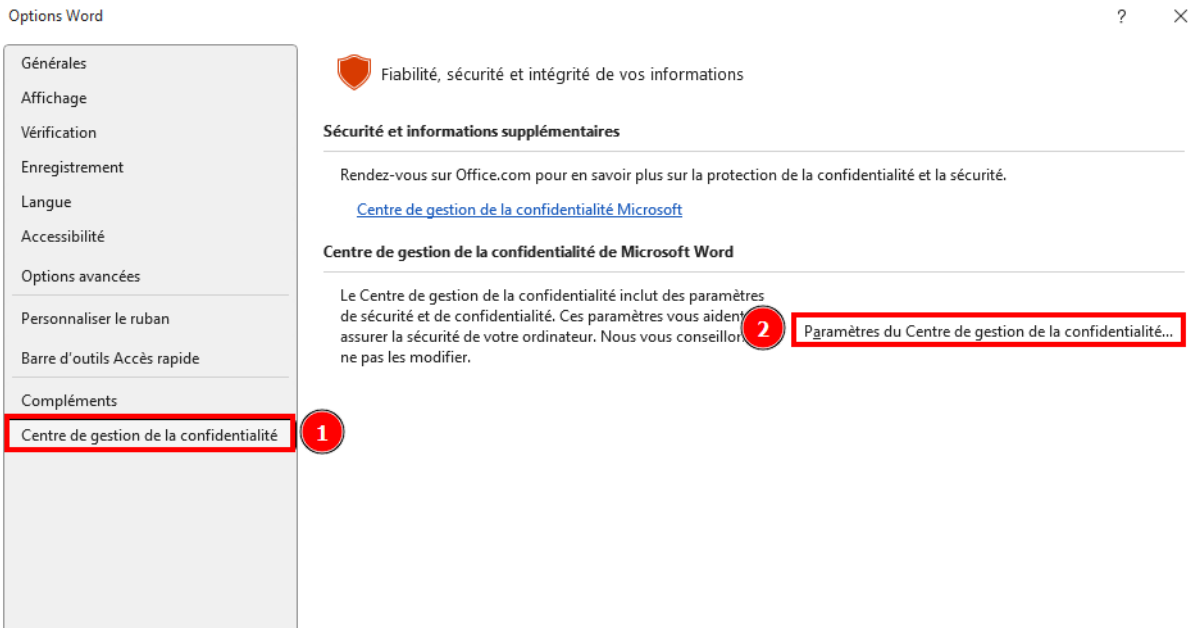
2. Désactiver l'exécution des macros non signées

- Les macros sont souvent utilisées pour exécuter des scripts malveillants.

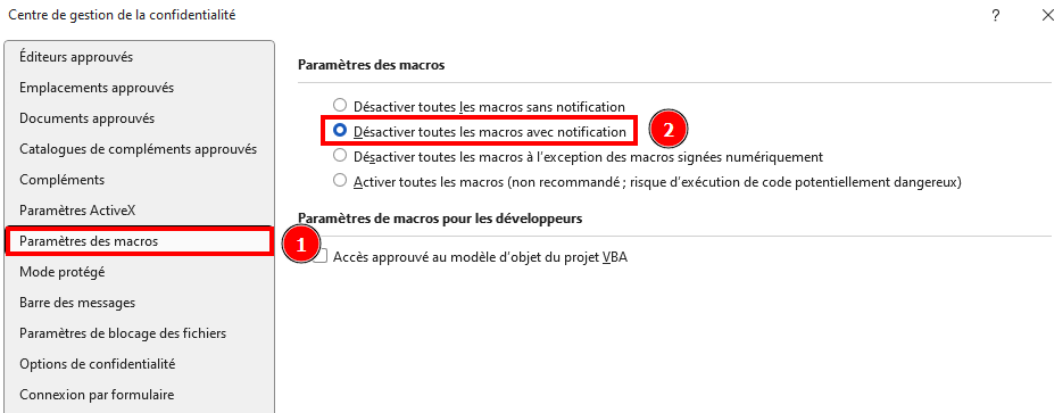
- Lancez une application Office (Word) puis allez dans -> **Option**.



- Puis dans **Centre de gestion de la confidentialité** *(1)*, cliquez sur **Paramètres du Centre de gestion de la confidentialité** *(2)*.



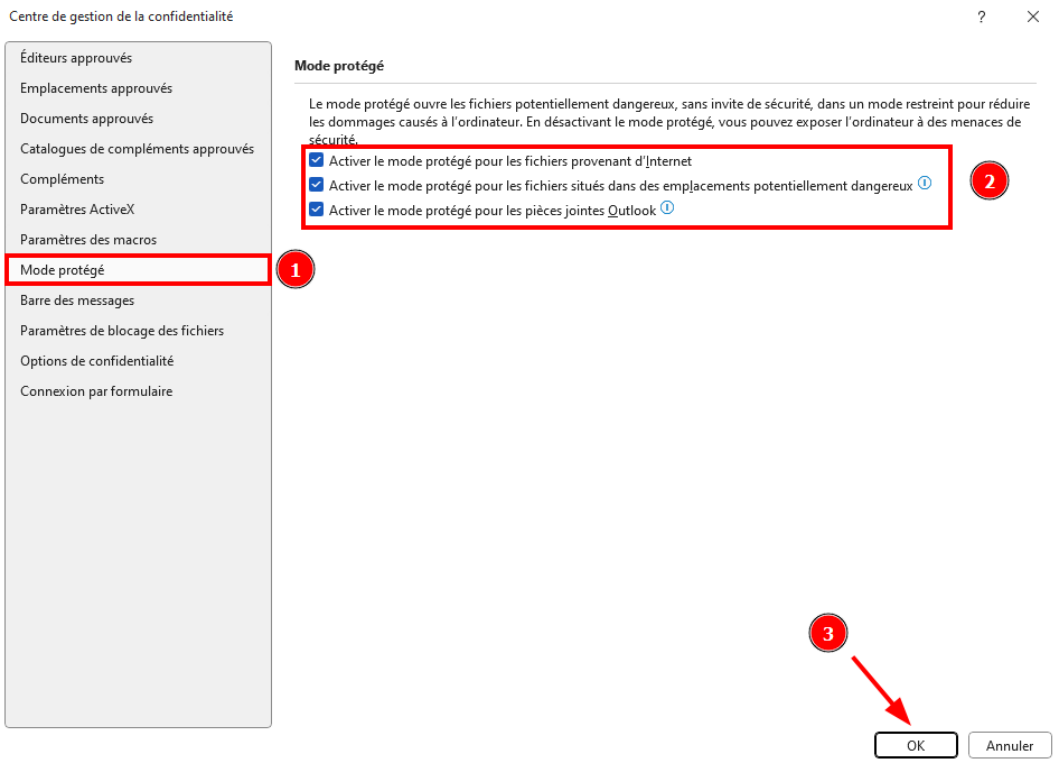
- Configurer les macros :
  - Accédez à **Paramètres des macros** *(1)*.
  - Sélectionnez **Désactiver toutes les macros avec notification** *(2)*.



3. Activer la vue protégée

- La vue protégée ouvre les fichiers dans un mode lecture seule, empêchant l'exécution de scripts malveillants

- Configurer la vue protégée :
    - Toujours dans le Centre de gestion de la confidentialité, cliquez sur **Mode protégé** *(1)*.
    - Cochez toutes les options, notamment :
        - **Activer le mode protégé pour les fichiers provenant d'Internet** *(2)*.
        - **Activer le mode protégé pour les fichiers situés dans des emplacements potentiellement dangereux** *(2)*.
        - **Activer la mode protégée pour les pièces jointes Outlook** *(2)*.
    - Pour finir, faites **OK** *(3)*.

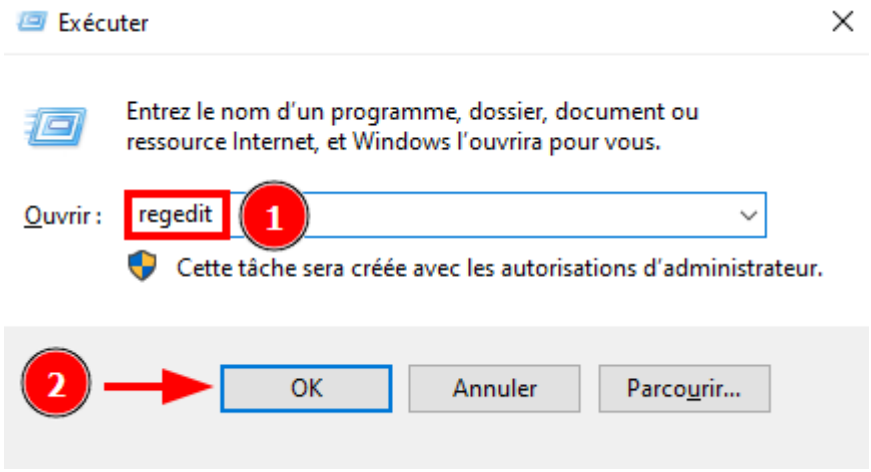


- Répétez ses étapes pour :
    - **PowerPoint**
    - **Excel**

4. Bloquer les fichiers activés dynamiquement

- Certaines fonctionnalités avancées d'Office (comme les liaisons DDE) peuvent être exploitées.

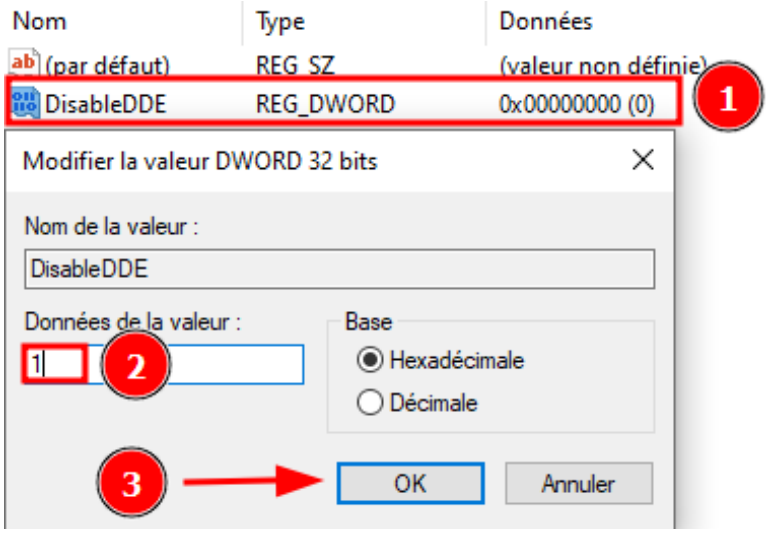
- Désactiver DDE :
  - Appuyez sur **Win + R**, tapez **regedit** *(1)*, puis appuyez sur **OK** *(2)*.



- Accédez à la clé suivante :
  - HKEY_CURRENT_USER\Software\Microsoft\Office\<version>\Word\Security

- Remplacez **<version>** par la version d'Office installée.

- Créez une nouvelle **valeur DWORD (32 bits)** nommée **DisableDDE** *(1)*.
- Attribuez à cette valeur la valeur **1** *(2)* et faites **OK** *(3)*.



- Désactiver DDE pour **Excel** :
  - Répétez les étapes ci-dessus en naviguant à :
    - HKEY_CURRENT_USER\Software\Microsoft\Office\<version>\Excel\Security

- Désactiver DDE pour **PowerPoint** :
  - Répétez les étapes ci-dessus en naviguant à :
    - HKEY_CURRENT_USER\Software\Microsoft\Office\<version>\PowerPoint\Security

5. Tester les protections

- Envoyer un fichier de test malveillant :
  - Vous pouvez utiliser des outils tels que **Gophish** ou des environnements sécurisés pour simuler un malspam.
  - Ouvrez le fichier dans Word ou Excel, et vérifiez que les paramètres empêchent l'exécution automatique.

6. Pourquoi ces étapes sont importantes ?

- **Macros non signées :** Bloquer les macros non vérifiées empêche l'exécution de scripts malveillants.
- **Mode protégée :** Empêche les fichiers non fiables de modifier votre système ou vos données.
- **DDE :** Élimine une vulnérabilité souvent exploitée dans des attaques ciblées.

14. Masterisation du poste Windows 10

1. Activer la vue protégée

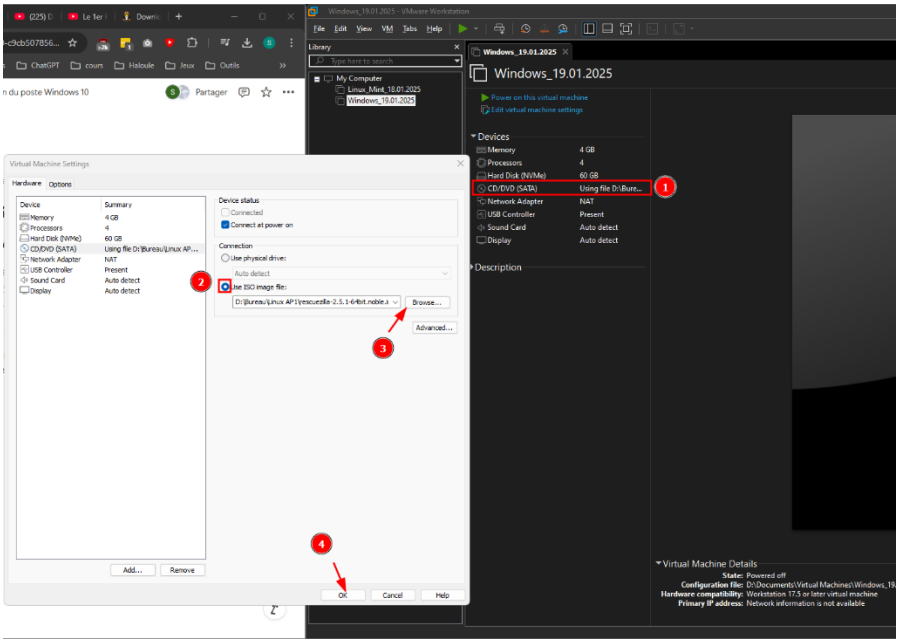
- La masterisation d'un poste Windows 10 crée une image standardisée pour un déploiement rapide et cohérent. Rescuezilla facilite cette tâche, avec une documentation essentielle pour éviter les erreurs.

2. Préalable

- Un support de stockage pour la sauvegarde (USB, SSD, HDD, etc.).
- Un système à sauvegarder et à cloner.
- Puis rendez-vous sur ce site pour télécharger l'ISO de Rescuezilla :
  - Rescuzilla

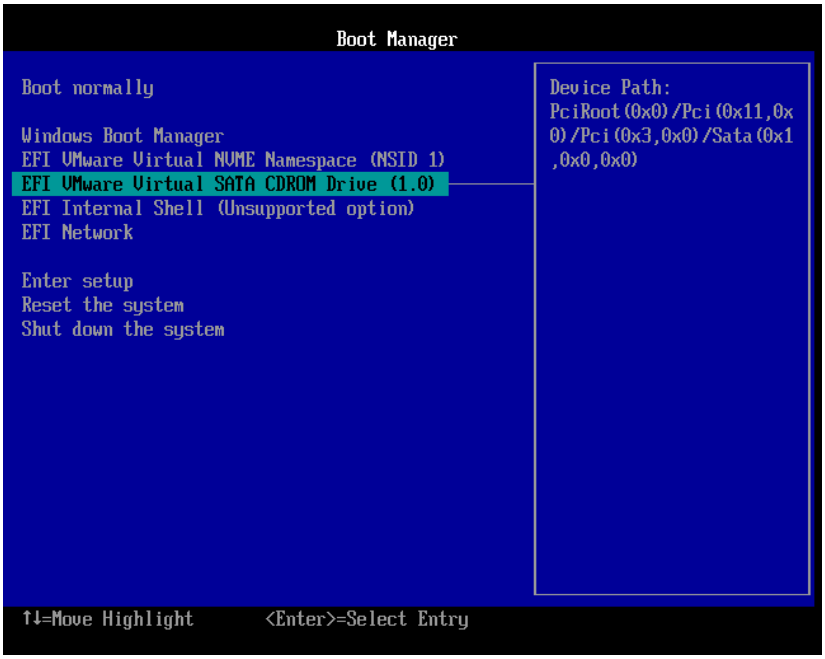
3. Configuration initiale

- Sélection de l'ISO dans VMware
- Sélectionnez votre VM sur VMware, cliquez sur **CD/DVD (SATA)** *(1)*. Cochez « Use ISO image file », puis cliquez sur le bouton **Browse...** *(2)* et sélectionnez **rescuezilla.iso** *(3)* que vous venez de télécharger. Cliquez ensuite sur **OK** *(4)*.



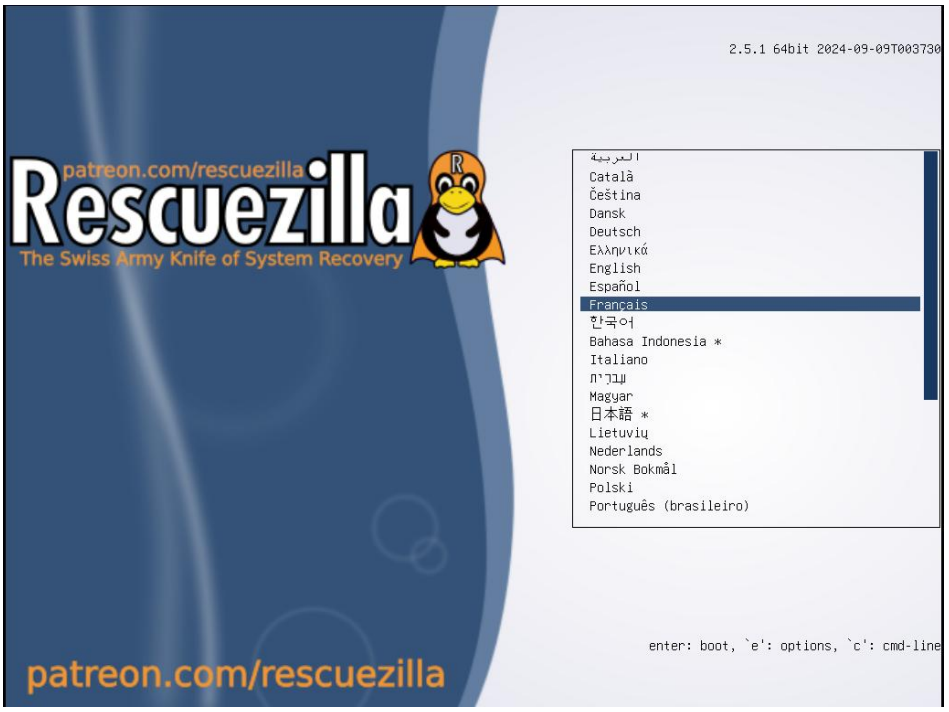
4. Démarrage de la VM et accès au BIOS

- Lancez la VM et, lorsque la fenêtre se lance, cliquez sur la touche **F2** de votre clavier pour entrer dans l'UEFI.
- Une fois dans le BIOS, descendez avec les flèches directionnelles jusqu'à sélectionner **EFI VMware Virtual SATA CDROM Drive (1.0)** et appuyez sur **Entrée**.

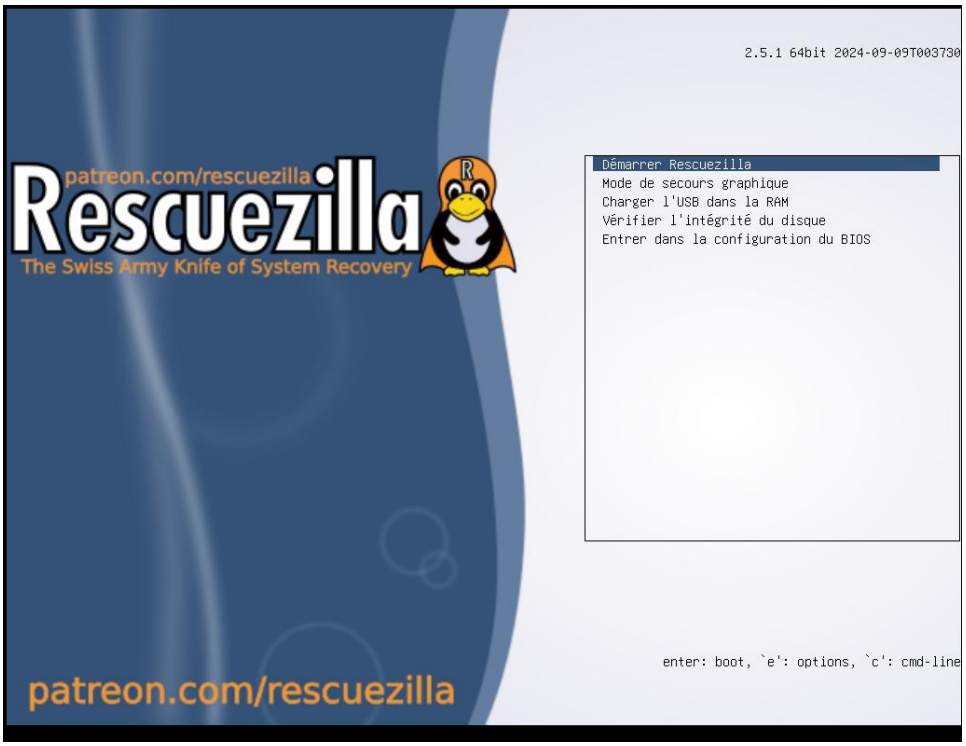


5. Utilisation de Rescuzilla

- Une fois dans Rescuezilla, sélectionnez votre langue en utilisant les flèches puis appuyez sur **Entrée**. Pour ce guide, nous choisirons le français.



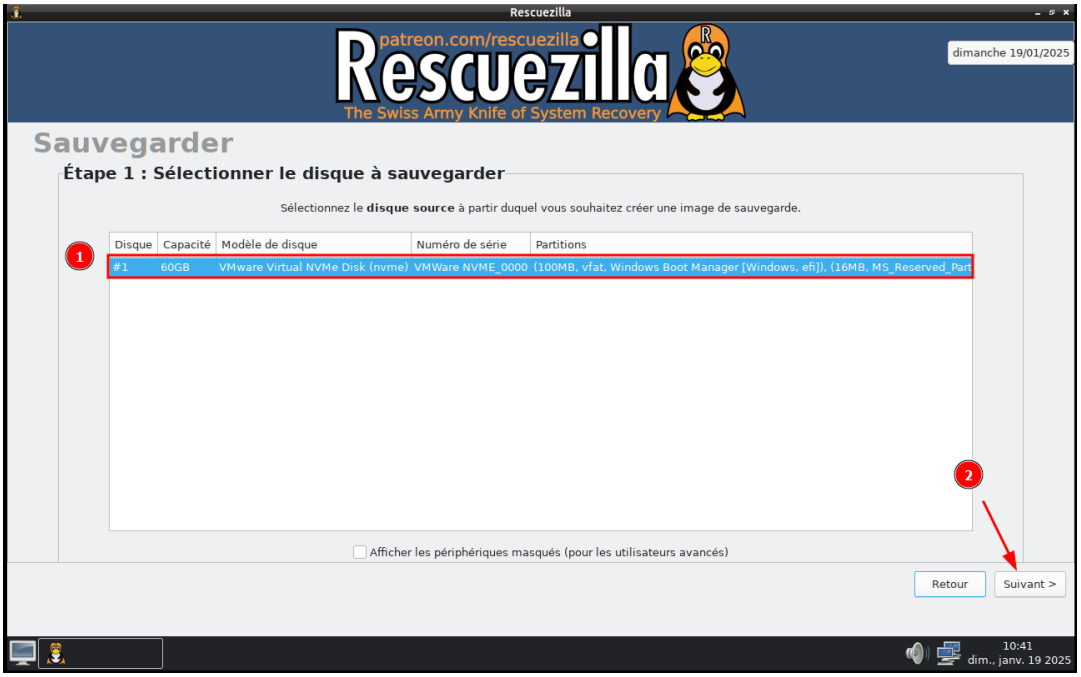
- Sélectionnez « Démarrer Rescuezilla » en utilisant les flèches puis appuyez sur **Entrée**.



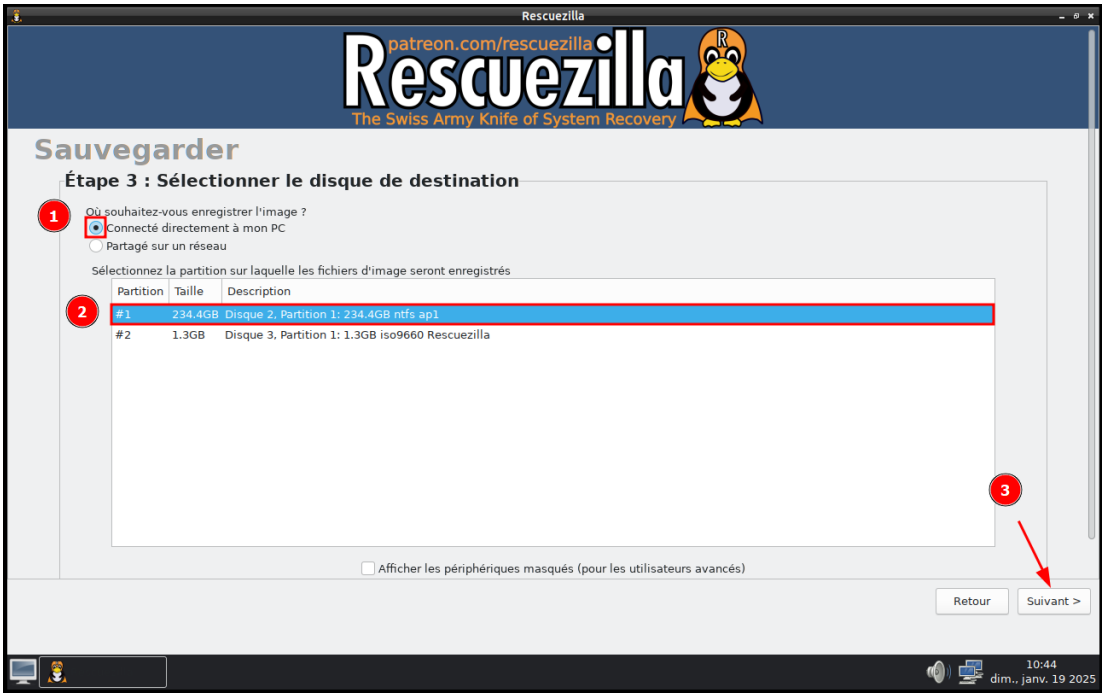
6. Sauvegarde du système

- Cliquez sur **Sauvegarder**.

- Sélectionnez le **disque à sauvegarder** *(1)* puis cliquez sur **Suivant** *(2)*.

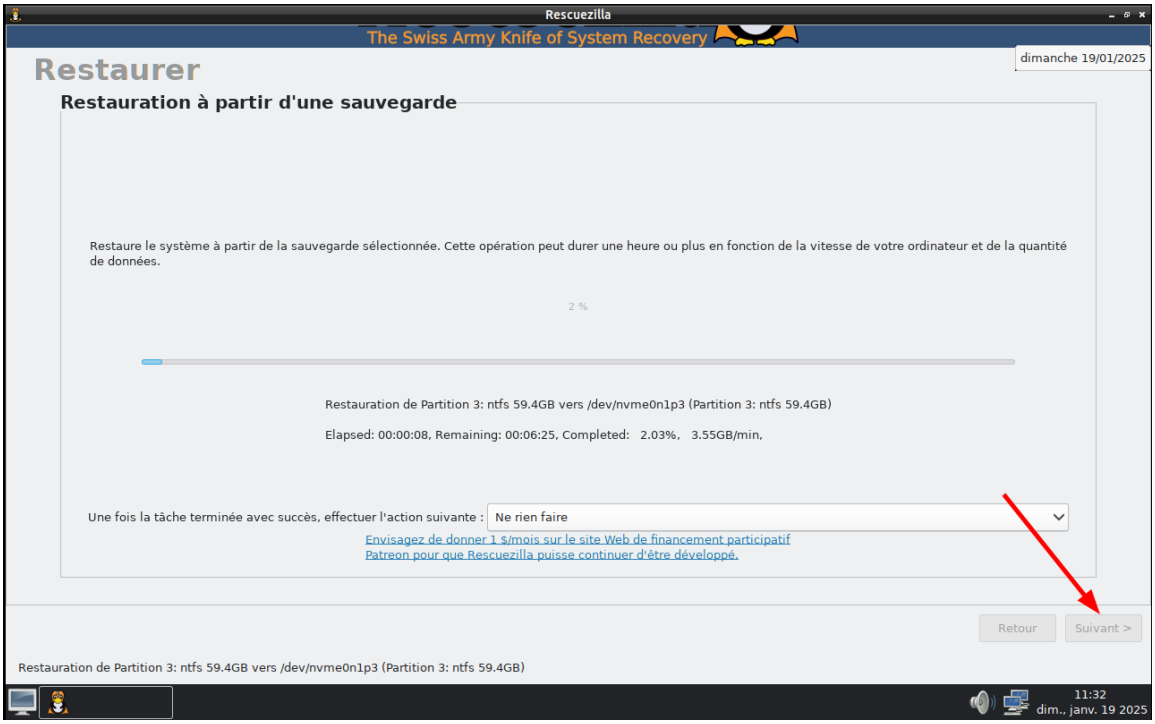


- Laissez cocher **« Connecté directement à mon PC »** *(1)*. Sélectionnez le **support sur lequel sera effectuée la sauvegarde** *(2)* et cliquez sur **Suivant** *(3)*.



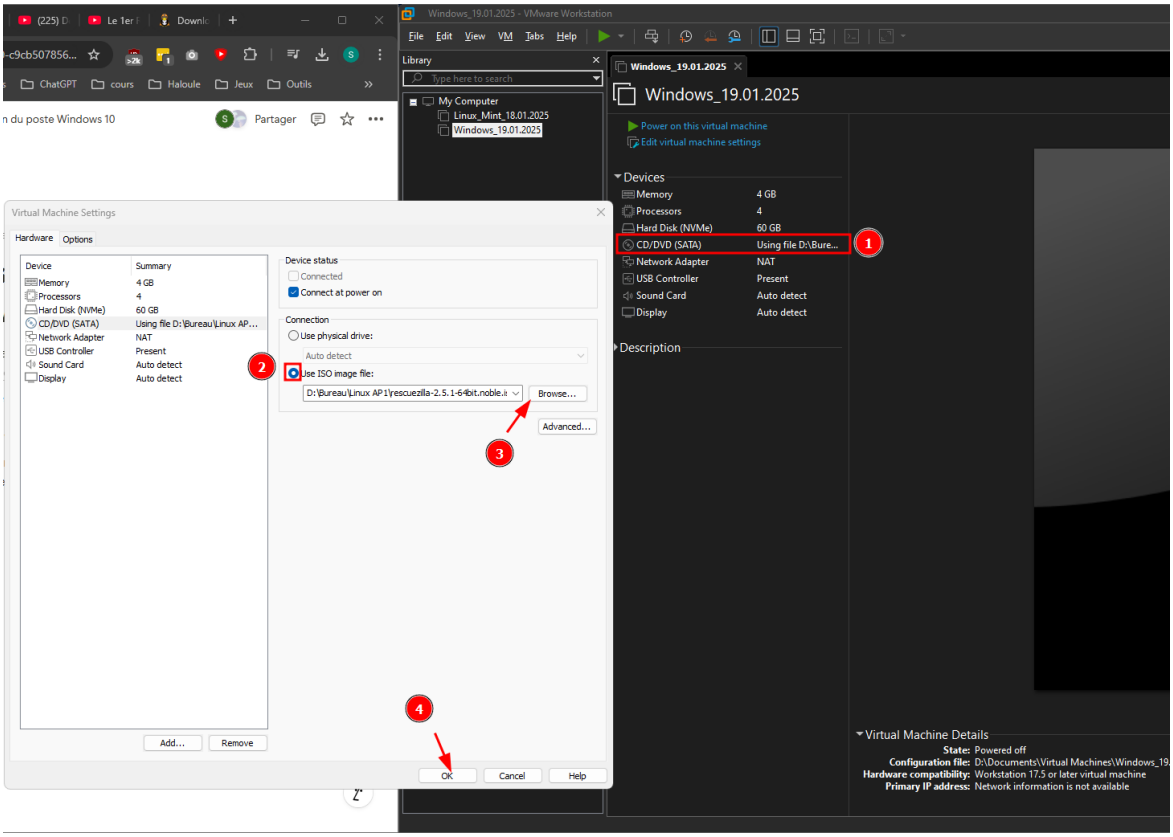
- **Renommez** *(1)* la sauvegarde si nécessaire, puis cliquez sur **Suivant** *(2)* pour lancer la sauvegarde.

- Une barre de progression indique l'avancement de la sauvegarde. Une fois terminée, cliquez sur **Suivant**.

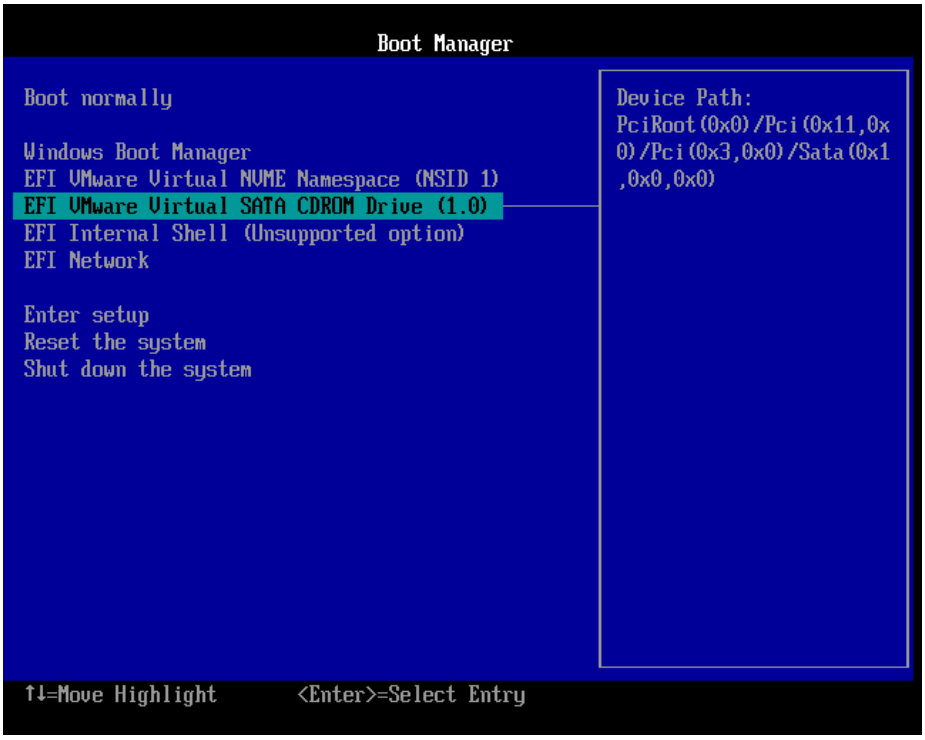


7. Restauration du système

- Pour restaurer un système, créez une nouvelle VM. Vous pouvez suivre le guide « 00. Création d'une machine virtuelle (VM) dans VMware » si besoin.
- Répétez la configuration initiale en sélectionnant « Use ISO image file » *(1,2)* et en choisissant **rescuezilla.iso** *(3)*.

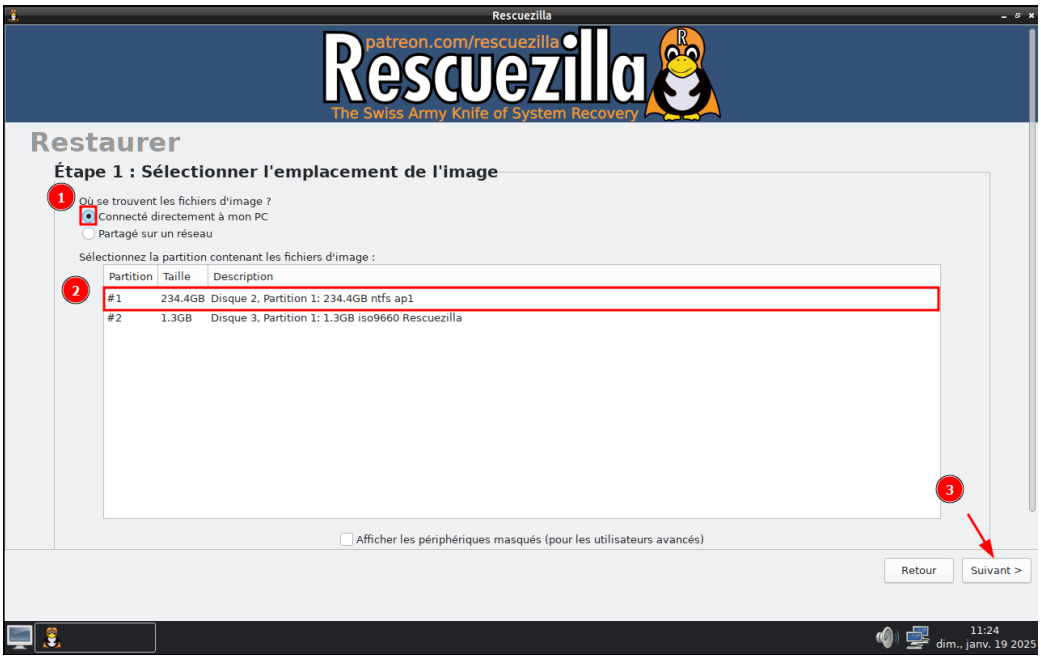


- Suivez les mêmes étapes que pour la sauvegarde afin de lancer Rescuezilla.

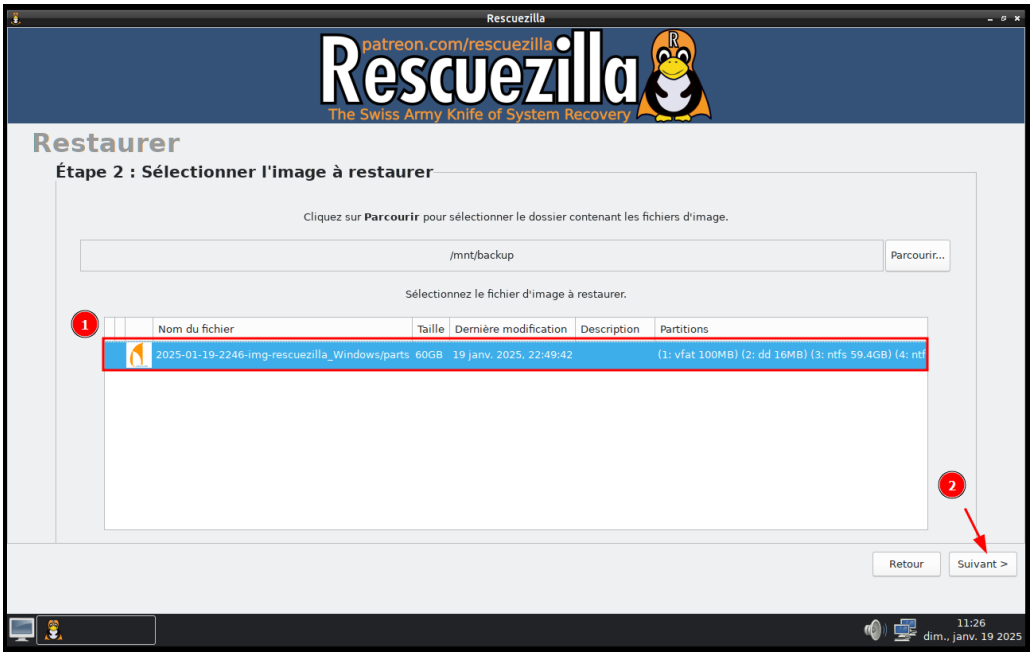


- Cliquez sur **Restaurer**.

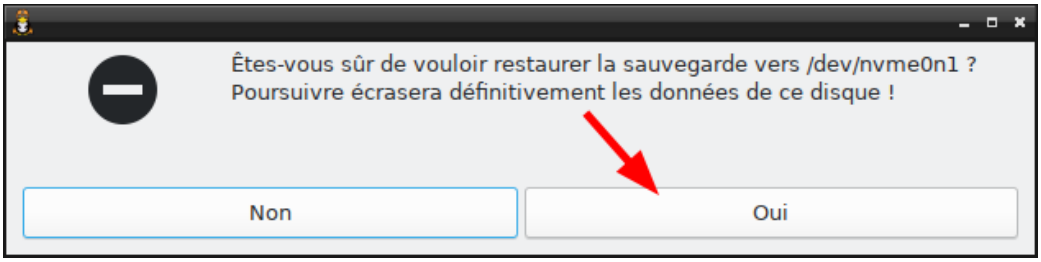
- Sélectionnez le support contenant la **sauvegarde** *(1)* et cliquez sur **Suivant** *(2)*.



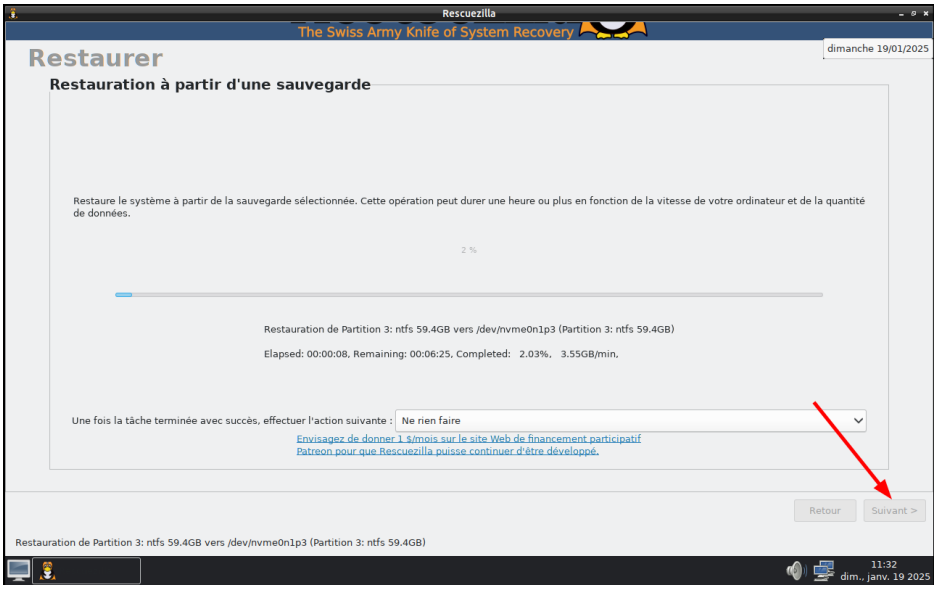
- Sélectionnez **l'image à restaurer** *(1)*, la VM cible, puis suivez les instructions pour terminer la restauration *(2)*.



- Cliquez sur **Oui** pour confirmer et démarrer la restauration.



- Une fois la restauration terminée, redémarrez la VM pour utiliser votre système restauré.



8. Pourquoi ces étapes sont importantes ?

- **Standardisation et cohérence** : La masterisation permet de garantir que tous les postes disposent de la même configuration et des mêmes outils, réduisant ainsi les variations et les problèmes de compatibilité.
- **Gain de temps et efficacité** : Les sauvegardes et restaurations rapides avec Rescuezilla simplifient le déploiement et la maintenance des postes en cas de panne ou de mise à jour.
- **Sécurité renforcée** : Une image de sauvegarde configurée correctement assure un environnement maîtrisé et limite les risques liés aux erreurs de configuration ou aux intrusions.

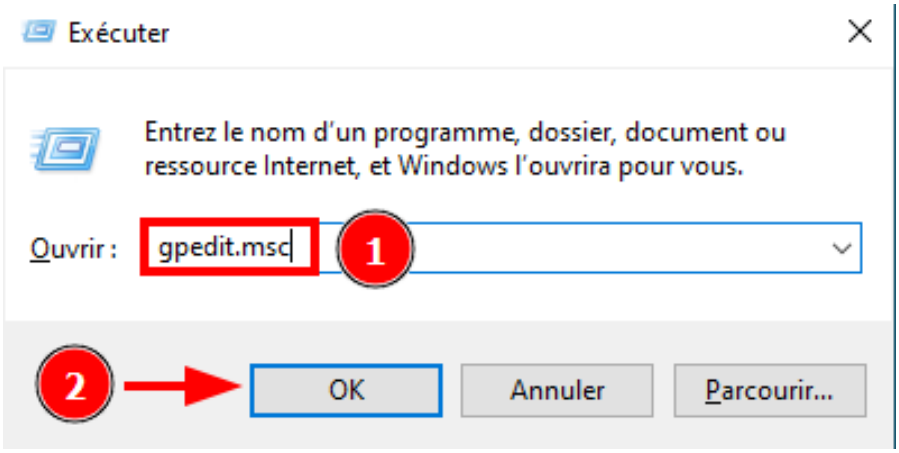
15. Chiffrement de disque avec BitLocker

1. Introduction

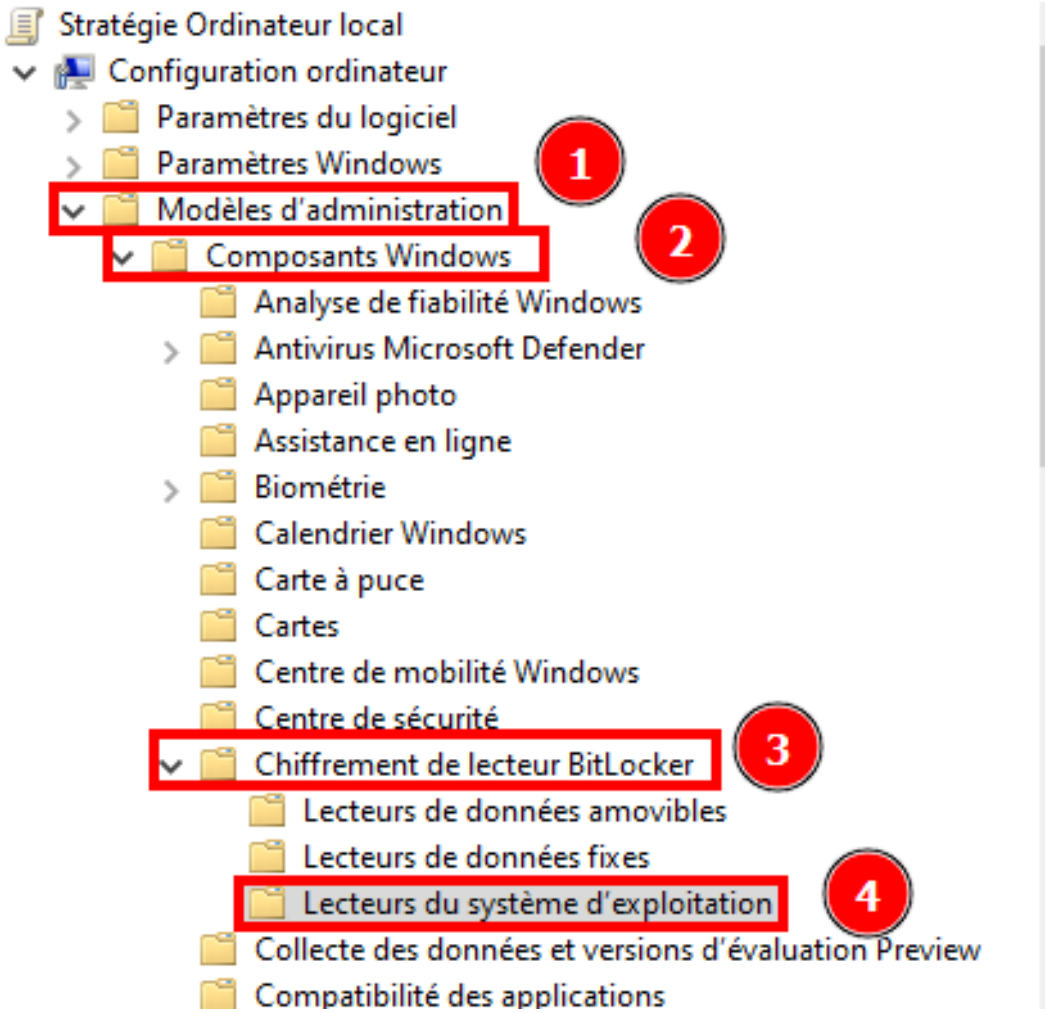
- **BitLocker** est une fonctionnalité de chiffrement intégrée à Windows qui protège les données en les rendant illisibles sans une clé ou un mot de passe. Son activation garantit la confidentialité des informations, même en cas de perte ou de vol de l'appareil.

2. Autoriser l'authentification au démarrage

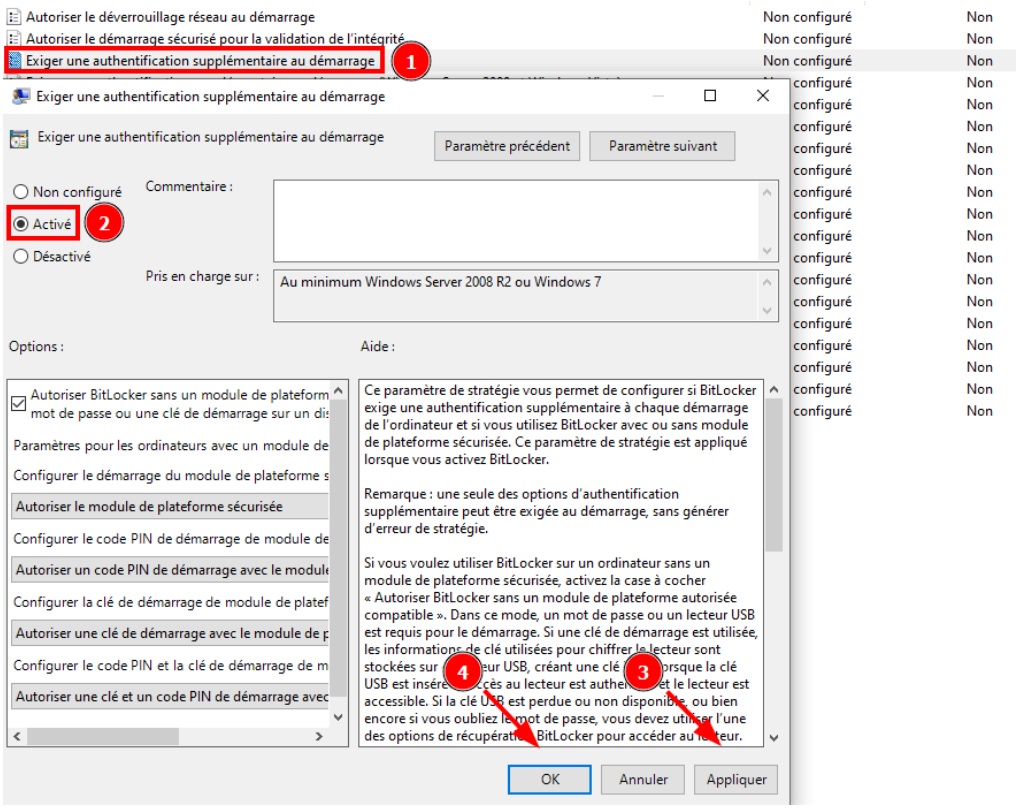
- Appuyez sur **Win + R**, tapez **gpedit.msc** *(1)*, puis appuyez sur **OK** *(2)*.



- Puis allez dans -> **Modèles d'administration** *(1)* -> **Composants Windows** *(2)* -> **Chiffrement de lecteur BitLocker** *(3)* -> **Lecteurs du système d'exploitation** *(4)*.

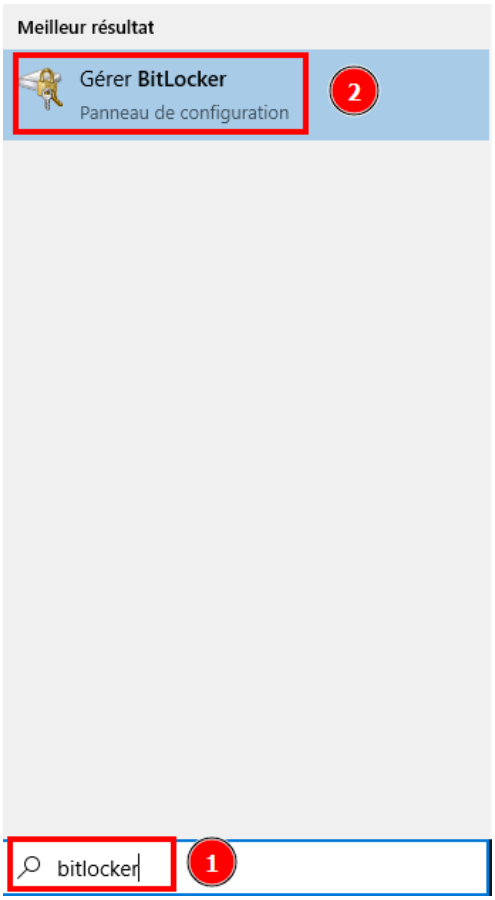


- Localisez **Exiger une authentification supplémentaire au démarrage** *(1)*, **Activé** *(2)* la stratégie puis faites **Appliquer** *(3)* et **OK** *(4)*.

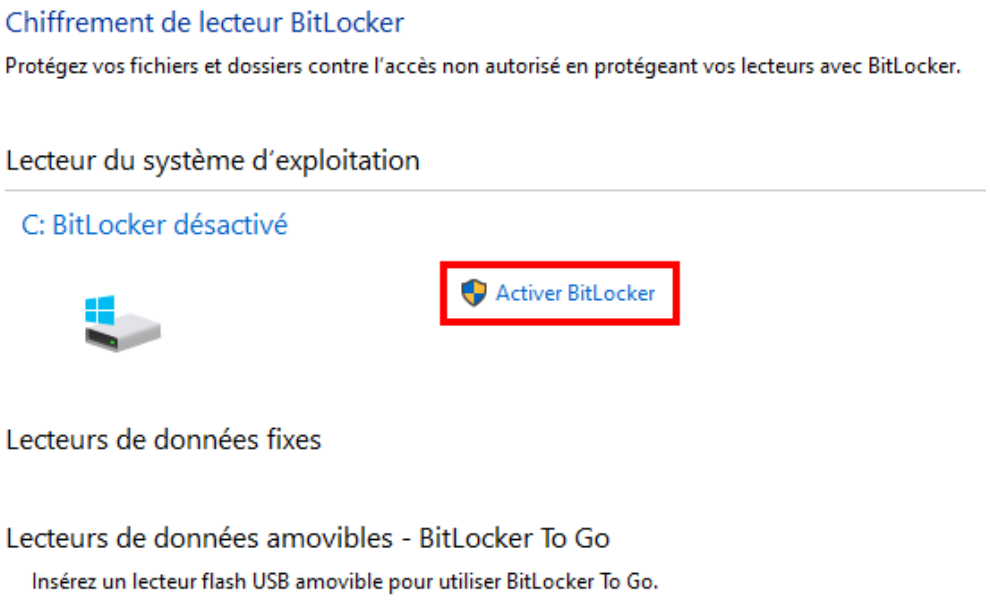


3. Activation de BitLocker

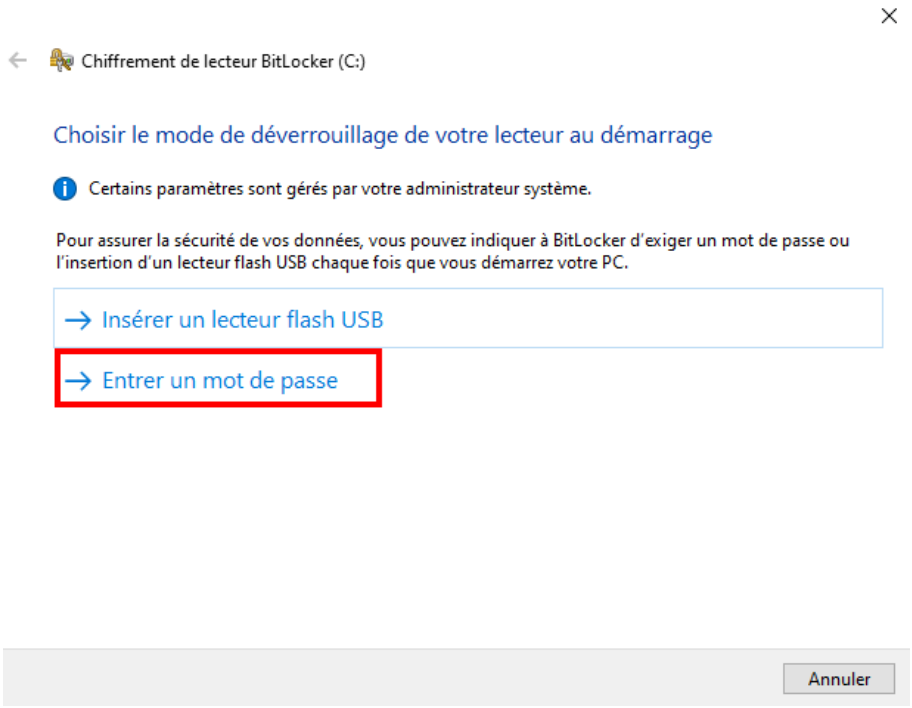
- Tapez **BitLocker** dans la barre de recherche Windows *(1)* et sélectionnez **Gérer BitLocker** *(2)*.



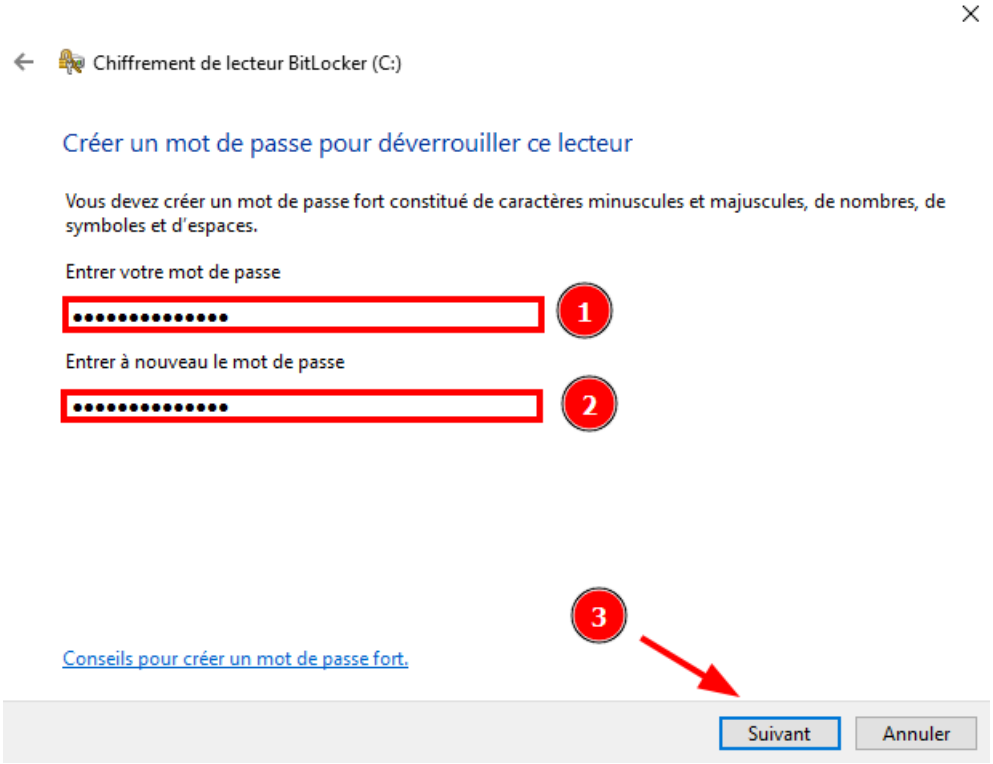
- Puis cliquez sur **Activer BitLocker.**



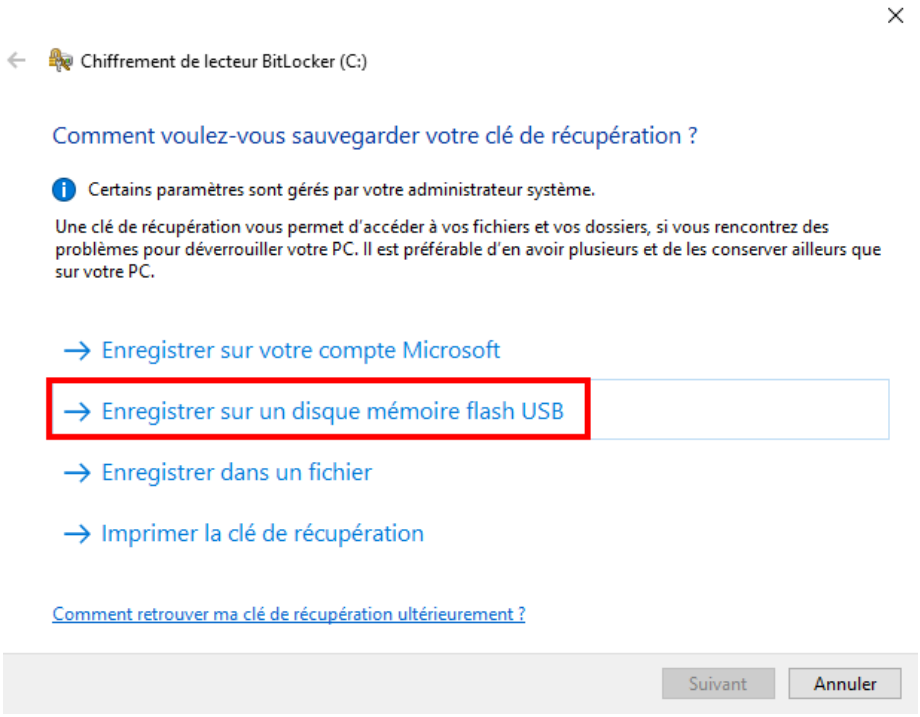
- Ensuite sélectionnez **Entrer un mot de Passe**.



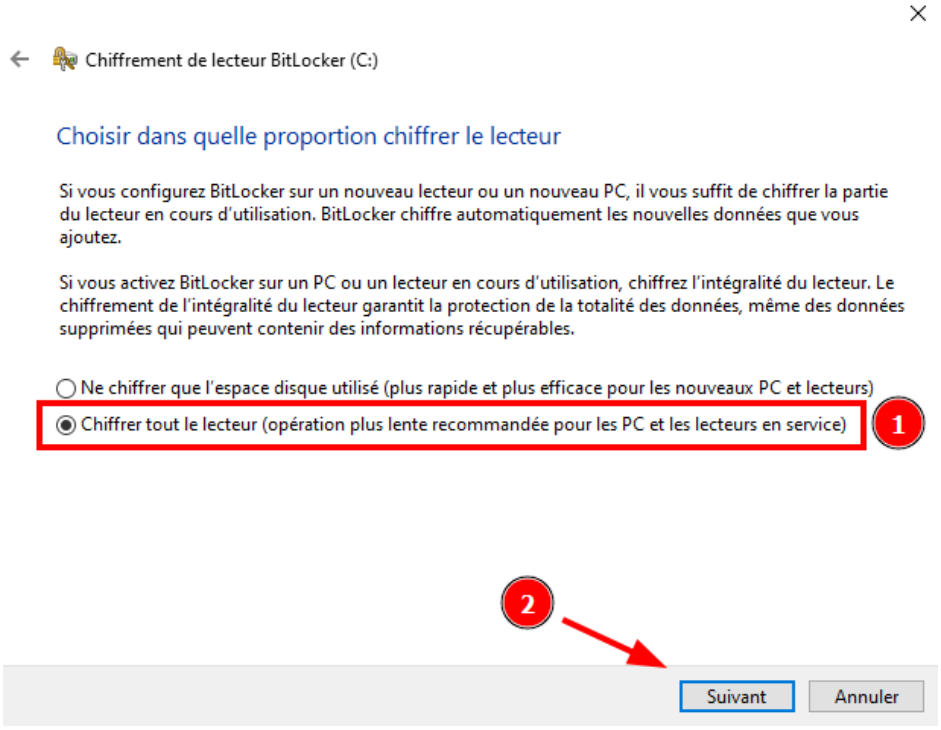
- Enfin **rentrez un mot de passe** *(1)* et **rentrez-le à nouveau** *(2)* puis faites **Suivant** *(3)*.



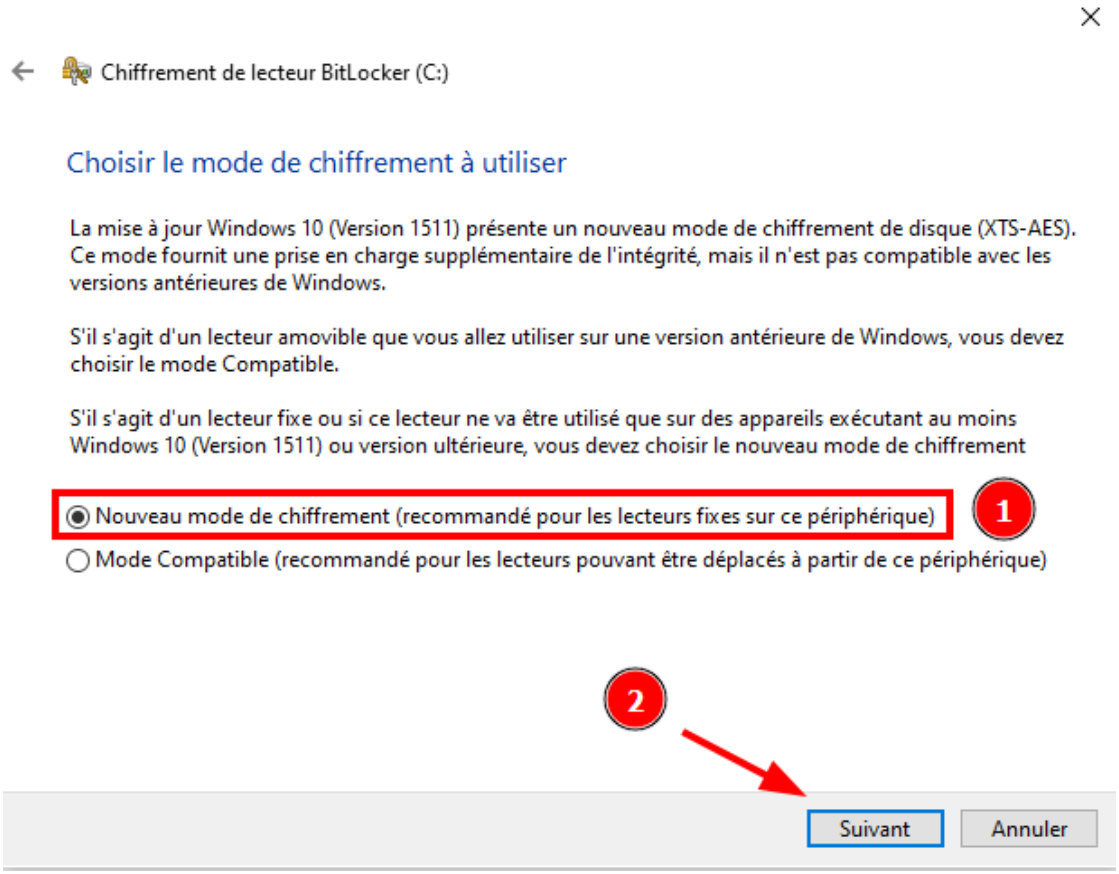
- Pour la clé de récupération, branchez une clé USB et sélectionnez **Enregistrer sur un disque mémoire flash USB.**



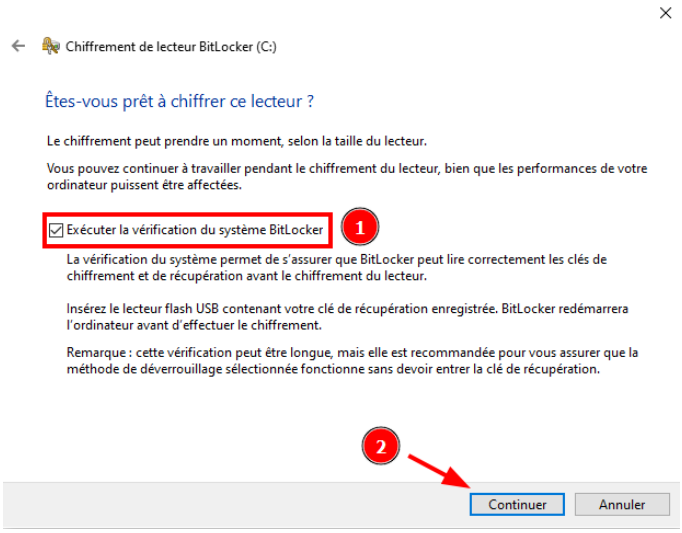
- Prenez la deuxième option pour **chiffrer tout le lecteur** *(1)* et faites **Suivant** *(2)*.



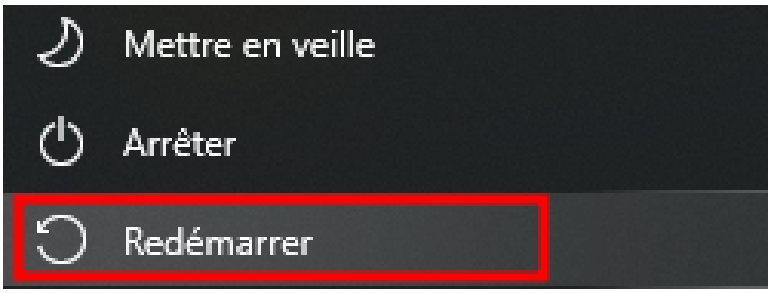
- Ensuite séléctionnez la première option pour un **nouveau mode de chiffrement** *(1)* et faites **Suivant** *(2)*.



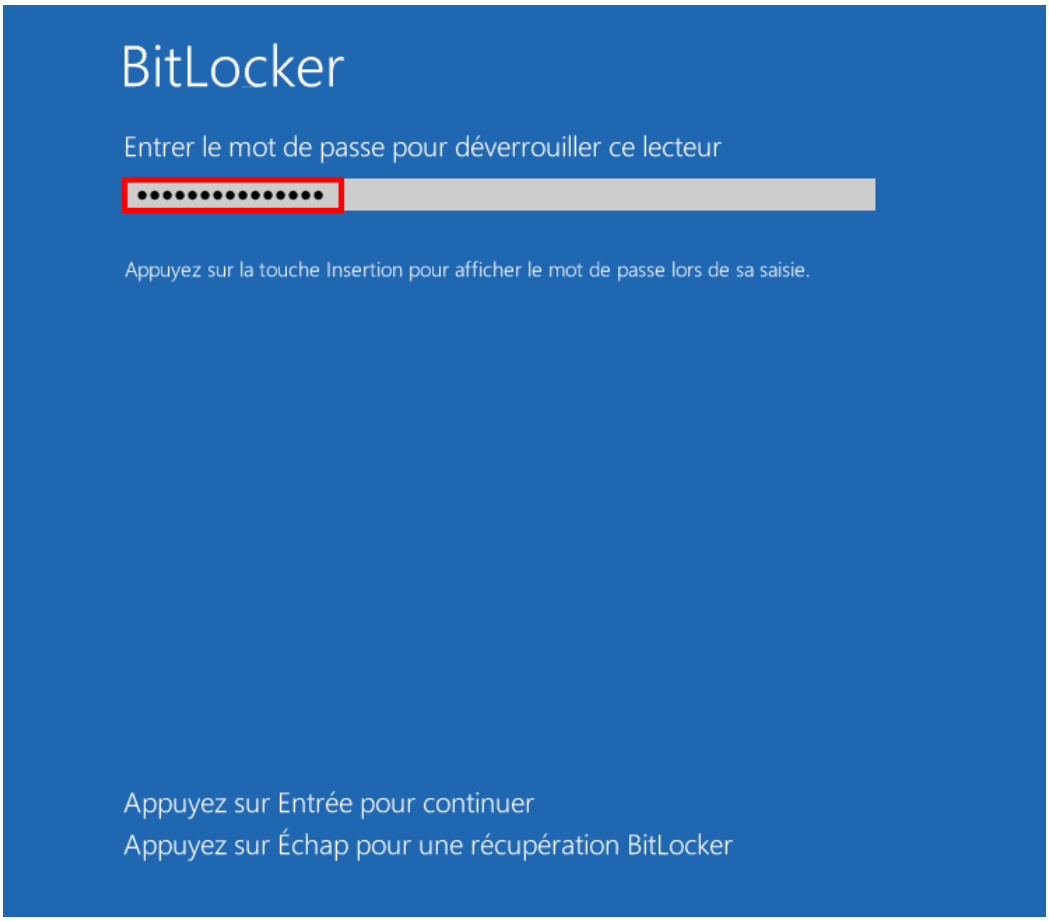
- Cochez la case **Exécuter la vérification du système BitLocker** *(1)* puis faites **Suivant** *(2)*.



- **Redémarrez** votre système.



- Et entrez le **mot de passe** que vous avez choisi **avant**.



- Votre **BitLocker** est maintenant configuré, et votre disque est **chiffré**.

3. Pourquoi cette étape est importante ?

- **Protection des données sensibles :** Le chiffrement empêche tout accès non autorisé aux informations en cas de vol ou de perte de l'appareil.
- **Conformité et sécurité :** BitLocker aide à respecter les exigences réglementaires comme le RGPD en protégeant les données confidentielles.

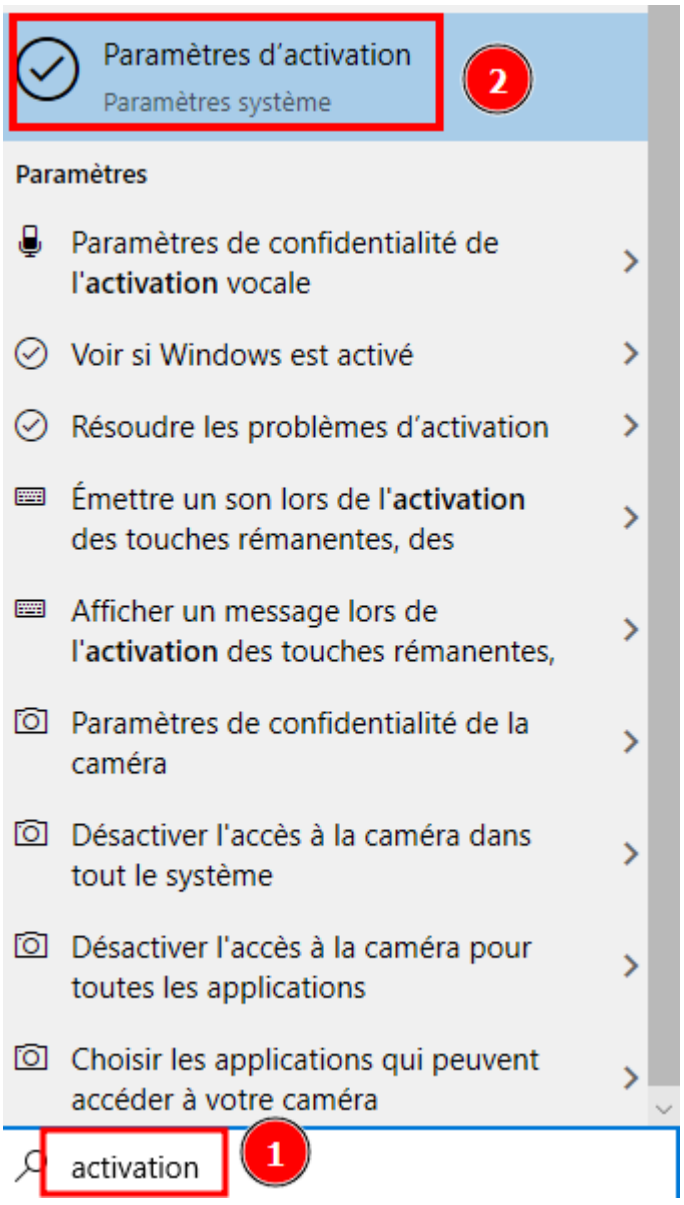
16. Activation de la clé Windows 10

1. Introduction

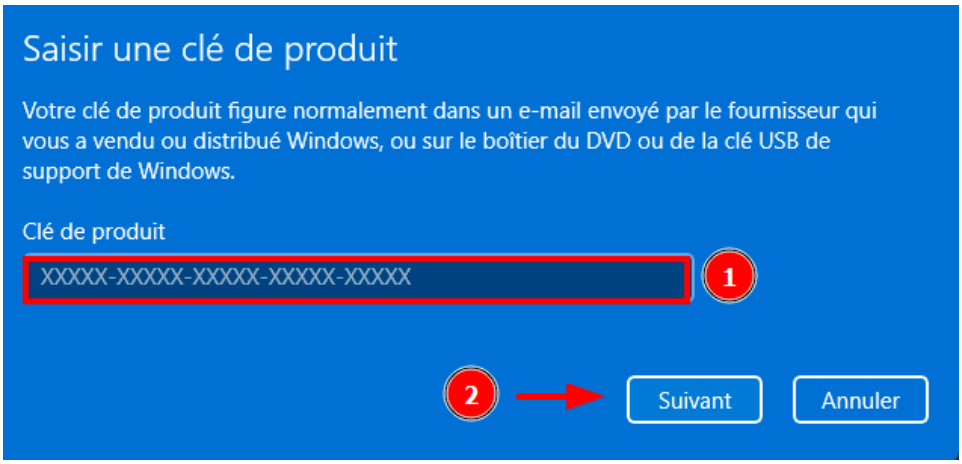
- Dans cette étape nous activerons la licence Windows 10 Entreprise.

2. Localisation de l'activation

- Rendez-vous sur la barre de recherche **Windows** et entrez "**Activation**" *(1)* puis sélectionnez la fonctionnalité "**Paramètre d'activation**" *(2)*.



- Puis modifiez la clé d'activation Windows par celui dont l'entreprise vous a fournis, entrez-le *(1)* et faites **Suivant** *(2)*.



- Maintenant votre Windows 10 Entreprise est **Actif.**

3. Pourquoi cette étape est importante ?

- **Conformité légale :** L'activation garantit l'utilisation d'une licence authentique, évitant tout risque lié à des violations de droits d'utilisation.
- **Accès aux fonctionnalités :** Une version activée débloque toutes les fonctionnalités de Windows, assurant une utilisation optimale et complète.
- **Mises à jour critiques :** L'activation permet de recevoir des mises à jour essentielles pour la sécurité et les performances du système.

3. Dépannage Windows

0. Documentation de dépannage pour la création d'une machine virtuelle dans VMware

0. Introduction

- Voici une documentation complète pour résoudre les problèmes courants liés à la création et à la configuration d'une machine virtuelle (VM) dans **VMware Workstation** ou **VMware Player**.

1. Problèmes : Impossible de lancer VMware

- **Symptôme** : VMware ne démarre pas ou affiche une erreur.
- **Solution** :
  - 1. Vérifiez que la virtualisation matérielle est activée dans le BIOS/UEFI :
    - Redémarrez votre machine et accédez au BIOS (souvent via **F2**, **DEL** ou **ESC** au démarrage).
    - Activez l'option **Intel VT-x** ou **AMD-V**.
  - 2. Vérifiez si VMware est correctement installé. Si nécessaire, réinstallez-le depuis le site officiel.

2. Problèmes : L'ISO du système d'exploitation n'est pas détecté

- **Symptôme** : VMware ne démarre pas ou affiche une erreur.
- **Solution** :
  - 1. Assurez-vous que l'ISO est attaché à la VM :
    - Accédez à Settings > CD/DVD (SATA) dans VMware.
    - Cochez l'option **Use ISO image file** et sélectionnez le fichier ISO.
  - 2. Vérifiez que l'ISO est valide :
    - <nom_du_fichier>.iso

3. Problèmes : La VM ne démarre pas après sa création

- **Symptôme** : La VM s'arrête immédiatement après avoir été lancée.
- **Solution** :
    - 1. Vérifiez la configuration du firmware :
        - Accédez à **Settings > Firmware** type et sélectionnez **UEFI**.
    - 2. Vérifiez la taille du disque virtuel :
        - Allez dans **Settings > Hard Disk** et assurez-vous que l'espace disque est suffisant (ex. : 60 GB minimum pour Windows).
    - 3. Assurez-vous que le système d'exploitation est bien sélectionné dans les paramètres de la VM.

4. Problèmes : Les performances de la VM sont faibles

- **Symptôme** : La VM est lente ou se bloque fréquemment.
- **Solution** :
    - 1. Augmentez la mémoire allouée à la VM :
        - Accédez **à Settings > Memory** et attribuez au moins 4 GB (ou 8192 MB pour des performances optimales).
    - 2. Augmentez le nombre de cœurs processeurs :
        - Allez dans **Settings > Processors** et configurez **2 cœurs** par processeur.
    - 3. Assurez-vous que votre hôte dispose de ressources suffisantes.

5. Problèmes : Le réseau ne fonctionne pas dans la VM

- **Symptôme** : La VM n'a pas accès à Internet ou au réseau local.
- **Solution** :
    - 1. Configurez l'adaptateur réseau sur **NAT** dans Settings > Network Adapter.
    - 2. Redémarrez le service réseau dans la VM :
        - Ouvrez les paramètres réseau et cliquez sur « Dépanner ».

6. Problème : La Snapshot échoue ou prend trop de temps

- **Symptôme** : La sauvegarde de l'état actuel de la VM via une Snapshot échoue.
- **Solution** :
    - 1. Vérifiez l'espace disque disponible sur le disque de l'hôte.
    - 2. Fermez toutes les applications inutiles dans la VM avant de prendre une Snapshot.
    - 3. Si le problème persiste, essayez de compacter le disque virtuel via VMware :
        - Allez dans Settings > Hard Disk > Utilities > Compact.

7. Problème : Erreurs pendant l'installation de l'OS

- **Symptôme** : L'installation du système d'exploitation se bloque ou échoue.
- **Solution** :
    - 1. Recréez la VM avec les options recommandées (ex. : NVMe pour le disque, 2 processeurs).
    - 2. Téléchargez une nouvelle copie de l'ISO et vérifiez son intégrité.
    - 3. Vérifiez les journaux d'erreurs de VMware pour diagnostiquer.

8. Annexes

- **Commandes utiles** :
    - Vérifier les ressources réseau dans la VM : ping 8.8.8.8.
    - Augmenter la mémoire disponible dans VMware : Settings > Memory.
- **Ressources supplémentaires** :
    - Documentation officielle VMware : Vmware.

1. Documentation de dépannage pour les paramètres biométriques et de verrouillage d'écran sous Windows 10

0. Introduction

- Voici une documentation complète pour résoudre les problèmes courants liés à la configuration de Windows Hello, des fonctionnalités biométriques, et des paramètres d'écran de verrouillage.

1. Problème : Windows Hello ne s'active pas

- **Symptôme** : Message « Windows Hello n'est pas disponible sur cet appareil ».
- **Solution** :
    - 1. Vérifiez la compatibilité matérielle :
        - Allez dans **Paramètres > Système > À propos de** et assurez-vous que votre appareil est compatible avec Windows Hello.
    - 2. Activez Windows Hello dans les stratégies de groupe :
        - Appuyez sur Win + R, tapez gpedit.msc, puis configurez :
            - **Autoriser l'utilisation de la biométrie → Activé**.
            - **Utiliser Windows Hello Entreprise → Activé**.
    - 3. Redémarrez l'appareil après avoir appliqué les changements.

2. Problème : La reconnaissance faciale ne fonctionne pas

- **Symptôme** : Windows Hello n'arrive pas à enregistrer ou reconnaître un visage.
- **Solution** :
    - 1. Vérifiez que la caméra est activée et fonctionnelle :
        - Testez-la via l'application **Caméra**.

- 2. Assurez-vous que la fonction de reconnaissance faciale est activée :
  - Dans gpedit.msc → **Composants Windows > Biométrie > Traits du visage**, configurez :
    - **Configurer la détection d'usurpation avancée** → **Activé**.
- 3. Si le problème persiste, mettez à jour les pilotes de la caméra.

3. Problème : La caméra s'active sur l'écran de verrouillage

- **Symptôme** : La caméra s'allume automatiquement à l'écran de verrouillage.
- **Solution** :
  - 1. Désactivez l'utilisation de la caméra via les stratégies de groupe :
    - gpedit.msc → **Panneau de configuration > Personnalisation > Empêcher l'activation de l'appareil photo de l'écran de verrouillage** → **Activé**.
  - 2. Vérifiez les paramètres dans **Paramètres > Confidentialité > Caméra** et désactivez les applications autorisées à accéder à la caméra.

4. Problème : L'activation vocale reste active à l'écran de verrouillage

- **Symptôme** : Les commandes vocales fonctionnent sur un appareil verrouillé.
- **Solution** :
  - 1. Désactivez l'activation vocale dans les paramètres :
    - **Paramètres > Confidentialité > Activation vocale** → Désactivez l'option.
  - 2. Pour les appareils utilisant Cortana, désactivez cette fonctionnalité dans **Paramètres > Applications > Applications par défaut**.

5. Problème : Les modifications des stratégies de groupe ne prennent pas effet

-

- **Symptôme** : Les paramètres configurés dans gpedit.msc n'apparaissent pas dans Windows.
- **Solution** :
    - 1. Mettez à jour les stratégies manuellement :
        - gpupdate /force
    - 2. Assurez-vous que l'utilisateur dispose des privilèges administratifs nécessaires.

6. Problème : L'anti-spoofing ne fonctionne pas correctement

- **Symptôme** : La reconnaissance faciale accepte des images ou vidéos au lieu du visage réel.
- **Solution** :
    - 1. Vérifiez que la caméra utilisée prend en charge l'anti-spoofing avancé.
    - 2. Activez l'option dans gpedit.msc :
        - **Configurer la détection d'usurpation avancée** → **Activé**.

7. Annexes

- **Commandes utiles** :
    - Appliquer les stratégies immédiatement : gpupdate /force.
    - Vérifier la compatibilité matérielle : **Paramètres > Système > À propos de**.
- **Ressources supplémentaires** :
    - Documentation officielle Windows Hello : Microsoft.

2. Documentation de dépannage pour la configuration DNS et la sécurité réseau sous Windows

0. Introduction

- Voici une documentation détaillée pour résoudre les problèmes courants liés à la configuration DNS, à la désactivation des protocoles obsolètes, et à l'application des politiques réseau.

1. Problème : Les modifications DNS ne prennent pas effet

- **Symptôme** : Après avoir configuré le registre ou les paramètres DNS, les changements ne sont pas appliqués.
- **Solution** :
    - 1. Redémarrez le service DNS :
        - net stop dnscache && net start dnscache
    - 2. Assurez-vous que la clé de registre est correcte et active :
        - Allez dans :

          « HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows NT\\DNSClient » et vérifiez la valeur **EnableMulticast** ou **DisableParallelAandAAAA**.
    - Redémarrez le système pour appliquer les changements.

2. Problème : L'activation/désactivation de SMBv1 ne fonctionne pas

- **Symptôme** : Le protocole SMBv1 reste actif malgré sa désactivation via les fonctionnalités Windows.
- **Solution** :

- 1. Vérifiez l'état actuel de SMBv1 :
  - Get-SmbServerConfiguration | Select EnableSMB1Protocol
- 2. Désactivez SMBv1 via PowerShell :
  - Disable-WindowsOptionalFeature -Online -FeatureName "SMB1Protocol"
- 3. Redémarrez le système pour finaliser la désactivation.

3. Problème : NTLMv1 reste actif malgré sa désactivation

- **Symptôme** : Le système continue d'accepter les connexions utilisant NTLMv1.
- **Solution** :
  - 1. Vérifiez la configuration des stratégies locales :
    - secpol.msc → **Stratégies locales > Options de sécurité > Restreindre NTLM**.
  - 2. Redémarrez le système.

4. Problème : UAC (Contrôle de compte utilisateur) ne s'active pas

- **Symptôme** : L'UAC reste désactivé ou son niveau de sécurité ne change pas.
- **Solution** :
  - 1. Activez l'UAC via le registre :
    - reg add "HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System" /v EnableLUA /t REG_DWORD /d 1 /f
  - 2. Redémarrez pour activer les modifications.
  - 3. Vérifiez les niveaux de notification dans le panneau de configuration :
    - **Paramètres > Comptes > Modifier les paramètres de contrôle de compte d'utilisateur**.

5. Problème : Les modifications via regedit provoquent des erreurs

- **Symptôme** : Messages "Erreur d'accès" ou "Impossible de modifier".
- **Solution** :
    - 1. Lancez regedit en tant qu'administrateur (clic droit > Exécuter en tant qu'administrateur).
    - 2. Si une clé est protégée, prenez-en le contrôle :
        - Cliquez droit sur la clé > **Autorisations > Avancé** > Changez le propriétaire en Administrateurs.
    - 3. Appliquez les modifications après avoir pris le contrôle.

6. Problème : Les requêtes DNS sont lentes ou échouent

- **Symptôme** : Le chargement des sites ou des services dépendant du DNS est lent.
- **Solution** :
    - 1. Testez la résolution DNS avec :
        - nslookup www.example.com
    - 2.Ajoutez des serveurs DNS publics comme fallback dans les paramètres réseau :
        - Exemples : 8.8.8.8 (Google), 1.1.1.1 (Cloudflare).

7. Annexes

- **Commandes utiles** :
    - Redémarrer le service DNS : net stop dnscache && net start dnscache.
    - Vérifier la compatibilité NTLM : gpresult /R.
- **Ressources supplémentaires** :
    - Guide officiel DNS de Microsoft : Microsoft.

3. Documentation de dépannage pour la sécurité des mots de passe et de l'authentification sous Windows

0. Introduction

- Voici une documentation complète pour résoudre les problèmes courants liés à la mise en œuvre de politiques de mots de passe, d'authentification, et de gestion des privilèges.

1. Problème : Les politiques de mots de passe ne sont pas appliquées

- **Symptôme** : Les utilisateurs peuvent définir des mots de passe simples ou ne sont pas forcés de les changer.
- **Solution** :
    - Vérifiez les paramètres de la stratégie locale :
        - Ouvrez secpol.msc et allez dans **Stratégies de compte > Stratégies de mot de passe**.
    - Assurez-vous que les options suivantes sont correctement configurées :
        - **Longueur minimale** : 12 caractères.
        - **Exigence de complexité** : Activé.
        - **Durée maximale** : 90 jours.
    - Appliquez les stratégies immédiatement :
        - gpupdate /force

2. Problème : Les mots de passe sont enregistrés en mémoire en clair

- **Symptôme** : Risque d'exploitation des informations d'identification stockées.
- **Solution** :
    - 1. Modifiez le registre pour désactiver cette fonctionnalité :
        - reg add "HKLM\\SYSTEM\\CurrentControlSet\\Control\\SecurityProviders\\WDigest" /v UseLogonCredential /t REG_DWORD /d 0 /f
    - 2. Redémarrez le système pour appliquer les modifications.

3. Problème : Kerberos utilise des méthodes de chiffrement faibles

- **Symptôme** : Les connexions réseau sont vulnérables à des attaques.
- **Solution** :
    - 1. Configurez les types de chiffrement Kerberos autorisés :
        - Ouvrez secpol.msc et allez dans **Options de sécurité > Sécurité réseau : Configurer les types de chiffrement autorisés pour Kerberos**.
        - Activez uniquement **AES128_HMAC_SHA1** et **AES256_HMAC_SHA1**.
    - 2. Validez et redémarrez pour appliquer les paramètres.

4. Problème : PowerShell V2 est toujours actif

- **Symptôme** : Des scripts malveillants pourraient exploiter des vulnérabilités de cette version obsolète.
- **Solution** :
    - 1. Désactivez PowerShell V2 avec PowerShell en mode administrateur :
    - 2. Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2 -NoRestart
    - 3. Redémarrez pour finaliser la désactivation.

5. Problème : AutoRun reste activé malgré la désactivation

- **Symptôme** : Les supports externes lancent automatiquement des programmes.
- **Solution** :
    - 1. Désactivez AutoRun via les politiques de groupe :
        - Ouvrez gpedit.msc et allez dans **Modèles d'administration > Composants Windows > Stratégies d'exécution automatique**.
        - Activez la politique **Désactiver l'exécution automatique** pour tous les lecteurs.
    - 2. Vérifiez les paramètres via le Panneau de configuration :
        - Allez dans **Matériel et audio > Exécution automatique** et décochez **Utiliser l'exécution automatique pour tous les médias**.

6. Annexes

- **Commandes utiles** :
    - Appliquer les stratégies immédiatement : gpupdate /force.
    - Vérifier les types de chiffrement Kerberos : klist.
- **Ressources supplémentaires** :
    - Documentation officielle Windows : Microsoft.

4. Documentation de dépannage pour la protection réseau sous Windows

0. Introduction

- Voici une documentation complète pour résoudre les problèmes courants liés à la configuration des signatures SMB/LDAP, des paramètres de sécurité réseau, et de la fonctionnalité SmartScreen.

1. Problème : Les signatures SMB ne s'activent pas

- **Symptôme** : Les paramètres configurés pour SMB (signatures numériques) ne prennent pas effet.
- **Solution** :
    - 1. Vérifiez les paramètres dans gpedit.msc :
        - Allez dans **Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité**.
        - Assurez-vous que les options suivantes sont activées :
            - **Client réseau Microsoft : communications signées numériquement (lorsque le serveur l'accepte)**.
            - **Client réseau Microsoft : communications signées numériquement (toujours)**.
    - 2. Redémarrez le système après avoir appliqué les modifications.
    - 3. Testez avec une commande PowerShell pour vérifier l'activation :
        - Get-SmbServerConfiguration | Select EnableSecuritySignature

2. Problème : Les modifications LDAP ne fonctionnent pas

- **Symptôme** : Les communications LDAP ne sont pas sécurisées malgré les configurations.
- **Solution** :
    - 1. Assurez-vous que la clé de registre **LDAPServerIntegrity** est correctement configurée :
        - Naviguez vers :

        - HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\NTDS\\Parameters
        - Créez ou modifiez la clé **LDAPServerIntegrity** en tant que DWORD avec une valeur de **2**.
    - 2. Redémarrez le système pour appliquer les changements.

3. Problème : Les utilisateurs locaux peuvent accéder à des ressources réseau non sécurisées

- **Symptôme** : Les comptes locaux accèdent à des ressources partagées sans restriction.
- **Solution** :
    - 1. Configurez les clés suivantes dans le registre :
        - Naviguez vers :
            - HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\LanmanWorkstation\\Parameters
        - Modifiez ou créez les valeurs suivantes :
            - **EnableSecuritySignature** : DWORD, valeur **1**.
            - **RequireSecuritySignature** : DWORD, valeur **1**.
    - 2. Redémarrez le système.

4. Problème : SmartScreen n'intercepte pas les téléchargements ou sites malveillants

- **Symptôme** : Les avertissements SmartScreen ne s'affichent pas.
- **Solution** :
    - 1. Vérifiez les paramètres SmartScreen dans **Paramètres > Sécurité Windows > Contrôle des applications et des navigateurs** :
        - Assurez-vous que les options suivantes sont activées :

        - **Vérifier les applications et les fichiers**.
        - **Bloquer les applications potentiellement indésirables**.
    - 2. Activez les stratégies via gpedit.msc :
        - Allez dans **Modèles d'administration > Composants Windows > Microsoft Edge**.
        - Configurez :
            - **Empêcher le contournement des avertissements de Windows Defender SmartScreen pour les fichiers → Activé**.
            - **Configurer Windows Defender SmartScreen → Activé**.
    - 3. Testez la fonctionnalité avec un fichier de test comme EICAR.

5. Annexes

- **Commandes utiles** :
    - Vérifier la configuration SMB : Get-SmbServerConfiguration.
    - Appliquer des modifications immédiates : gpupdate /force.
    - Vérifier les clés LDAP dans le registre.
- **Ressources supplémentaires** :
    - Documentation Microsoft sur SMB et SmartScreen : Microsoft.

5. Documentation de dépannage pour la configuration de Windows Defender

0. Introduction

- Voici une documentation complète pour résoudre les problèmes courants liés à l'activation et à la configuration de Windows Defender.

1. Problème : Windows Defender est désactivé

- **Symptôme** : Message "Votre antivirus est désactivé" ou impossibilité d'activer Windows Defender.
- **Solution** :
    - 1. Vérifiez si un autre antivirus est installé :
        - Désinstallez tout logiciel antivirus tiers via le panneau de configuration.
    - 2. Activez Windows Defender via PowerShell :
        - Set-MpPreference -DisableRealtimeMonitoring $false
    - 3. Redémarrez le système et vérifiez l'état dans **Paramètres > Mise à jour et sécurité > Sécurité Windows**.

2. Problème : Les protections avancées (exploits, ransomware) ne s'activent pas

- **Symptôme** : Les options comme l'accès contrôlé aux dossiers ou la protection contre les exploits sont grisées.
- **Solution** :
    - 1. Vérifiez les permissions administratives pour modifier les paramètres.
    - 2. Activez les fonctionnalités via PowerShell :
        - Set-MpPreference -EnableControlledFolderAccess Enabled
        - Set-ProcessMitigation -System -Enable
    - 3. Ajoutez des applications autorisées pour l'accès contrôlé aux dossiers si nécessaire :
        - Add-MpPreference -ControlledFolderAccessAllowedApplications "C:\\Path\\To\\Application.exe"

3. Problème : Windows Defender ne détecte pas les menaces

- **Symptôme** : Les scans ne trouvent pas de menaces malgré la présence de fichiers malveillants.
- **Solution** :
    - 1. Vérifiez si la base de signatures est à jour :
        - Update-MpSignature
    - 2. Exécutez une analyse complète via PowerShell :
        - Start-MpScan -ScanType FullScan
    - 3. Testez avec un fichier de test comme EICAR pour valider la détection.

4. Problème : Les analyses planifiées ne s'exécutent pas

- **Symptôme** : Les analyses configurées dans le planificateur de tâches ne s'exécutent pas.
- **Solution** :
    - 1. Ouvrez le Planificateur de tâches :
        - Appuyez sur Win + R, tapez taskschd.msc, et appuyez sur **Entrée**.
    - 2. Vérifiez les paramètres dans **Bibliothèque > Microsoft > Windows > Windows Defender**.
        - Double-cliquez sur **Windows Defender Scheduled Scan**.
        - Activez **Exécuter avec les autorisations maximales** et configurez les déclencheurs.
    - 3. Redémarrez le service de planification :
        - net stop schedule && net start schedule

5. Problème : Protection SmartScreen inactive

- **Symptôme** : Les téléchargements malveillants ne sont pas bloqués.
- **Solution** :
    - 1. Activez SmartScreen dans les paramètres :
        - **Paramètres > Sécurité Windows > Contrôle des applications et des navigateurs > SmartScreen**.
    - 2. Forcez l'activation via le registre :
        - Set-ItemProperty -Path "HKLM:\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer" -Name SmartScreenEnabled -Value RequireAdmin

6. Annexes

- **Commandes utiles** :
    - Mettre à jour Windows Defender : Update-MpSignature.
    - Exécuter un scan rapide : Start-MpScan -ScanType QuickScan.
    - Activer la protection contre les exploits : Set-ProcessMitigation -System -Enable.
- **Ressources supplémentaires** :
    - Documentation officielle Windows Defender : Microsoft.

6. Documentation de dépannage pour la journalisation des événements sous Windows

0. Introduction

- Voici une documentation détaillée pour résoudre les problèmes courants liés à la journalisation des événements Windows, incluant la gestion des journaux et la configuration avancée de la journalisation.

1. Problème : Les journaux atteignent leur limite de taille trop rapidement

- **Symptôme** : Les nouveaux événements écrasent les anciens journaux, entraînant une perte d'informations.
- **Solution** :
    - 1. Augmentez la taille maximale des journaux :
        - Ouvrez **eventvwr.msc**.
        - Cliquez droit sur le journal concerné (ex. : **Sécurité**) > **Propriétés**.
        - Modifiez la taille sous **Taille maximale du journal** (par ex. : 32 768 Ko).
    - 2. Activez l'option **Rempl.évén. si nécessaire (plus anciens en premier)** pour conserver les événements récents.
    - 3. Redémarrez le service **Journal des événements Windows** pour appliquer les modifications :
        - net stop eventlog && net start eventlog

2. Problème : Les commandes PowerShell ne sont pas enregistrées

- **Symptôme** : Les commandes exécutées dans PowerShell n'apparaissent pas dans les journaux d'événements.
- **Solution** :
    - 1. Activez la journalisation des scripts PowerShell :
        - Lancez gpedit.msc > **Modèles d'administration > Composants Windows > Windows PowerShell**.

        - Activez **Activer la journalisation de blocs de script PowerShell**.
        - Activez également **Enregistrer les scripts PowerShell**.
    - 2. Validez que les journaux apparaissent dans **Journaux des applications et des services > Microsoft > Windows > PowerShell**.

3. Problème : La journalisation des lignes de commande ne fonctionne pas

- **Symptôme** : Les arguments des commandes exécutées ne sont pas capturés.
- **Solution** :
    - 1. Ajoutez la clé suivante dans le registre pour inclure les lignes de commande :
        - reg add "HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\Audit" /v ProcessCommandLineInclude /t REG_DWORD /d 1 /f
    - 2. Redémarrez le système pour appliquer les modifications.

4. Problème : Les journaux sont vides ou inaccessibles

- **Symptôme** : Les journaux ne contiennent aucune donnée ou affichent une erreur lors de l'accès.
- **Solution** :
    - 1. Vérifiez les permissions des journaux :
        - Ouvrez **C:\Windows\System32\winevt\Logs**.
        - Assurez-vous que le groupe **Administrateurs** a les permissions nécessaires.
    - 2. Réparez les journaux corrompus :
        - wevtutil clear-log [NomDuJournal]

5. Problème : La journalisation des événements spécifiques échoue

- **Symptôme** : Les événements personnalisés ne sont pas enregistrés dans les journaux.
- **Solution** :
  - 1. Configurez les stratégies d'audit :
    - Lancez secpol.msc > **Stratégies locales > Stratégies d'audit**.
    - Activez les options **Réussite** et **Échec** pour les événements nécessaires (ex. : connexion, modification de fichiers).
  - 2. Vérifiez les journaux correspondants dans **Journaux des applications et services**.

6. Annexes

- **Commandes utiles** :
  - Vider un journal : wevtutil clear-log [NomDuJournal].
  - Lister les journaux disponibles : wevtutil el.
- **Ressources supplémentaires** :
  - Guide officiel Microsoft sur la journalisation : Microsoft.

7. Documentation de dépannage pour les mesures de sécurité avancées sous Windows

0. Introduction

- Voici une documentation complète pour résoudre les problèmes courants liés à la mise en œuvre des paramètres de sécurité avancés, y compris la journalisation étendue, les politiques d'audit, et la protection des scripts PowerShell.

1. Problème : Les paramètres avancés de sécurité ne s'appliquent pas

- **Symptôme** : Les commandes PowerShell ou les modifications du registre ne prennent pas effet.
- **Solution** :
    - 1. Vérifiez que les commandes PowerShell sont exécutées avec des privilèges administratifs :
        - Lancez PowerShell en tant qu'administrateur (clic droit > **Exécuter en tant qu'administrateur**).
    - 2. Redémarrez le système pour appliquer les modifications après avoir configuré les clés de registre ou exécuté les commandes.

2. Problème : La journalisation des scripts PowerShell ne fonctionne pas

- **Symptôme** : Les scripts PowerShell ne sont pas capturés dans les journaux d'événements.
- **Solution** :
    - 1. Activez la journalisation dans les stratégies locales :
        - Ouvrez gpedit.msc > **Modèles d'administration > Composants Windows > Windows PowerShell**.
        - Activez **Activer l'enregistrement des modules** et **Activer l'enregistrement des blocs de scripts**.
    - 2. Vérifiez que les journaux apparaissent dans :
        - **Applications et Services > Microsoft > Windows > PowerShell > Operational**.
    - 3. Activez la journalisation via le registre si nécessaire :
        - reg add "HKLM\\Software\\Policies\\Microsoft\\Windows\\PowerShell\\ScriptBlockLogging" /v EnableScriptBlockLogging /t REG_DWORD /d 1 /f

3. Problème : L'exécution de scripts non signés n'est pas bloquée

- **Symptôme** : Les scripts non signés peuvent encore être exécutés, même après avoir configuré la politique d'exécution.
- **Solution** :
    - 1. Configurez la politique d'exécution pour exiger une signature numérique :
        - Set-ExecutionPolicy AllSigned
    - 2. Vérifiez la politique actuelle :
        - Get-ExecutionPolicy
    - 3. Testez l'exécution d'un script non signé pour vérifier le blocage.

4. Problème : La commande AuditPol retourne des erreurs

- **Symptôme** : La commande AuditPol ne renvoie pas les politiques d'audit configurées.
- **Solution** :
    - 1. Exécutez la commande en tant qu'administrateur :
        - AuditPol /get /category:*
    - 2. Si le problème persiste, activez les catégories d'audit nécessaires dans secpol.msc :
        - **Stratégies locales > Stratégies d'audit**.

5. Problème : Les configurations DeviceGuard ne s'activent pas

- **Symptôme** : La clé de registre EnableVirtualizationBasedSecurity ne semble pas avoir d'effet.
- **Solution** :
    - 1. Assurez-vous que la virtualisation est activée dans le BIOS/UEFI.
    - 2. Activez DeviceGuard via le registre :

        - reg add "HKLM\\SYSTEM\\CurrentControlSet\\Control\\DeviceGuard" /v EnableVirtualizationBasedSecurity /t REG_DWORD /d 1 /f
    - 3. Redémarrez le système pour appliquer les modifications.

6. Annexes

- **Commandes utiles** :
    - Vérifier les politiques d'exécution : Get-ExecutionPolicy.
    - Activer les paramètres d'audit : AuditPol /get /category:*.
    - Activer la journalisation des scripts : Set-ExecutionPolicy AllSigned.
- **Ressources supplémentaires** :
    - Documentation officielle Windows PowerShell : Microsoft.

8. Documentation de dépannage pour la sécurisation de LSASS sous Windows

- Voici une documentation complète pour résoudre les problèmes courants liés à la sécurisation du processus LSASS (Local Security Authority Subsystem Service).

1. Problème : La configuration du mode protégé de LSASS échoue

- **Symptôme** : Impossible de modifier la clé de registre ou de définir la valeur **RunAsPPL**.
- **Solution** :
    - 1. Assurez-vous d'exécuter l'Éditeur du Registre en tant qu'administrateur :
        - Appuyez sur Win + R, tapez regedit, puis cliquez droit sur l'icône pour sélectionner **Exécuter en tant qu'administrateur**.
    - 2. Si la clé **RunAsPPL** n'existe pas, créez-la :

- 3. Naviguez vers :
  - HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Lsa
  - Cliquez droit > **Nouveau > Valeur DWORD (32 bits)** > Nommez-la **RunAsPPL**.
- 4. Assurez-vous que la valeur est définie sur **1** :
  - reg add "HKLM\\SYSTEM\\CurrentControlSet\\Control\\Lsa" /v RunAsPPL /t REG_DWORD /d 1 /f

2. Problème : LSASS ne fonctionne pas en mode protégé après redémarrage

- **Symptôme** : La commande PowerShell ne montre pas que LSASS est en mode protégé.
- **Solution** :
  - 1. Vérifiez que la virtualisation est activée dans le BIOS/UEFI.
  - 2. Vérifiez les journaux d'événements pour des erreurs LSASS :
    - Ouvrez **eventvwr.msc** et recherchez les événements liés à **LSA** ou **LSASS**.
  - 3. Si le problème persiste, réappliquez la configuration avec des privilèges administratifs :
    - Get-Process -Name lsass | Select-Object Name, Path

3. Problème : Les permissions pour la clé de registre LSA sont insuffisantes

- **Symptôme** : Vous recevez une erreur "Accès refusé" lors de la modification.
- **Solution** :
  - 1. Prenez possession de la clé :
    - Cliquez droit sur **Lsa** > **Autorisations > Avancé** > Changez le propriétaire en **Administrateurs**.
  - 2. Appliquez les permissions nécessaires :

- icacls "HKLM\\SYSTEM\\CurrentControlSet\\Control\\Lsa" /grant Administrators:F

4. Annexes

- **Commandes utiles** :
  - Vérifier le mode protégé de LSASS : Get-Process -Name lsass | Select-Object Name, Path.
  - Modifier les clés du registre : reg add "HKLM\\SYSTEM\\CurrentControlSet\\Control\\Lsa".
- **Ressources supplémentaires** :
  - Documentation Microsoft sur la sécurisation de LSASS : Microsoft.

10. Documentation de dépannage pour le pare-feu et le blocage des connexions sous Windows

0. Introduction

- Voici une documentation complète pour résoudre les problèmes courants liés à la configuration du pare-feu Windows et au blocage des connexions non autorisées.

1. Problème : Impossible d'activer le pare-feu Windows

- **Symptôme** : Le pare-feu Windows ne s'active pas ou affiche une erreur.
- **Solution** :
  - 1. Vérifiez que le service Pare-feu est en cours d'exécution :
    - net start mpssvc

- 2. Si le service ne démarre pas, réinitialisez le pare-feu :
  - netsh advfirewall reset
- 3. Redémarrez votre ordinateur et réessayez d'activer le pare-feu via le panneau de configuration.

2. Problème : Les règles personnalisées ne s'appliquent pas

- **Symptôme** : Les connexions ciblées par des règles restent ouvertes ou non bloquées.
- **Solution** :
  - 1. Vérifiez si les règles sont bien configurées :
    - Accédez à **Paramètres avancés** dans le pare-feu Windows et assurez-vous que les règles sont activées.
  - 2. Réappliquez les règles via PowerShell :
    - New-NetFirewallRule -DisplayName "Blocage PowerShell" -Direction Outbound -Program "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe" -Action Block
  - 3. Redémarrez le pare-feu pour recharger les règles :
    - netsh advfirewall reload

3. Problème : Notifications absentes lors du blocage

- **Symptôme** : Aucune alerte n'est affichée lorsque le pare-feu bloque une connexion.
- **Solution** :
  - 1. Activez les notifications dans **Paramètres > Pare-feu Windows Defender > Notifications**.
  - 2. Vérifiez que la règle correspondante est configurée pour alerter en cas de blocage :
    - Modifiez la règle et cochez l'option **M'avertir lors d'un blocage**.

4. Problème : Le port 445 ou d'autres ports sensibles ne sont pas bloqués

- **Symptôme** : Les connexions sur des ports tels que 445 (SMB) restent actives.
- **Solution** :
    - 1. Créez une règle de blocage dans le pare-feu :
        - Allez dans **Règles de trafic entrant > Nouvelle règle > Port**.
        - Sélectionnez **TCP** et entrez le port **445**.
        - Configurez l'action sur **Bloquer la connexion**.
    - 2. Répétez ce processus pour d'autres ports sensibles :
        - Bloquez **23 (Telnet)**.
        - Autorisez **22 (SSH)**, **80 (HTTP)**, et **443 (HTTPS)**.

5. Problème : Les binaires spécifiques (LOLBins) ne sont pas bloqués

- **Symptôme** : Des outils comme PowerShell ou certutil.exe restent accessibles malgré les règles.
- **Solution** :
    - 1. Vérifiez le chemin complet du binaire ciblé (par exemple, PowerShell) et configurez une règle de blocage :
        - New-NetFirewallRule -DisplayName "Blocage PowerShell" -Direction Outbound -Program "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe" -Action Block
    - 2. Testez l'exécution des binaires bloqués pour valider les règles.

6. Annexes

- **Commandes utiles** :
  - Réinitialiser le pare-feu : netsh advfirewall reset.
  - Ajouter une règle via PowerShell : New-NetFirewallRule.
- **Ressources supplémentaires** :
  - Documentation officielle Microsoft sur le pare-feu : Microsoft.

11. Documentation de dépannage pour la gestion des mises à jour Windows

0. Introduction

- Voici une documentation complète pour résoudre les problèmes courants liés à l'activation et à la configuration des mises à jour automatiques sur Windows.

1. Problème : Les mises à jour automatiques ne fonctionnent pas

- **Symptôme** : Windows Update ne télécharge pas ou n'installe pas les mises à jour automatiquement.
- **Solution** :
  - 1. Vérifiez que le service Windows Update est actif :
    - Appuyez sur Win + R, tapez services.msc, et trouvez **Windows Update**.
    - Assurez-vous que le **Type de démarrage** est défini sur **Automatique (Démarrage différé)**.
  - 2. Réinitialisez Windows Update :
    - net stop wuauserv
    - net start wuauserv

- 3. Recherchez les mises à jour manuellement dans **Paramètres > Mise à jour et sécurité > Windows Update**.

2. Problème : Les mises à jour restent bloquées pendant le téléchargement

- **Symptôme** : Le téléchargement des mises à jour reste figé ou affiche un message d'erreur.
- **Solution** :
  - 1. Supprimez le cache de Windows Update :
    - Arrêtez le service Windows Update :
      - net stop wuauserv
    - Supprimez le contenu du dossier de cache :
      - del /s /q %windir%\\SoftwareDistribution
    - Redémarrez le service :
      - net start wuauserv
  - 2. Redémarrez le système et relancez le téléchargement des mises à jour.

3. Problème : Windows Update provoque des redémarrages inopportuns

- **Symptôme** : Le système redémarre sans prévenir après une mise à jour.
- **Solution** :
  - 1. Configurez les heures actives :
    - Allez dans **Paramètres > Mise à jour et sécurité > Windows Update > Modifier les heures d'activité**.
    - Définissez une plage horaire pour empêcher les redémarrages automatiques pendant les heures de travail.
  - 2. Désactivez les redémarrages automatiques via les stratégies de groupe :

- Lancez gpedit.msc > **Modèles d'administration > Composants Windows > Windows Update > Configurer les redémarrages automatiques**.
- Activez cette option et configurez-la selon vos besoins.

4. Problème : Les mises à jour ne concernent pas d'autres produits Microsoft

- **Symptôme** : Les mises à jour Office ou des autres logiciels Microsoft ne sont pas téléchargées.
- **Solution** :
  - 1. Activez l'option dans **Paramètres > Mise à jour et sécurité > Windows Update > Options avancées**.
  - 2. Cochez **Recevoir des mises à jour pour d'autres produits Microsoft**.

5. Problème : Les mises à jour sont lentes ou échouent fréquemment

- **Symptôme** : Le processus de mise à jour prend du temps ou affiche des messages d'erreur.
- **Solution** :
  - 1. Vérifiez la connexion réseau et assurez-vous qu'elle est stable.
  - 2. Lancez l'outil de résolution des problèmes intégré :
    - Allez dans **Paramètres > Mise à jour et sécurité > Résolution des problèmes > Windows Update**.
  - 3. Si nécessaire, utilisez l'outil de dépannage Microsoft :
    - Exécutez l'outil de réparation de Windows Update depuis Microsoft.

6. Annexes

- **Commandes utiles** :
  - Réinitialiser Windows Update : net stop wuauserv && net start wuauserv.
  - Supprimer le cache de mise à jour : del /s /q %windir%\\SoftwareDistribution.
- **Ressources supplémentaires** :
  - Guide officiel Windows Update : Microsoft.

12. Documentation de dépannage pour la création d'un utilisateur standard sous Windows

0. Introduction

- Voici une documentation complète pour résoudre les problèmes courants liés à la création, à la configuration et à la vérification d'un compte utilisateur standard.

1. Problème : Impossible d'ouvrir la gestion des utilisateurs

- **Symptôme** : La commande lusrmgr.msc retourne une erreur ou l'outil ne s'ouvre pas.
- **Solution** :
  - 1. Vérifiez que vous utilisez une édition compatible de Windows (Pro ou Entreprise).
  - 2. Lancez lusrmgr.msc avec des droits administratifs :
    - Appuyez sur Win + R, tapez cmd, puis utilisez la commande suivante :
      - runas /user:Administrateur "mmc lusrmgr.msc"

2. Problème : L'utilisateur standard n'est pas créé

- **Symptôme** : La création de l'utilisateur via l'interface échoue.
- **Solution** :
    - 1. Utilisez la ligne de commande pour créer l'utilisateur :
        - net user NomUtilisateur /add
        - net localgroup Users NomUtilisateur /add
    - 2. Vérifiez que l'utilisateur apparaît dans la liste :
        - net user

3. Problème : L'utilisateur standard a des droits administratifs

- **Symptôme** : L'utilisateur peut effectuer des tâches réservées aux administrateurs.
- **Solution** :
    - 1. Retirez l'utilisateur du groupe Administrateurs :
        - net localgroup Administrateurs NomUtilisateur /delete
    - 2. Assurez-vous qu'il appartient uniquement au groupe Utilisateurs :
        - net localgroup Users NomUtilisateur /add

4. Problème : Les paramètres de sécurité ne s'appliquent pas au nouvel utilisateur

- **Symptôme** : Les restrictions configurées via gpedit.msc ou secpol.msc ne sont pas effectives.
- **Solution** :
    - 1. Mettez à jour les stratégies via la commande suivante :
        - gpupdate /force
    - 2. Assurez-vous que les paramètres sont correctement configurés :
        - **secpol.msc → Stratégies locales > Attribution des droits utilisateur**.

- **gpedit.msc → Modèles d'administration > Composants Windows**.

5. Problème : Les tests de privilèges échouent

- **Symptôme** : L'utilisateur peut toujours accéder à des paramètres ou effectuer des actions administratives.
- **Solution** :
  - 1. Connectez-vous avec le nouvel utilisateur et tentez les actions suivantes :
    - Installer une application.
    - Modifier les paramètres système avancés.
  - 2. Si l'utilisateur peut effectuer ces actions, vérifiez son appartenance aux groupes avec :
    - net localgroup NomUtilisateur
  - 3. Appliquez les restrictions manquantes via gpedit.msc ou secpol.msc.

6. Problème : Les notifications et animations au démarrage persistent

- **Symptôme** : Les animations de première connexion ou les notifications Windows sont actives.
- **Solution** :
  - 1. Désactivez les paramètres via gpedit.msc :
    - **Modèles d'administration > Système > Ouverture de session**.
    - Configurez **Désactiver l'animation à la première connexion** sur **Activé**.
  - 2. Répétez pour les paramètres des notifications :
    - **Composants Windows > Contenu cloud** :
      - Désactiver les expériences consommateur : **Activé**.

7. Annexes

- **Commandes utiles** :
  - Créer un utilisateur standard : net user NomUtilisateur /add.
  - Retirer un utilisateur des administrateurs : net localgroup Administrateurs NomUtilisateur /delete.
  - Forcer l'application des stratégies : gpupdate /force.
- **Ressources supplémentaires** :
  - Documentation officielle Microsoft : Microsoft.

4. Bibliographie Windows

Introduction

- Pour renforcer la sécurité de votre système Windows, voici une liste d'actions recommandées avec leurs tutoriels et aides détaillés.

0. Création d'une machine virtuelle (VM) dans VMware :

- Bien configurer votre machine virtuelle est très importante pour le reste de l'installation.
    - Aide 1: IT-Connect
    - Aide 2: VMware tools
    - Aide 3: Malekal

1. Paramètres biométriques et d'écran de verrouillage :

- Configuration de la sécurité biométrique car cela est essentielle pour limiter les risques d'accès non autorisé via l'écran de connexion.
    - Aide 1: Microsoft
    - Aide 2: Zebulon
    - Aide 3: Admx
    - Aide 4: Youtube

2. DNS et sécurité réseau :

- Configuration des paramètres DNS et réseau pour renforcer la sécurité du système.
    - Aide 1: Rickardnobel

- Aide 2: Superuser
- Aide 3: Dartmouth
- Aide 4: Microsoft
- Aide 5: Ionos
- Aide 6: Articuate
- Aide 7: Youtube

3. Sécurité des mots de passe et de l'authentification :

- Application des politiques renforcées pour les mots de passe et l'authentification afin de minimiser les risques liés aux comptes utilisateurs.

- Aide 1: Microsoft
- Aide 2: Microsoft
- Aide 3: InfoSecInstitute
- Aide 4: Logpoint
- Aide 5: FireSecure
- Aide 6: TenForums
- Aide 7: Lenovo support

4. Protection réseau :

- Activation des paramètres pour la protection du réseau pour protéger les utilisateurs contre les sites malveillants.

- Aide 1: Microsoft
- Aide 2: Microsoft
- Aide 3: Youtube

5. Configuration de Windows Defender :

- Configuration de Windows Defender contre les logiciels malveillants, les exploits, et autres menaces en ligne.

- Aide 1: WikiHow
- Aide 2: Microsoft
- Aide 3: BytePlus

BIBLIOGRAPHIE

6. Journalisation des évènements Windows :

- Journalisation des évènements pour surveiller les activités du système, détecter les comportements suspects, et conserver des preuves en cas d'incident de sécurité.
    - Aide 1: Malekal
    - Aide 2: It-Connect
    - Aide 3: Microsoft

7. Mesures de sécurite avancées :

- Renforcement de la sécurité du système.
    - Aide 1: Microsoft
    - Aide 2: Admx
    - Aide 3: RdpGuard
    - Aide 4: Automox

8. Securisation de Lsass :

- Sécurisation de Lsass pour renforcer la sécurité pour empêcher le vol d'identifiants.
    - Aide 1: Youtube

9. Gestion des applications :

- Suppression des applications indésirables.
    - Aide 1: Malekal
    - Aide 2: Pages-informatique

10. Pare-feu et Blocage des Connexions :

- Renforcement du réseau pour bloquer des connexions non autorisées.

Aide 1: OVHCloud

11. Gestion des mises a jour Windows :

- Maintiens d'un système à jour pour éviter certaines failles de sécurité.
    - Aide 1: Microsoft

12. Creation d'un utilisateur standard pour la mise en production :

- Désactivation du compte administrateur par un compte utilisateur standard ce qui réduit les risques de sécurité et suit les bonnes pratiques de déploiement.
    - Aide 1: Malekal

13. Installation des logiciels pour Windows 10 :

- Installations des logiciels bureautique pour la productivité des employés.
    - Aide 1: Chocolatey
    - Aide 2: UniGetUI
    - Aide 3: LeCrabeInfo

14. Securisation de MS Office :

- Sécurisation de Office ainsi que de ses applications afin d'éviter les vulnérabilités.
    - Aide 1: Microsoft
    - Aide 2: Appvizer

BIBLIOGRAPHIE

15. Masterisation du poste Windows 10 :

- Déploiement de l'image afin de faciliter la tâche.

    - Aide 1: Malekal
    - Aide 2: Rescuzilla

16. Chiffrement de disque avec BitLocker :

- Chiffrement du disque afin de protéger les fuites de données ainsi que de potentielle attaque.

    - Aide 1: Youtube
    - Aide 2: IT-connect
    - Aide 3: Atera

17. Activation de la cle Windows 10 :

- Activation de Windows 10 Entreprise pour bénéficier de toutes les fonctionnalités.

    - Aide 1: Easeus

00. Installation de Linux Mint sur VMware

0.Introduction

Les machines virtuelles sont des outils puissants qui permettent d'exécuter plusieurs systèmes d'exploitation sur un même appareil, sans avoir besoin de matériel supplémentaire. Elles sont particulièrement utiles pour des usages tels que le test d'applications, la formation, ou encore la création d'environnements isolés pour le développement et les expérimentations. Dans le cadre de ce guide, vous apprendrez à créer une machine virtuelle pour Linux Mint, ce qui peut être utile pour tester des applications, configurer des environnements de développement ou garantir une isolation pour des activités sensibles.

Voici un guide détaillé pour créer une machine virtuelle (VM) dans **VMware Workstation** ou **VMware Player**.

---

1. Ouvrir VMware Workstation/Player

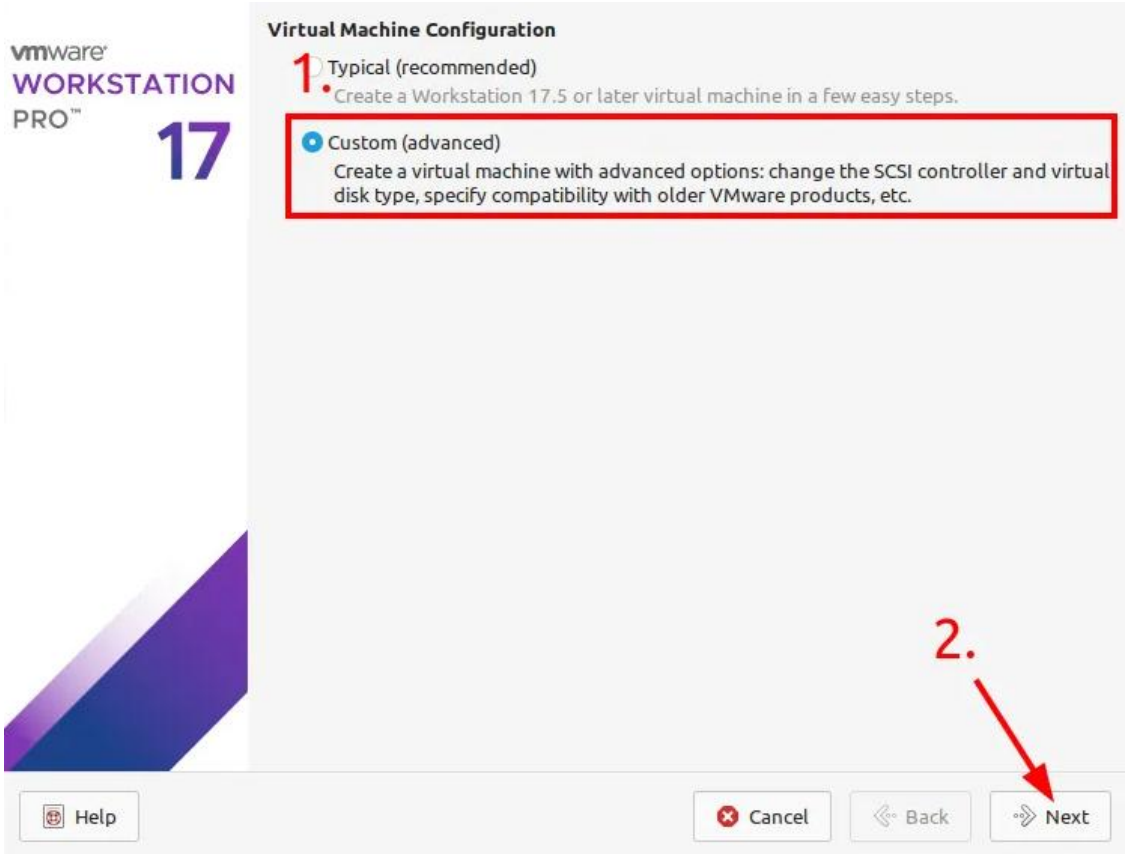
1. Lancez VMware Workstation ou VMware Player sur votre poste.
2. Sur l'écran principal, cliquez sur **Create a New Virtual Machine** (Créer une nouvelle machine virtuelle).

---

2. Sélection du type de configuration

1. Une fenêtre s'ouvre vous demandant de choisir entre :
    - **Typical (recommended)** : pour une configuration rapide.
    - **Custom (advanced)** : pour plus de personnalisation.

   Action :
    - Sélectionnez **Custom (advanced)** *(1)* puis cliquez sur **Next**. *(2)*
    - Cliquez à nouveau sur **Next**.



22-11-2024_09-27-05.png

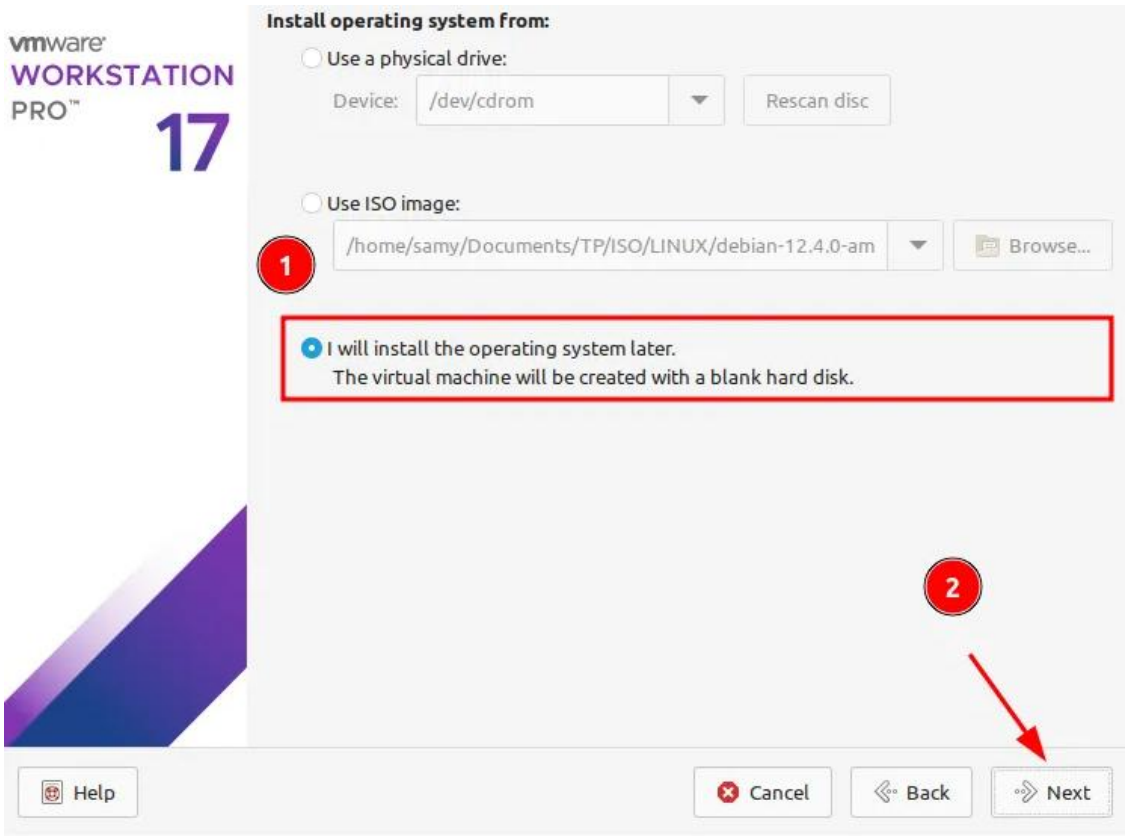
---

3. Choisir la source du système d'exploitation

1. Trois options apparaissent :
    - **i will install the operating system later** : choisissez cette option si vous voulez configurer la VM et installer l'OS plus tard.
    - **Use ISO image** : pour installer un système à partir d'un fichier ISO (par exemple, Linux Mint).
    - **Use a physical drive** : pour installer l'OS depuis un disque physique.

Action :

- Sélectionnez **I will install the operating system later.** *(1)*
- Cliquez sur **Next**. *(2)*



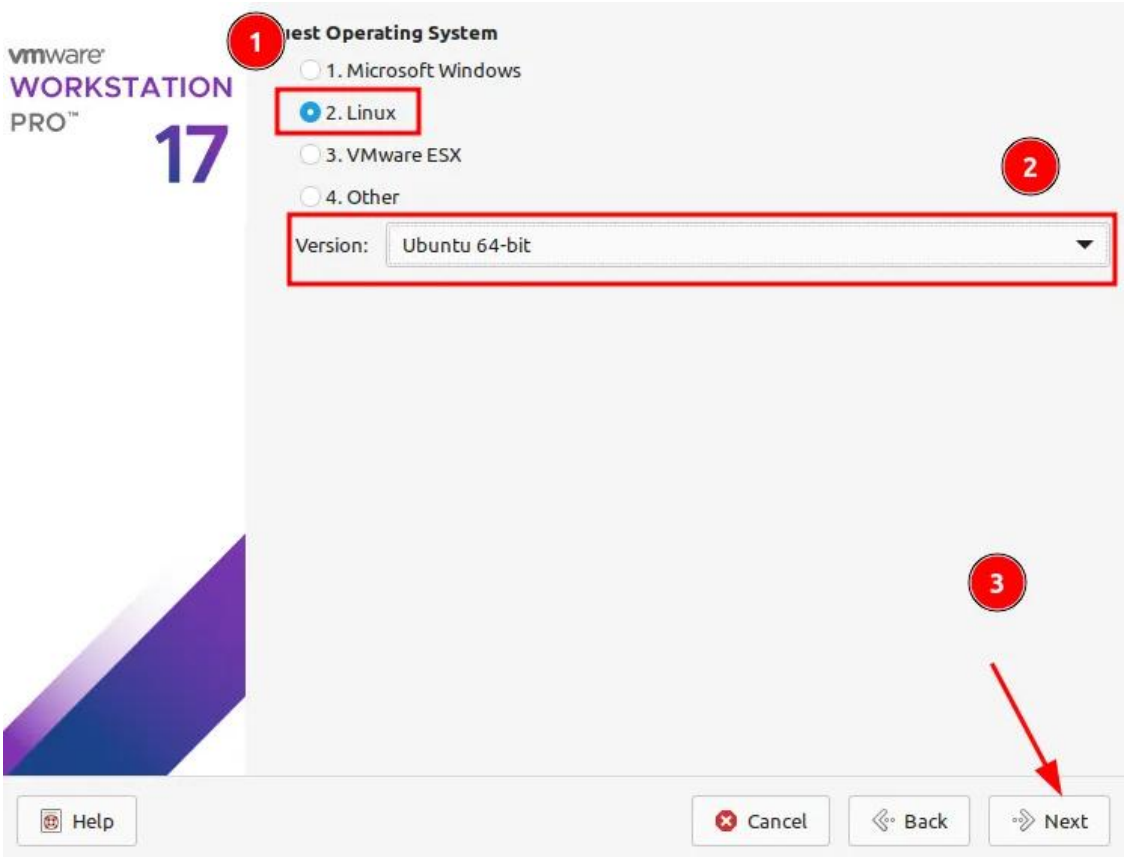
22-11-2024_10-25-31.png

---

4. Sélectionner le système d'exploitation invité

1. Dans la liste, choisissez **Linux**. *(1)*
2. Dans le menu déroulant, sélectionnez la version correspondante, par exemple : **Ubuntu 64-bit**. *(2)*

   Action : Cliquez sur **Next**. *(3)*



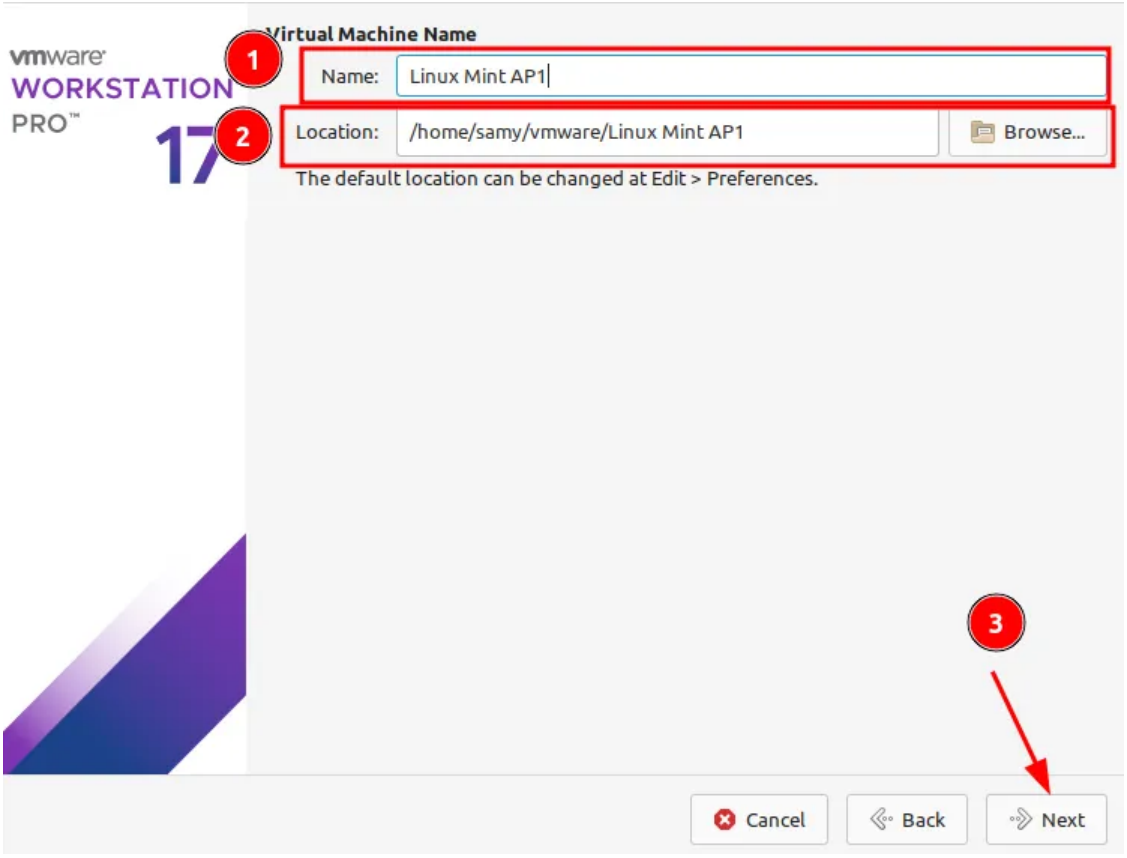
22-11-2024_10-27-32.png

---

5. Nommer la VM et choisir l'emplacement

1. **Name :** Donnez un nom significatif à votre VM, par exemple : `Linux Mint AP1`. *(1)*
2. **Location :** Cliquez sur **Browse** pour choisir où les fichiers de la VM seront enregistrés. *(2)*

   Action : Cliquez sur **Next**. *(3)*



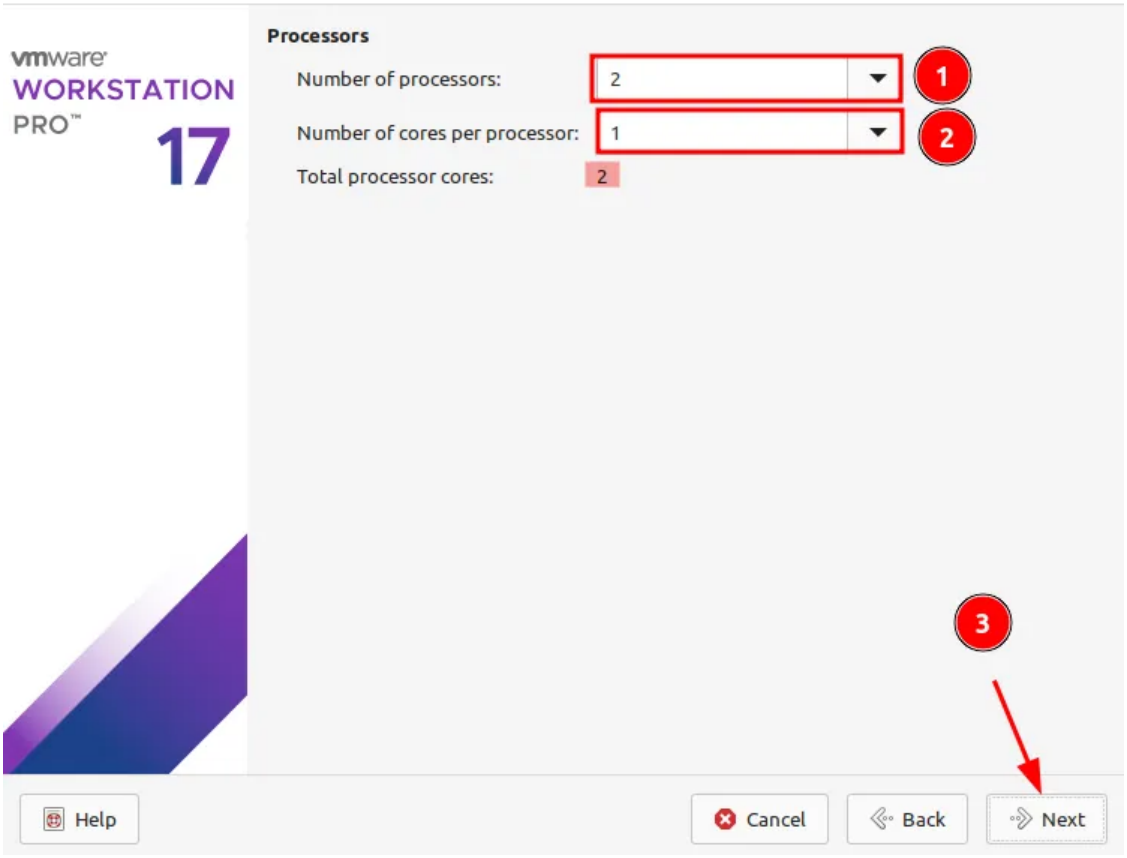
22-11-2024_10-30-14.png

---

6. Configurer le processeur

1. **Number of processors :** Sélectionnez le nombre de processeurs utilisés pour la machine (par exemple, **2**). *(1)*
2. **Number of cores per processor :** Sélectionnez le nombre de cœurs par processeur (par exemple, **1**). *(2)*

   Action : Cliquez sur **Next**. *(3)*



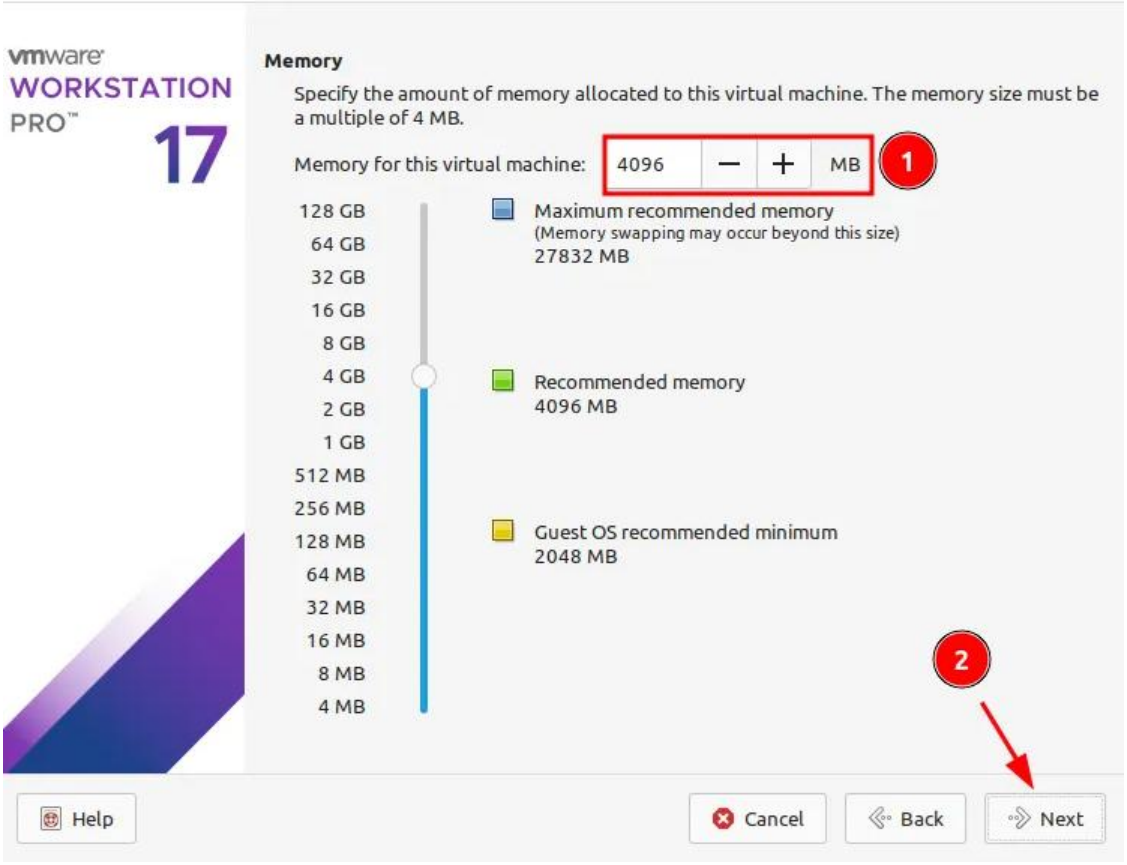
22-11-2024_10-35-54.png

---

7. Configurer la mémoire

1. Réglez la mémoire souhaitée pour le système en utilisant le curseur ou le champ numérique sous **Memory for this virtual machine** (par exemple, **4096 MB** pour 4 Go). *(1)*

   Action : Cliquez sur **Next**. *(2)*



22-11-2024_10-38-11.png

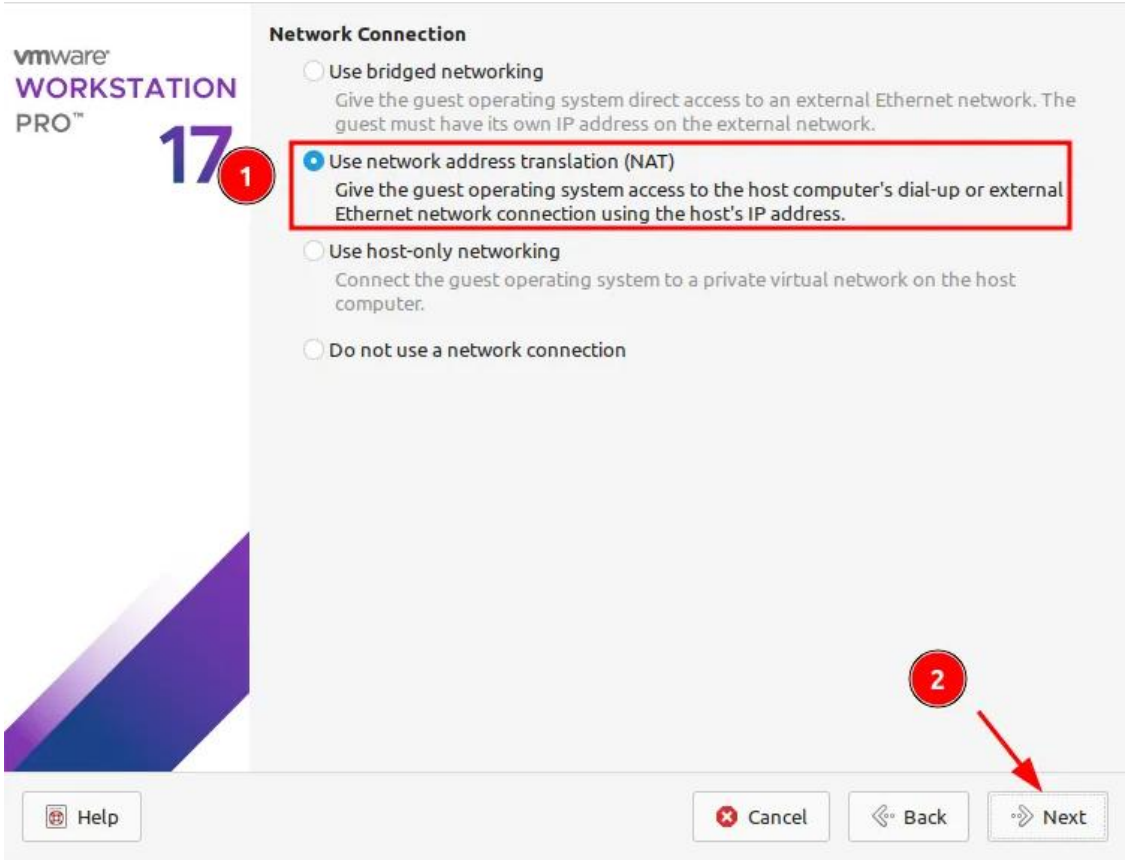
---

8. Configuration du réseau

1. Quatre options apparaissent :
    - **Use bridged networking** : pour connecter directement au réseau physique.
    - **Use network address translation (NAT)** : pour accéder à Internet via l'hôte.
    - **Use host-only networking** : pour isoler la VM sur un réseau privé local.
    - **Do not use a network connection** : pour créer une VM sans connexion réseau.

Action :

- Sélectionnez **Use network address translation (NAT)**. *(1)*
- Cliquez sur **Next**. *(2)*



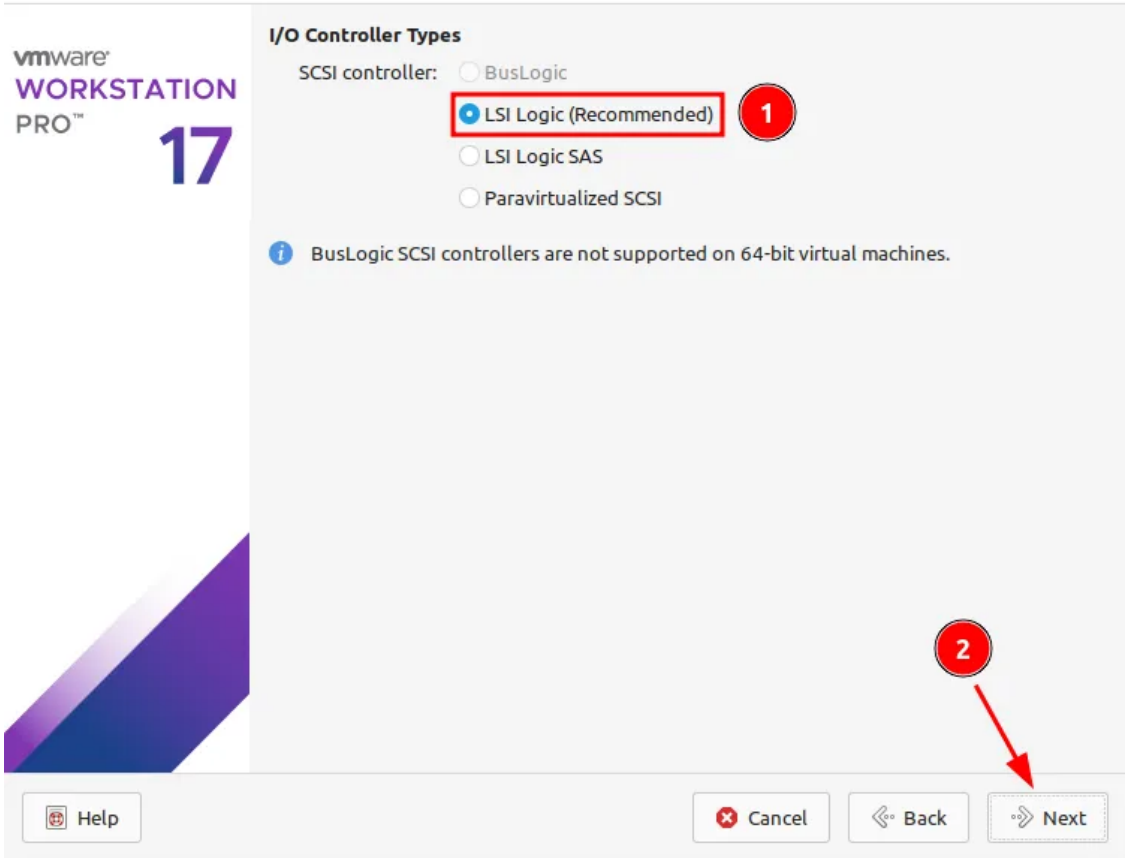
22-11-2024_10-39-00.png

---

9. Configuration du contrôleur d'E/S

1. Trois options apparaissent pour le contrôleur SCSI :
   - **LSI Logic (Recommended)** : par défaut.
   - **LSI Logic SAS** : pour des systèmes avancés.
   - **Paravirtualized SCSI** : pour des performances spécifiques.

   Action :
   - Choisissez **LSI Logic (Recommended)**. *(1)*
   - Cliquez sur **Next**. *(2)*

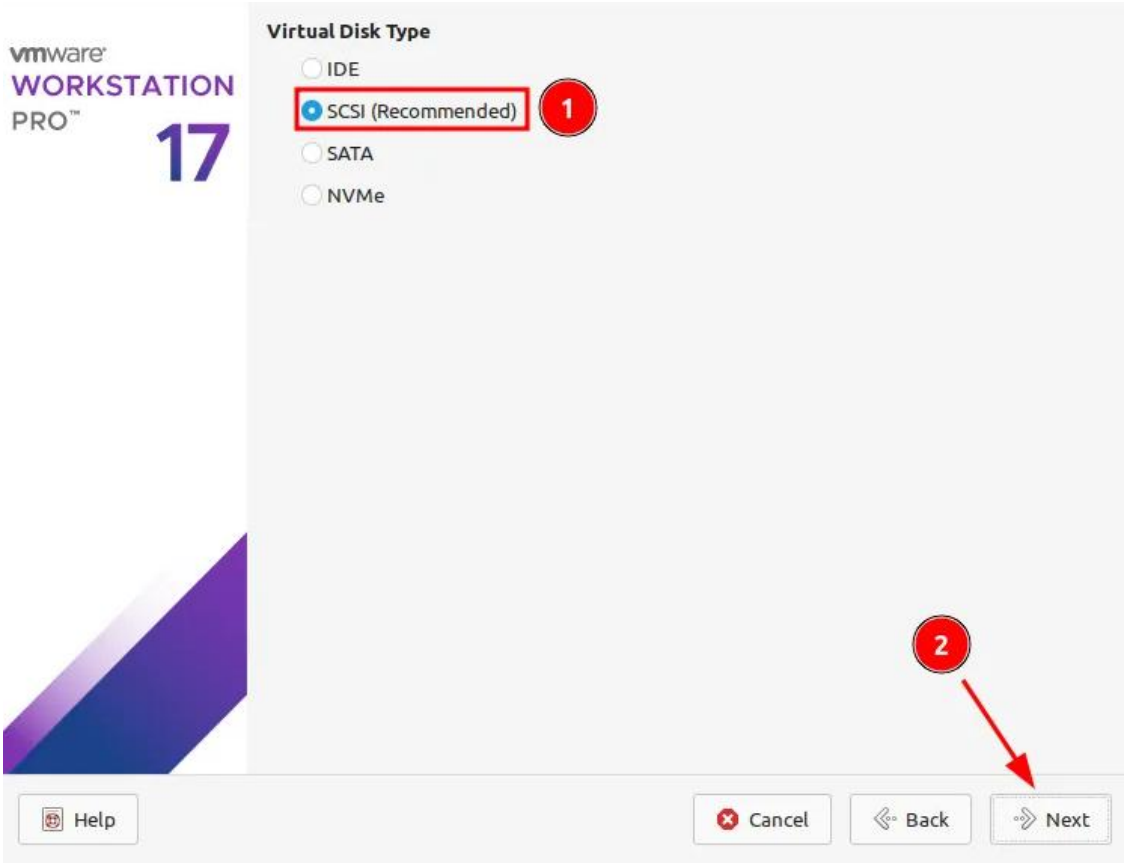


22-11-2024_10-40-36.png

---

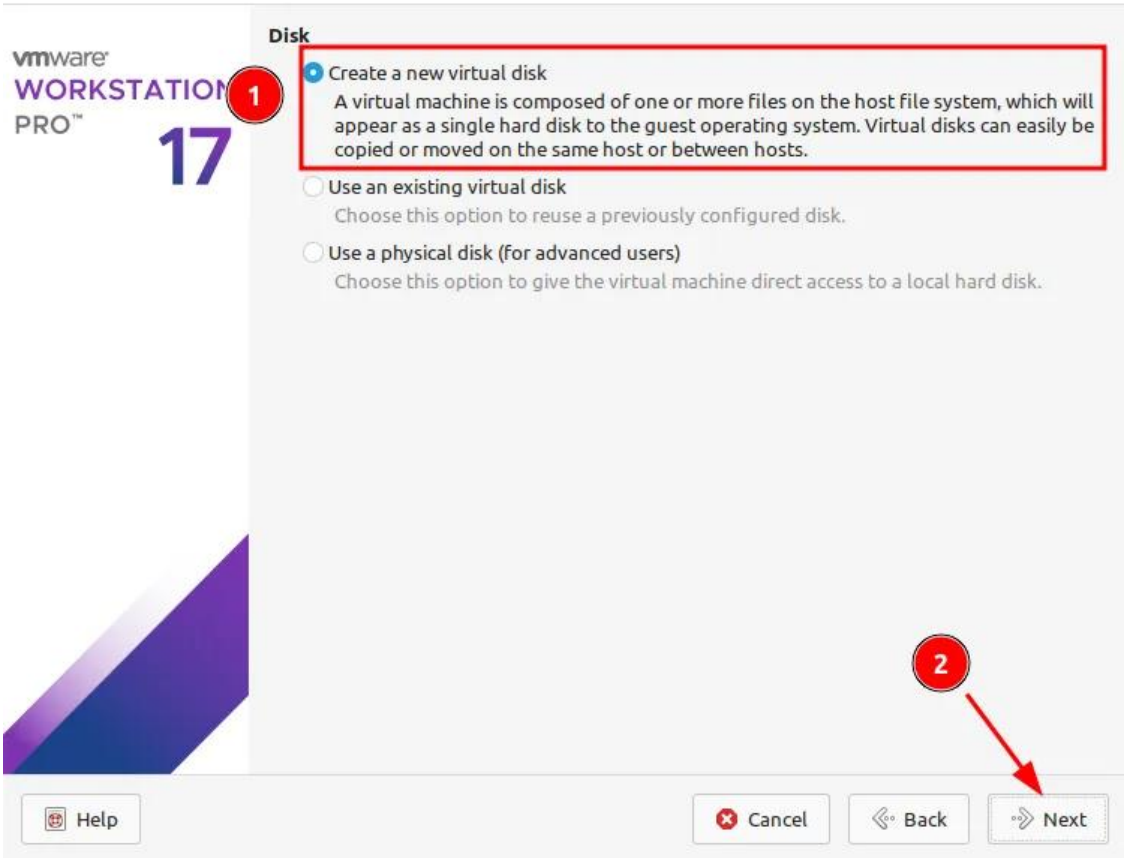
10. Configurer le disque dur

1. **Virtual disk type :** Sélectionnez **SCSI (Recommended)** *(1)*, puis cliquez sur **Next**. *(2)*



22-11-2024_10-43-10.png

2. **Disk :** Sélectionnez **Create a new virtual disk** *(1)*, puis cliquez sur **Next**. *(2)*

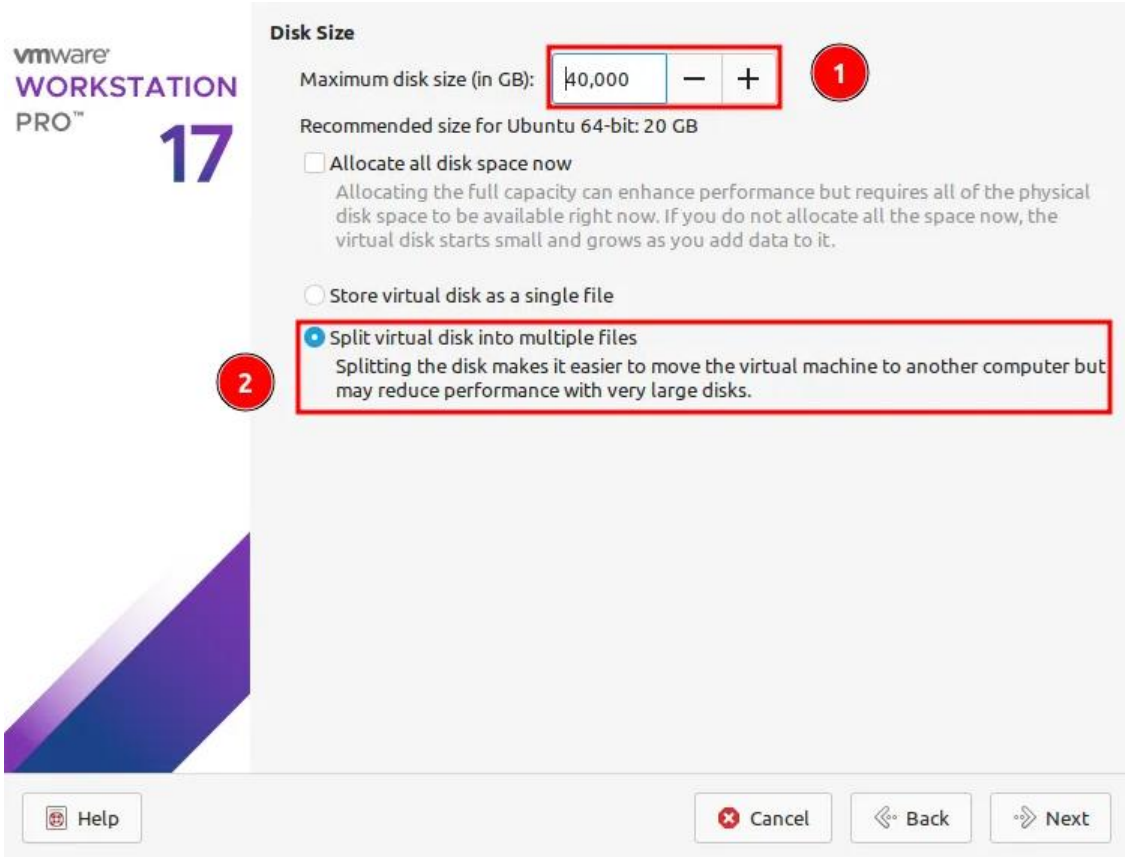


22-11-2024_10-43-52.png

3. **Maximum Disk Size :** Entrez une taille (par exemple, **40 Go**). *(1)*
4. **Stockage :**
    - **Store virtual disk as a single file** : stocke le disque virtuel en un seul fichier (plus rapide, mais moins flexible).
    - **Split virtual disk into multiple files** : divise le disque virtuel en plusieurs fichiers (meilleur pour la portabilité).

Action :

- Choisissez **Split virtual disk into multiple files** *(2)* et cliquez sur **Next**.
- Cliquez à nouveau sur **Next**.
- Cliquez sur **Finish**.

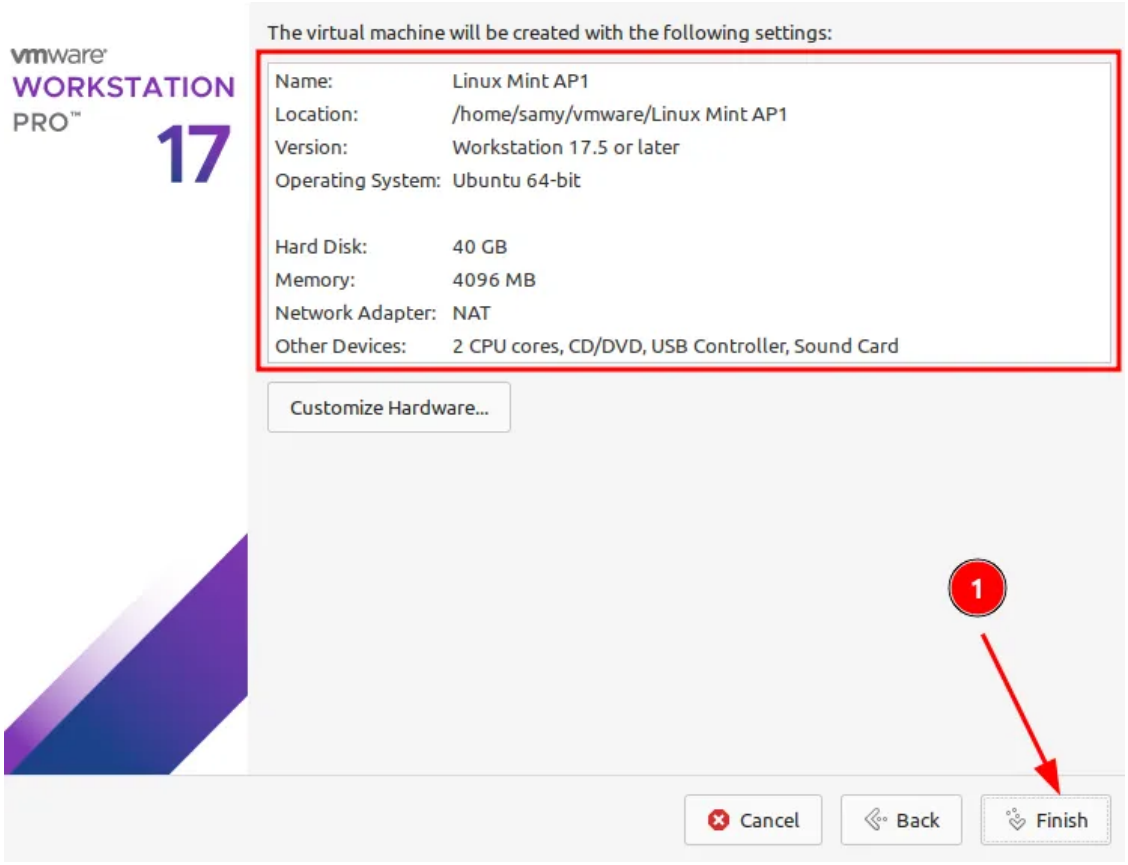


22-11-2024_10-45-45.png

---

11. Vérification et personnalisation

1. VMware affiche un résumé de la configuration choisie.
2. Cliquez sur **Customize Hardware** pour ajuster les paramètres : **Action :** Après personnalisation, cliquez sur **Close**, puis sur **Finish**. *(1)*
    - **Memory :** La mémoire allouée à la VM est cruciale pour les performances. Par exemple, allouez au moins **4 Go (4096 Mo)** pour une utilisation fluide de Linux Mint.
    - **Processors :** Le nombre de processeurs et de cœurs par processeur détermine la vitesse d'exécution des tâches. Il est recommandé d'utiliser au moins **2 cœurs**.
    - **Network Adapter :** Configurez le mode réseau sur **NAT** pour un accès Internet ou **Host-Only** pour isoler la VM du réseau principal. **Action :** Après personnalisation, cliquez sur **Close**, puis sur **Finish**. *(1)*



22-11-2024_10-47-24.png

---

12. Lancement de la VM

1. Dans VMware, sélectionnez la VM que vous venez de créer.
2. Cliquez sur **CD/DVD (SATA)**. *(1)*
3. Cliquez sur **Use ISO image**, puis sur **Browse…** *(2)*
4. Cliquez sur **Save** *(3)*
5. Cliquez sur le bouton **démarrer** *(4)* pour démarrer la machine virtuelle.

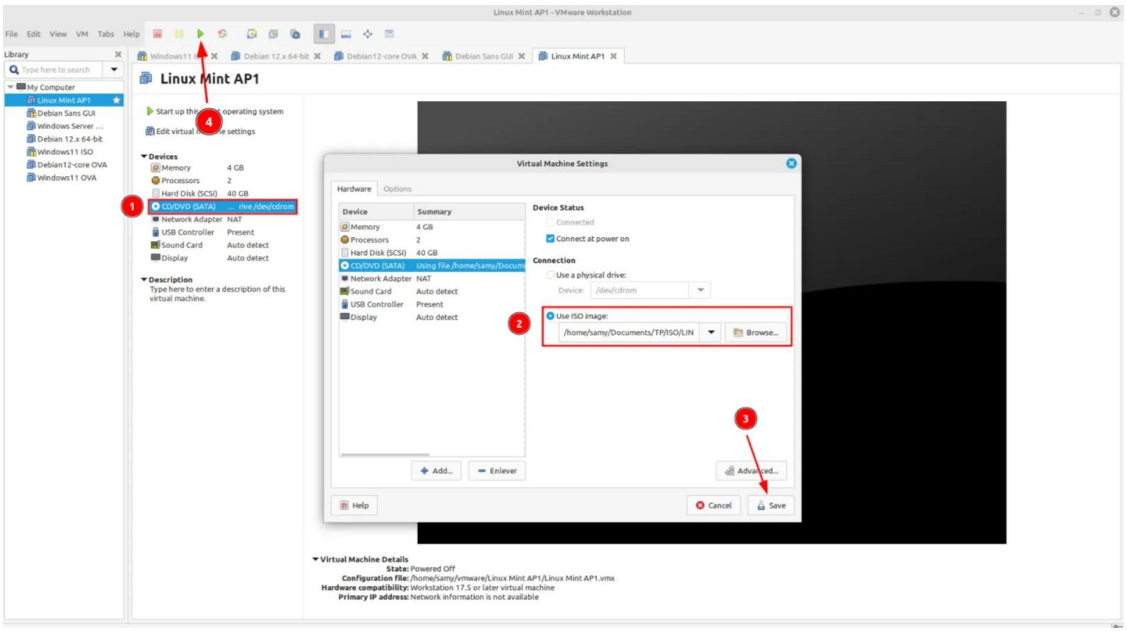


image.png

---

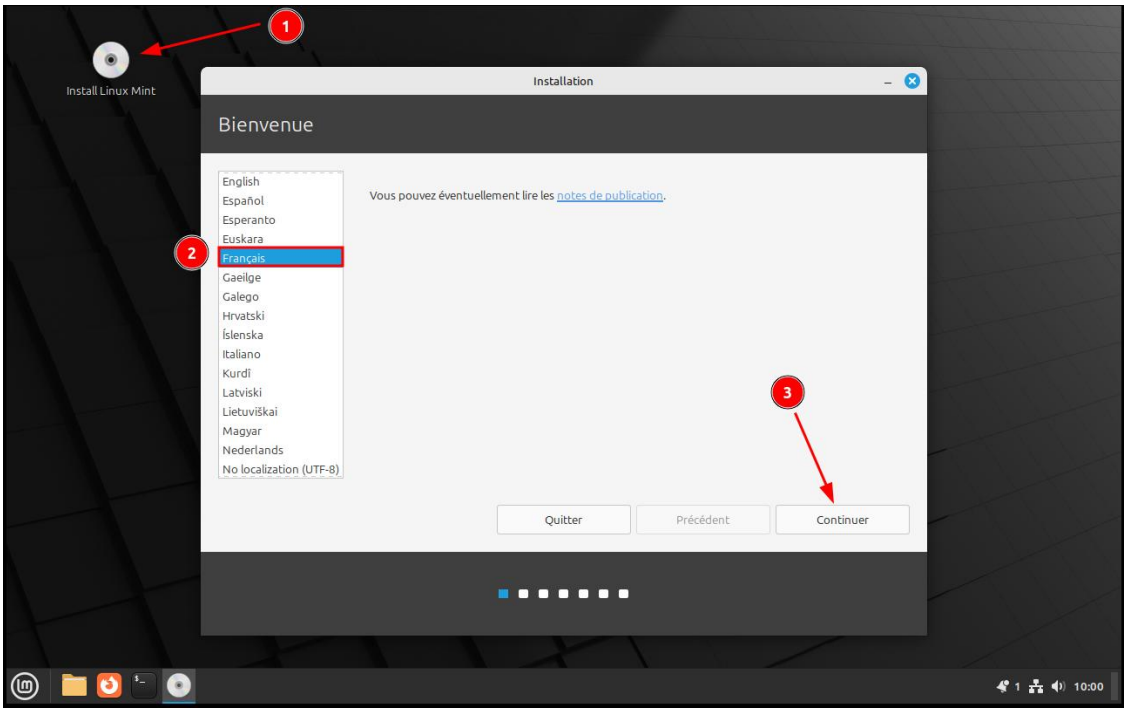
13. Installation de Linux Mint

1. Appuyez plusieurs fois sur la touche **Entrée**.
2. Cliquez sur **Start Linux Mint**.

22-11-2024_10-55-49.png

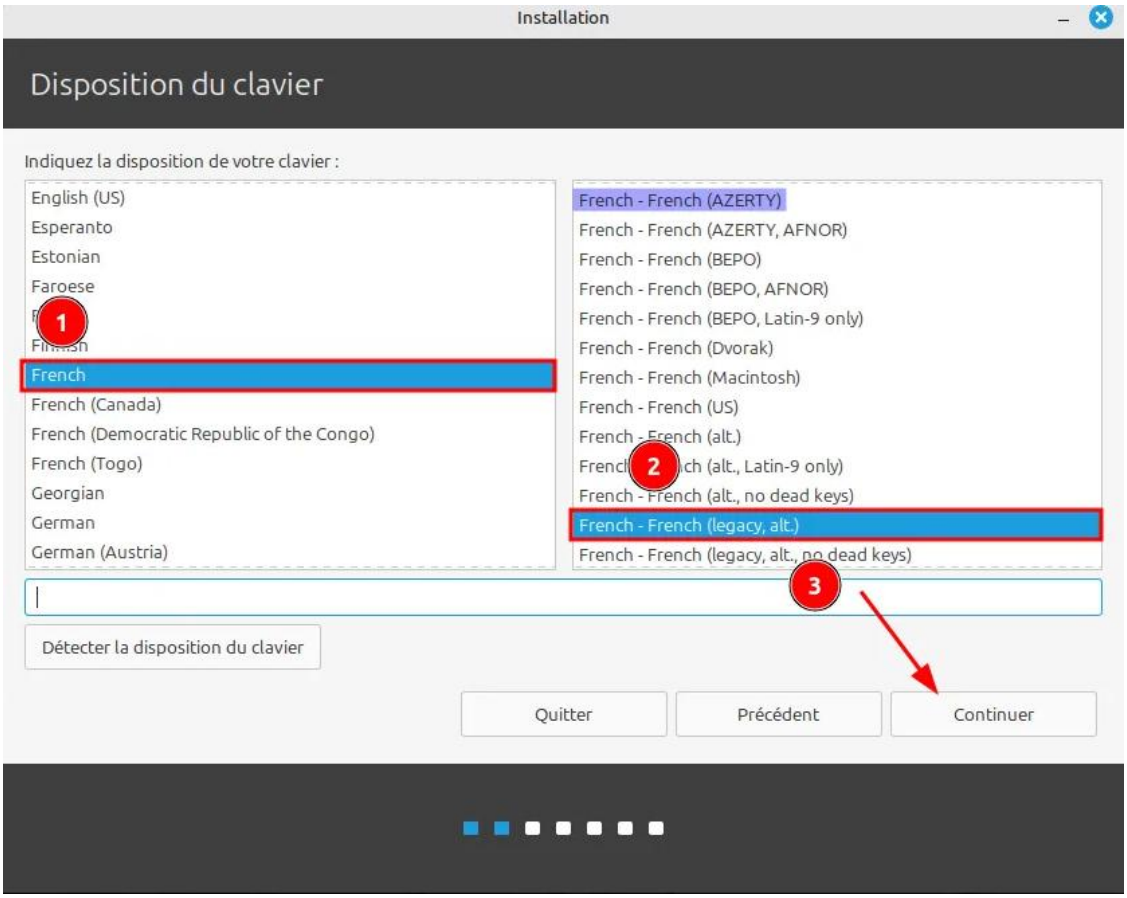
3. Une fois arrivé sur le bureau de Linux Mint, cliquez sur l'icône **Install Linux Mint**. *(1)*

4. Ensuite, dans le menu de sélection de langue, choisissez **Français** *(2)*, puis cliquez sur **Continuer**. *(3)*



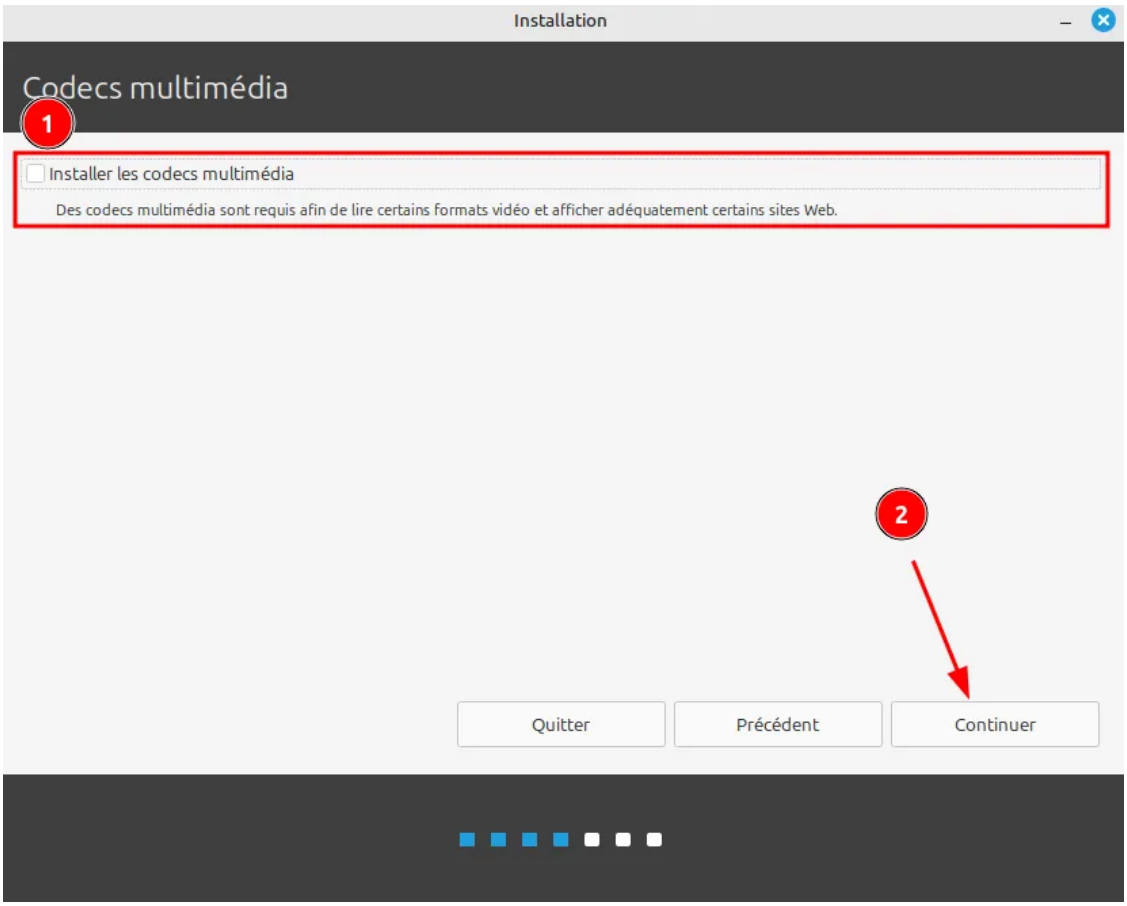
22-11-2024_11-00-57.png

5. Pour la disposition du clavier, sélectionnez dans le menu déroulant **French** *(1)*, puis dans l'autre menu déroulant, sélectionnez **French - French (legacy, alt.)** *(2)*, puis cliquez sur **Continuer**. *(3)*



22-11-2024_11-04-46.png

6. Cocher l'option **Installer les codecs multimédia**, *(1)* puis cliquez sur **Continuer**. *(2)*



22-11-2024_11-06-37.png

7. Sélectionnez **Effacer le disque et installer Linux Mint** *(1)* (cette option supprimera toutes les données préexistantes sur le disque, alors assurez-vous que vous n'avez pas besoin des fichiers actuels avant de continuer), puis cliquez sur Fonctions avancées…*(2)*

8. Cocher ensuite sur les deux options suivantes :

    - **Utiliser LVM pour la nouvelle installation de Linux Mint** *(3) (LVM permet de gérer de manière flexible l'espace disque, facilitant ainsi la gestion des partitions et les redimensionnements futurs).*
    - **Chiffrer la nouvelle installation de Linux Mint pour la sécurité** *(4) (Le chiffrement protège vos données contre tout accès non autorisé en cas de vol ou de perte de l'appareil)*

9. Cliquez sur **OK** *(5)* ****puis cliquez sur **Installer maintenant** *(6)*.

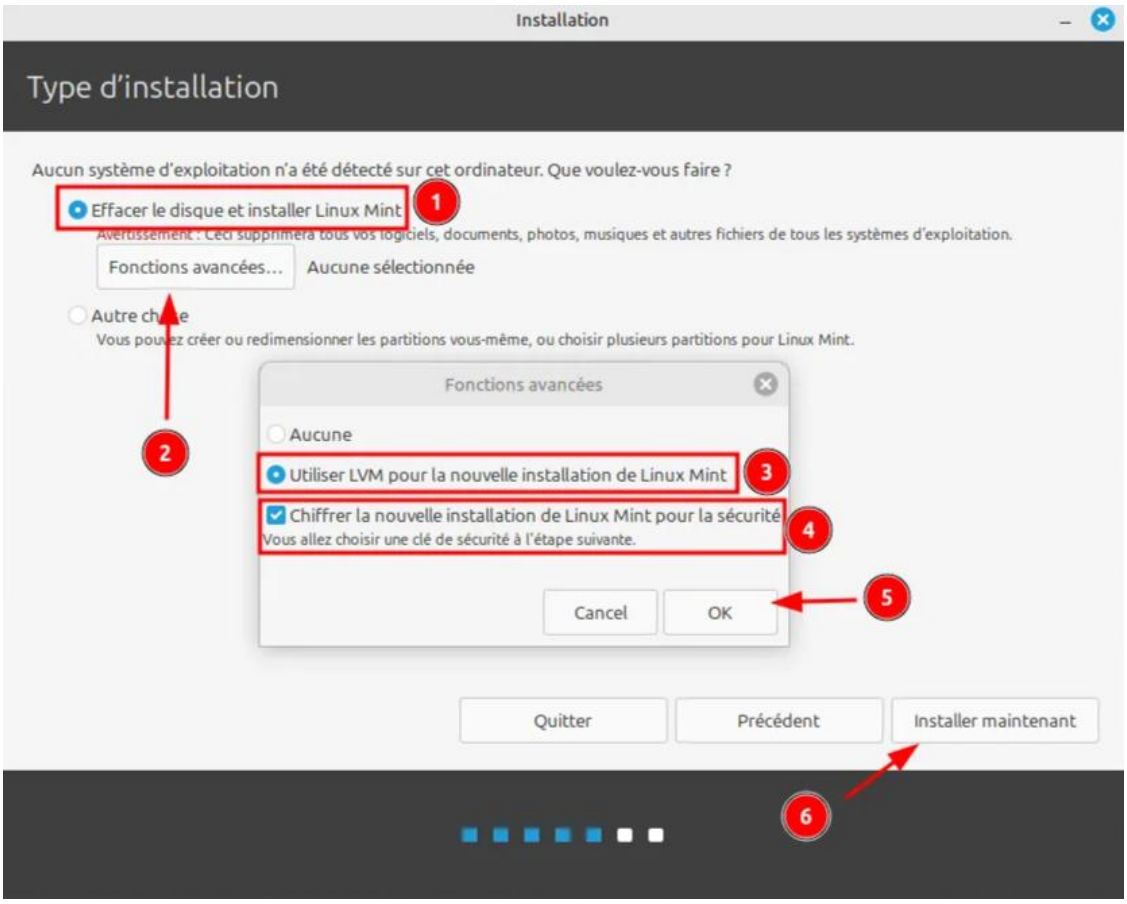


image.png

10. Pour le chiffrement du disque dur, remplissez les champs suivants :

    - **Choisir une clé de sécurité (1).**
    - **Confirmer la clé de sécurité (2).**

    Si vous souhaitez que le système vous génère une clé de récupération dans le cas où vous oublieriez la clé de sécurité, cochez l'option **Activer la clé de récupération.**

    - Cliquez sur **Browse** pour choisir l'emplacement de la **clé de récupération**.

    Pour plus de sécurité, vous pouvez cocher l'option **Écraser l'espace disque vide**. *(3)* Cela permet de remplir tout le disque pour empêcher la récupération de données avec des outils comme Recuva. Cependant, notez que cette opération peut être très longue, car elle effectue un formatage complet du disque. Prévoyez suffisamment de temps avant de sélectionner cette option.

    Cliquez ensuite sur **Installer maintenant**. *(4)*

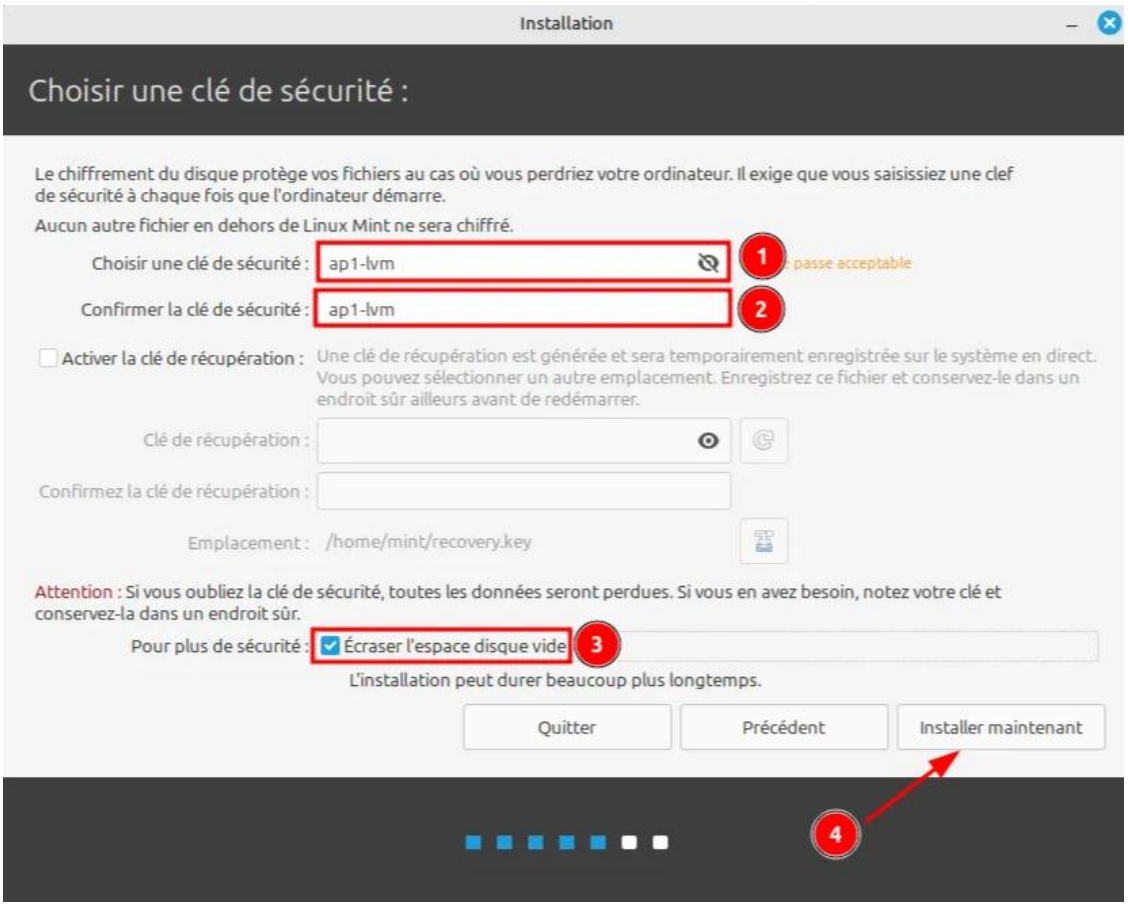


image.png

11. Cliquez ensuite sur **Continuer** *(1)* pour appliquer les changement sur le disque.

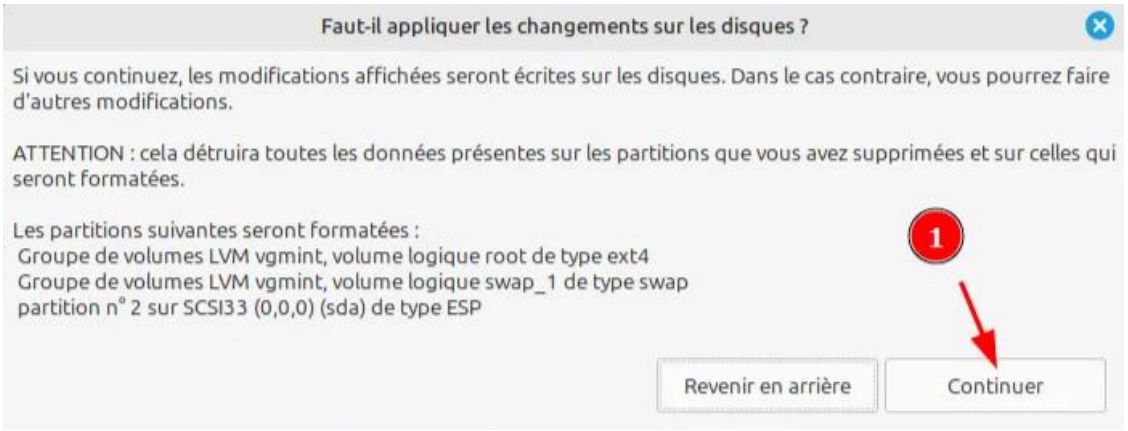
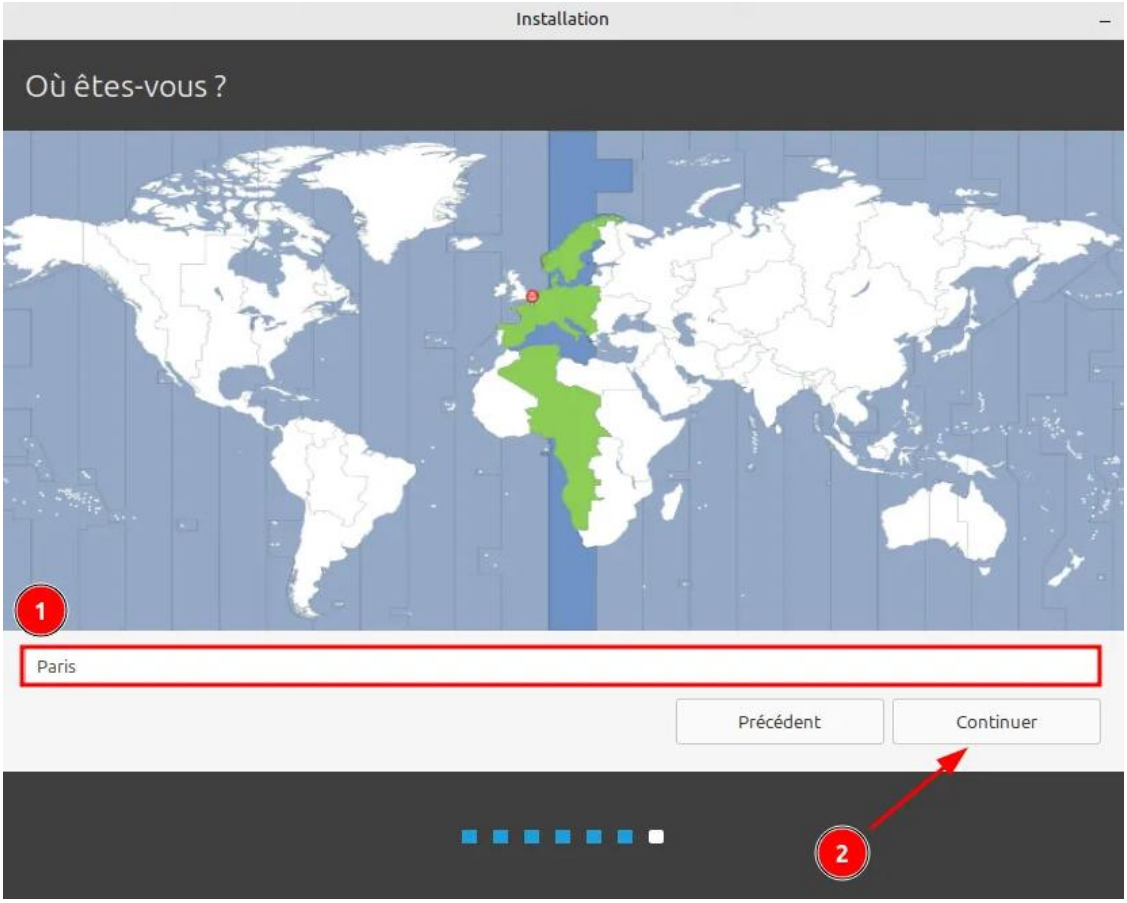


image.png

12. Sélectionnez **Paris** *(1)* dans le menu déroulant pour le fuseau horaire, puis cliquez sur **Continuer**. *(2)*



22-11-2024_11-11-52.png

13. Remplissez les champs suivants :

    - **Votre nom** : Entrez votre nom. *(1)*
    - **Nom de votre ordinateur :** Choisissez un nom significatif. *(2)*
    - **Nom d'utilisateur :** Entrez votre nom d'utilisateur. *(3)*
    - **Mot de passe :** Choisissez un mot de passe sécurisé. *(4)*
    - **Confirmez votre mot de passe :** Entrez le mot de passe une seconde fois. *(5)*
    - Cochez **Demander mon mot de passe pour ouvrir une session**.*(6)*
    - Cochez **Chiffrer mon dossier personnel** si souhaité.*(7)*
    - Puis cliquez sur **Continuer**.*(8)*

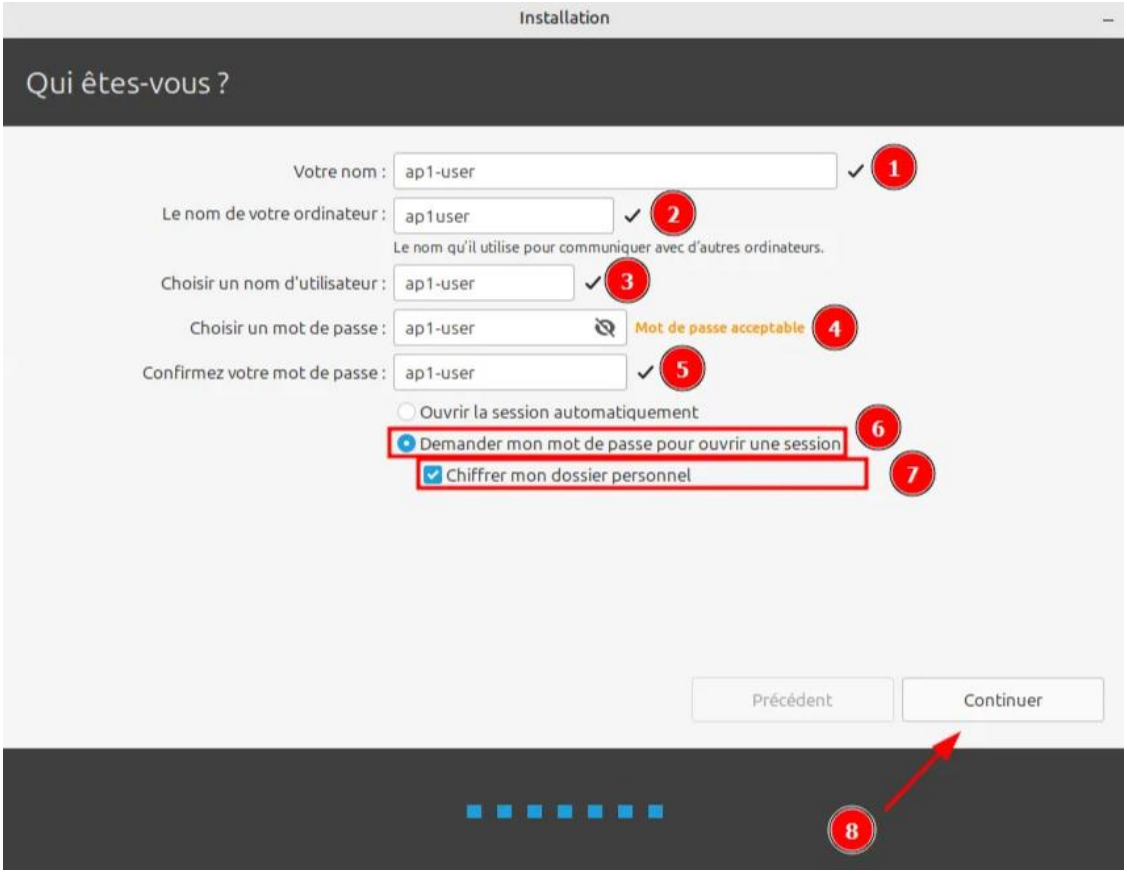
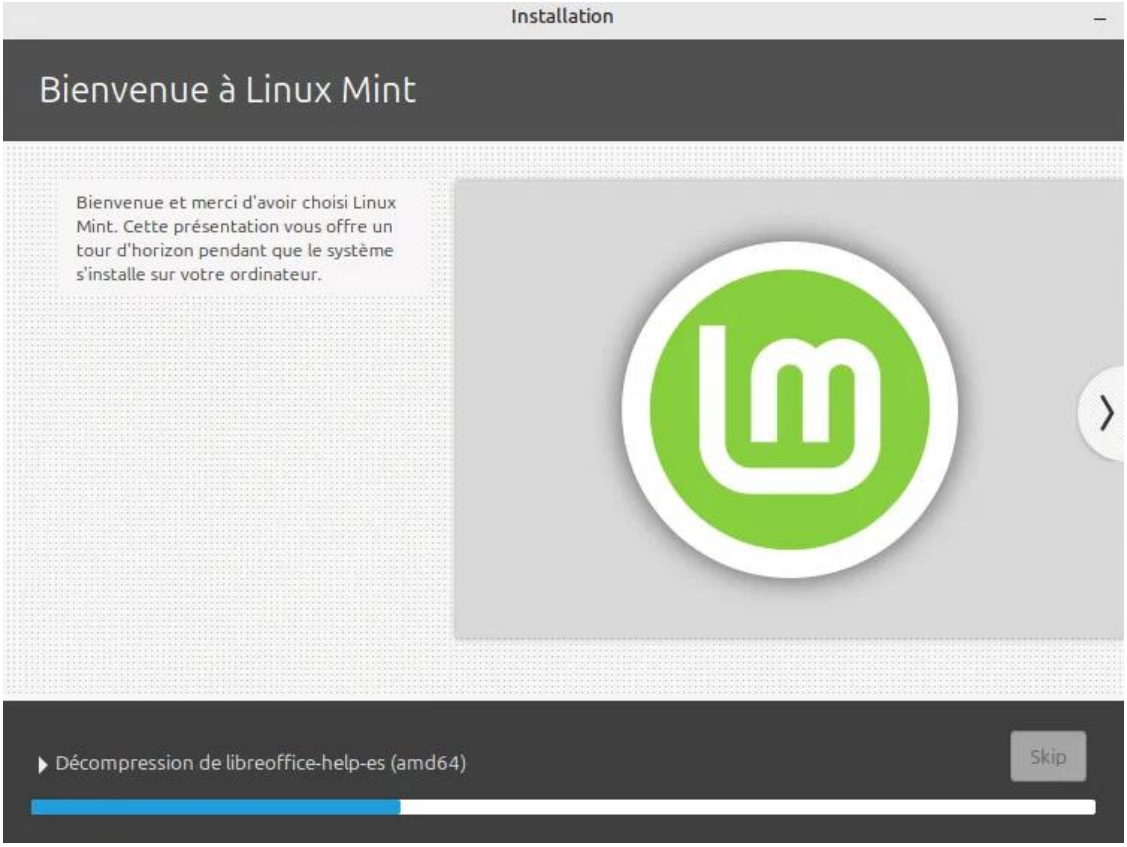


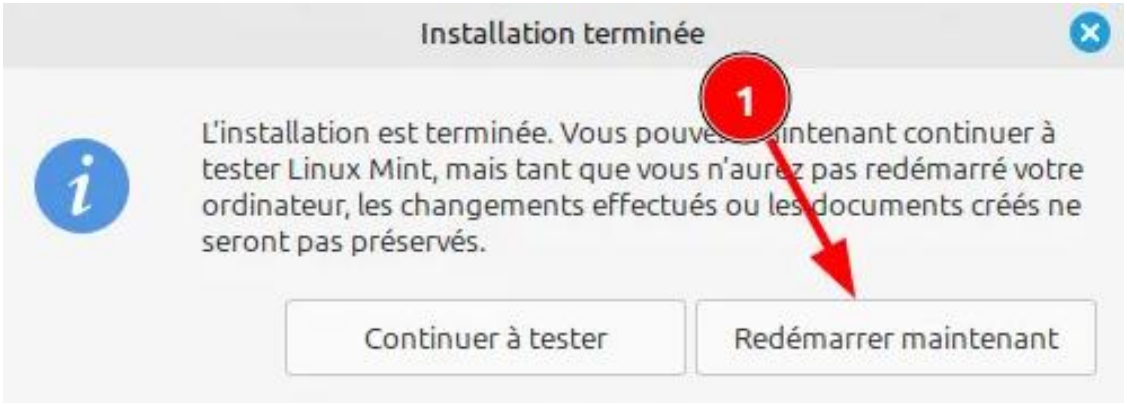
image.png

14. Une fenêtre d'installation s'ouvre avec une barre de progression.



22-11-2024_11-16-48.png

15. Une fois l'installation terminée, cliquez sur **Redémarrer maintenant**. *(1)*

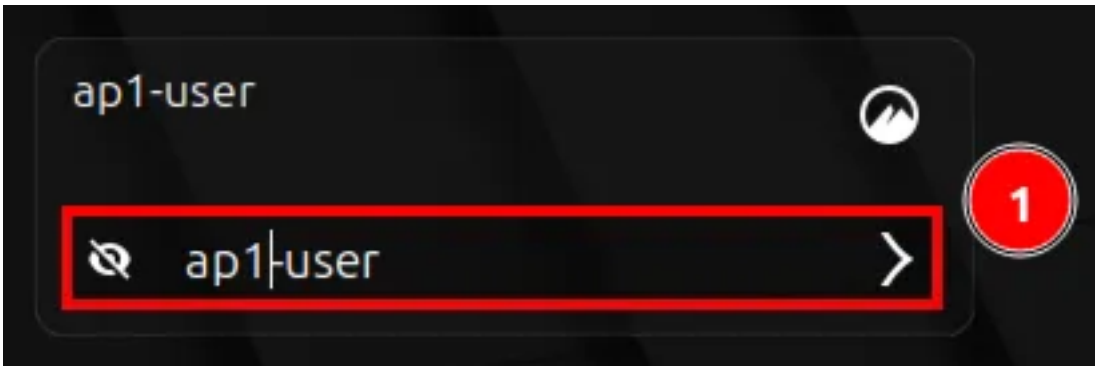


22-11-2024_11-18-41.png

16. Une fois l'ordinateur redémarrer entrer votre clé LVM.

image.png

17. Entrez votre mot de passe pour vous connecter à votre bureau *(1)*



22-11-2024_11-22-15.png

Bienvenue sur **Linux Mint**.

Vous pouvez maintenant passer à la prochaine étape : mettre à jour votre système et configurer vos options de sécurité et de personnalisation pour profiter pleinement de votre nouvel environnement Linux Mint.

1. Mise a jour du système

1. Mise à jour du système

Les mises à jour régulières sont essentielles pour maintenir votre système sécurisé et performant. Elles corrigent des vulnérabilités connues, renforcent la stabilité et garantissent que les dernières fonctionnalités sont disponibles.

Voici les étapes pour effectuer cette opération :

1. **Mettre à jour la liste des paquets disponibles :**

   ```
   sudo apt update -y
   ```

   ```
   ap1-user@ap1-user:~$ sudo apt update
   [sudo] Mot de passe de ap1-user :
   ```

   image.png

2. **Voir la liste des paquets à mettre à jour :**

   ```
   sudo apt list --upgradable
   ```

   ```
   ap1-user@ap1-user:~$ apt list --upgradable
   En train de lister... Fait
   ```

   image.png

3. **Mettre à jour les paquets installés :**

   ```
   sudo apt upgrade -y
   ```

```
ap1-user@ap1-user:~$ sudo apt upgrade
Lecture des listes de paquets... Fait
```

image.png

Pour tout le projet de sécurisation de Linux, nous utiliserons **nano** ou **gedit** pour modifier les fichiers de configuration. Assurez-vous qu'ils sont installés sur votre système :

- Installer nano et gedit :

```
sudo apt install nano -y
sudo apt install gedit -y
```

```
ap1-user@ap1user:~$ sudo apt install nano -y
sudo apt install gedit -y
```

image.png

Ces éditeurs permettent une édition simple et efficace, aussi bien en ligne de commande (nano) qu'en interface graphique (gedit).

---

2. Automatiser les mises à jour de sécurité via unattended-upgrades

Pour assurer que votre système reçoit les correctifs de sécurité sans intervention manuelle, installez et configurez `unattended-upgrades`.

1. **Installer `unattended-upgrades` :**

   ```
   sudo apt install unattended-upgrades -y
   ```

   ```
   ap1-user@ap1-user:~$ sudo apt install unattended-upgrades -y
   Lecture des listes de paquets... Fait
   ```

   image.png

2. **Configurer les mises à jour automatiques :**

   Lancez la commande suivante pour configurer l'outil :

   ```
   sudo dpkg-reconfigure --priority=low unattended-upgrades
   ```

   ```
   ap1-user@ap1-user:~$ sudo dpkg-reconfigure --priority=low unattended-upgrades
   ```

   image.png

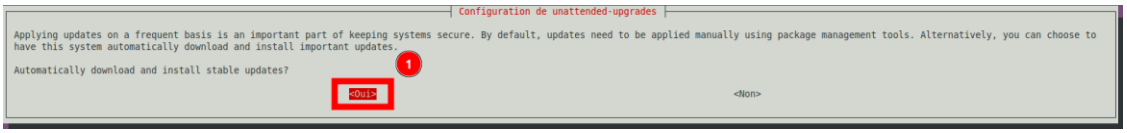


image.png

Cela active les mises à jour de sécurité automatiquement.

3. Donnez les permissions nécessaires avant d'éditer les fichiers de configuration :

```
sudo chmod 700 /etc/apt/apt.conf.d/50unattended-upgrades
sudo chmod 700 /etc/apt/apt.conf.d/20auto-upgrades
```

```
ap1-user@ap1user:~$ sudo chmod 700 /etc/apt/apt.conf.d/50unattended-upgrades
sudo chmod 700 /etc/apt/apt.conf.d/20auto-upgrades
```

image.png

Ces valeurs sont des permissions octales utilisées pour contrôler l'accès aux fichiers. Une erreur courante est de donner des permissions trop larges par inadvertance, par exemple avec "chmod 777" qui permet à n'importe qui de lire, écrire et exécuter le fichier. Cela peut exposer le système à des risques de sécurité. Il est recommandé de toujours restreindre les permissions au minimum nécessaire. Chaque chiffre représente un type de permission accordé au propriétaire du fichier (user). Par exemple : « 700 » signifie que seul le propriétaire peut lire ("4"), écrire ("2") et exécuter ("1") le fichier.

Si vous souhaitez en savoir plus sur comment utilisez la commande chmod rendez vous à l'annexe 1 commande chmod

4. **Création d'un fichier de configuration personnalisé :**

Modifiez le fichier `50unattended-upgrades` en utilisant la commande suivante :

```
sudo gedit /etc/apt/apt.conf.d/50unattended-upgrades
```

```
ap1-user@ap1user:~$ sudo gedit /etc/apt/apt.conf.d/50unattended-upgrades
```

image.png

et coller les paramètres suivants :

```
// Mettre automatiquement à jour les paquets provenant des origines s
pécifiées
Unattended-Upgrade::Allowed-Origins {
    "${distro_id}:${distro_codename}";
    "${distro_id}:${distro_codename}-security"; // Mises à jour de sé
curité critiques
    // Maintenance de Sécurité Étendue (ESM) pour des distributions a
nciennes :
    // Cela ne s'applique que si cette option est installée et dispon
ible.
    "${distro_id}ESMApps:${distro_codename}-apps-security";
    "${distro_id}ESM:${distro_codename}-infra-security";
    //"${distro_id}:${distro_codename}-updates"; // Mises à jour régu
lières (désactivées ici)
```

```
    //"${distro_id}:${distro_codename}-proposed"; // Mises à jour pro
posées (non recommandées)
    //"${distro_id}:${distro_codename}-backports"; // Backports (nouv
elles versions pour anciens systèmes)
};

// Liste des paquets à exclure des mises à jour automatiques
Unattended-Upgrade::Package-Blacklist {
    // Exemple : Exclure les paquets problématiques si nécessaire
    // "linux-"; // Exclure les noyaux pour une gestion manuelle
    // "snapd"; // Exclure Snap si non désiré
};

// Cette option contrôle si les versions de développement d'Ubuntu
Unattended-Upgrade::DevRelease "false";

// Définir les origines spécifiques des mises à jour à installer auto
matiquement
Unattended-Upgrade::Origins-Pattern {
    // Dépôts Linux Mint Wilma
    "o=linuxmint,a=wilma,n=wilma,l=linuxmint,c=main";
    "o=linuxmint,a=wilma,n=wilma,l=linuxmint,c=upstream";
    "o=linuxmint,a=wilma,n=wilma,l=linuxmint,c=import";
    "o=linuxmint,a=wilma,n=wilma,l=linuxmint,c=backport";

    // Dépôts Ubuntu Noble (24.04)
    "o=Ubuntu,a=noble-security,n=noble,l=Ubuntu,c=main";
    "o=Ubuntu,a=noble-security,n=noble,l=Ubuntu,c=universe";
    "o=Ubuntu,a=noble-security,n=noble,l=Ubuntu,c=restricted";
    "o=Ubuntu,a=noble-security,n=noble,l=Ubuntu,c=multiverse";

    "o=Ubuntu,a=noble-updates,n=noble,l=Ubuntu,c=main";
    "o=Ubuntu,a=noble-updates,n=noble,l=Ubuntu,c=universe";
    "o=Ubuntu,a=noble-updates,n=noble,l=Ubuntu,c=restricted";
    "o=Ubuntu,a=noble-updates,n=noble,l=Ubuntu,c=multiverse";
};

// Nettoyage automatique des dépendances inutilisées après une mise à
jour
Unattended-Upgrade::Remove-New-Unused-Dependencies "true";
Unattended-Upgrade::Remove-Unused-Dependencies "true";
Unattended-Upgrade::Remove-Unused-Kernel-Packages "true";

// Retarder les mises à jour pour réduire les temps d'indisponibilité
Unattended-Upgrade::Automatic-Reboot "false"; // Désactive le redémar
rage automatique
Unattended-Upgrade::Automatic-Reboot-Time "05:00"; // Planifie manuel
lement le redémarrage à 5h00

// Paramètres additionnels pour des mises à jour plus sûres
Unattended-Upgrade::MinimalSteps "true"; // Mise à jour par étapes po
ur éviter les erreurs
```

```
Unattended-Upgrade::InstallOnShutdown "true"; // Applique les mises à jour à l'arrêt du système
Unattended-Upgrade::AutoFixInterruptedDpkg "true"; // Répare automatiquement les erreurs de dpkg

// Activer les journaux pour suivre ce qui est mis à jour
Unattended-Upgrade::Verbose "true"; // Journalisation détaillée
Unattended-Upgrade::SyslogEnable "true"; // Active l'enregistrement dans les journaux système
Unattended-Upgrade::SyslogFacility "daemon"; // Définit la catégorie des journaux comme "daemon"

// Configuration des notifications par email en cas de mise à jour
//Unattended-Upgrade::Mail "admin-gsb@example.com"; // Remplacez par une adresse email valide
//Unattended-Upgrade::MailOnlyOnError "true"; // Envoie des emails uniquement en cas d'erreur

// Options avancées
//Unattended-Upgrade::OnlyOnACPower "true"; // Effectue les mises à jour uniquement si la machine est branchée
//Unattended-Upgrade::Skip-Updates-On-Metered-Connections "true"; // Évite les mises à jour sur connexions limitées
//Unattended-Upgrade::Allow-downgrade "false"; // Empêche la rétrogradation des paquets
//Acquire::http::Dl-Limit "70"; // Limite la vitesse de téléchargement des paquets à 70 KB/s
//Unattended-Upgrade::Debug "false"; // Mode débogage désactivé (activez-le en cas de problème)
```

5. **Configurer la fréquence des mises à jour automatiques dans `20auto-upgrades` :**

   Modifiez le fichier `20auto-upgrades` en utilisant la commande suivante :

   ```
   sudo gedit /etc/apt/apt.conf.d/20auto-upgrades
   ```

   ```
   ap1-user@ap1user:~$ sudo gedit /etc/apt/apt.conf.d/20auto-upgrades
   ```

   image.png

   et coller les paramètres suivants :

   ```
   // Commandes liées à APT pour contrôler la fréquence des mises à jour automatiques
   APT::Periodic::Update-Package-Lists "1"; // Met à jour la liste des paquets chaque jour
   APT::Periodic::Unattended-Upgrade "1"; // Exécute les mises à jour automatiques quotidiennement
   APT::Periodic::Download-Upgradeable-Packages "1"; // Télécharge les paquets mis à jour quotidiennement
   APT::Periodic::AutocleanInterval "7"; // Supprime les paquets obsolètes de la cache tous les 7 jours
   ```

6. **Vérifications et redémarrage du service :**

   - Redémarrez puis Vérifiez le statut du service :

     ```
     sudo systemctl restart unattended-upgrades.service
     sudo systemctl status unattended-upgrades.service
     ```

     ```
     ap1-user@ap1user:~$ sudo systemctl restart unattended-upgrades.service
     sudo systemctl status unattended-upgrades.service
     ● unattended-upgrades.service - Unattended Upgrades Shutdown
          Loaded: loaded (/usr/lib/systemd/system/unattended-upgrades.service; enabl>
          Active: active (running) since Sat 2024-12-21 15:36:37 CET; 17ms ago
            Docs: man:unattended-upgrade(8)
        Main PID: 26813 (unattended-upgr)
           Tasks: 1 (limit: 4549)
          Memory: 5.3M (peak: 5.3M)
             CPU: 13ms
          CGroup: /system.slice/unattended-upgrades.service
                  └─26813 /usr/bin/python3 /usr/share/unattended-upgrades/unattended>

     déc. 21 15:36:37 ap1user systemd[1]: Started unattended-upgrades.service - Unat>
     lines 1-12/12 (END)
     ```

     image.png

7. **Configurer les timers apt pour les mises à jour quotidiennes :**

   Redémarrez et activez les timers suivants pour synchroniser automatiquement les paquets :

   - **Timer apt-daily :**

     ```
     sudo systemctl restart apt-daily.timer
     sudo systemctl status apt-daily.timer
     ```

     ```
     ap1-user@ap1user:~$ sudo systemctl restart apt-daily.timer
     sudo systemctl status apt-daily.timer
     ● apt-daily.timer - Daily apt download activities
          Loaded: loaded (/usr/lib/systemd/system/apt-daily.timer; enabled; preset: >
          Active: active (waiting) since Sat 2024-12-21 15:37:36 CET; 13ms ago
         Trigger: Sun 2024-12-22 00:13:03 CET; 8h left
        Triggers: ● apt-daily.service

     déc. 21 15:37:36 ap1user systemd[1]: apt-daily.timer: Deactivated successfully.
     déc. 21 15:37:36 ap1user systemd[1]: Stopped apt-daily.timer - Daily apt downlo>
     déc. 21 15:37:36 ap1user systemd[1]: Stopping apt-daily.timer - Daily apt downl>
     déc. 21 15:37:36 ap1user systemd[1]: Started apt-daily.timer - Daily apt downlo>
     ```

     image.png

   - **Timer apt-daily-upgrade :**

     ```
     sudo systemctl restart apt-daily-upgrade.timer
     sudo systemctl status apt-daily-upgrade.timer
     ```

```
ap1-user@ap1user:~$ sudo systemctl restart apt-daily-upgrade.timer
sudo systemctl status apt-daily-upgrade.timer
● apt-daily-upgrade.timer - Daily apt upgrade and clean activities
     Loaded: loaded (/usr/lib/systemd/system/apt-daily-upgrade.timer; enabled; >
     Active: active (waiting) since Sat 2024-12-21 15:37:55 CET; 13ms ago
    Trigger: Sun 2024-12-22 06:14:33 CET; 14h left
   Triggers: ● apt-daily-upgrade.service

déc. 21 15:37:55 ap1user systemd[1]: Stopping apt-daily-upgrade.timer - Daily a>
déc. 21 15:37:55 ap1user systemd[1]: Started apt-daily-upgrade.timer - Daily ap>
lines 1-8/8 (END)
```

image.png

8. **Exécution à blanc pour tester les mises à jour :**

```
sudo unattended-upgrades --dry-run
```

```
ap1-user@ap1user:~$ sudo unattended-upgrades --dry-run
Enabled logging to syslog via daemon facility
Démarrage du script de mise à niveau automatique
Les origines autorisées sont : o=Linuxmint,a=wilma, o=Linuxmint,a=wilma-security
, o=LinuxmintESMApps,a=wilma-apps-security, o=LinuxmintESM,a=wilma-infra-securit
y, o=linuxmint,a=wilma,n=wilma,l=linuxmint,c=main, o=linuxmint,a=wilma,n=wilma,l
=linuxmint,c=upstream, o=linuxmint,a=wilma,n=wilma,l=linuxmint,c=import, o=linux
mint,a=wilma,n=wilma,l=linuxmint,c=backport, o=Ubuntu,a=noble-security,n=noble,l
=Ubuntu,c=main, o=Ubuntu,a=noble-security,n=noble,l=Ubuntu,c=universe, o=Ubuntu,
a=noble-security,n=noble,l=Ubuntu,c=restricted, o=Ubuntu,a=noble-security,n=nobl
e,l=Ubuntu,c=multiverse, o=Ubuntu,a=noble-updates,n=noble,l=Ubuntu,c=main, o=Ubu
ntu,a=noble-updates,n=noble,l=Ubuntu,c=universe, o=Ubuntu,a=noble-updates,n=nobl
e,l=Ubuntu,c=restricted, o=Ubuntu,a=noble-updates,n=noble,l=Ubuntu,c=multiverse
Liste noire initiale :
Liste blanche initiale (not strict) :
Aucun paquet à mettre à niveau automatiquement ni à supprimer automatiquement
La liste des paquets conservés ne peut pas être déterminée en mode simulé.
```

image.png

Cette commande permet de simuler les mises à jour sans appliquer de changements.

9. **Vérification des timers planifiés :**

```
sudo systemctl list-timers
```

```
ap1-user@ap1user:~$ sudo systemctl list-timers
NEXT                         LEFT LAST                         PASSED UNIT                         ACTIVATES
Sat 2024-12-21 16:30:46 CET         51min Sat 2024-12-21 15:32:00 CET     7min ago anacron.timer                anacron.service
Sat 2024-12-21 16:50:55 CET       1h 11min Sat 2024-12-21 15:11:00 CET           - fwupd-refresh.timer          fwupd-refresh.service
Sun 2024-12-22 00:00:00 CET            8h -                               - dpkg-db-backup.timer         dpkg-db-backup.service
Sun 2024-12-22 00:00:00 CET            8h -                               - logrotate.timer              logrotate.service
Sun 2024-12-22 00:13:03 CET            8h Sat 2024-12-21 14:15:06 CET     - apt-daily.timer              apt-daily.service
Sun 2024-12-22 01:13:23 CET            9h -                               - mdmonitor-oneshot.timer      mdmonitor-oneshot.service
Sun 2024-12-22 03:07:10 CET           11h -                               - plocate-updatedb.timer       plocate-updatedb.service
Sun 2024-12-22 03:10:10 CET           11h -                               - e2scrub_all.timer            e2scrub_all.service
Sun 2024-12-22 06:08:38 CET           14h Sat 2024-12-21 15:26:33 CET    12min ago motd-news.timer               motd-news.service
Sun 2024-12-22 06:14:33 CET           14h Sat 2024-12-21 14:15:06 CET           - apt-daily-upgrade.timer      apt-daily-upgrade.service
Sun 2024-12-22 10:41:36 CET           19h -                               - mdcheck_continue.timer       mdcheck_continue.service
Sun 2024-12-22 11:27:22 CET           19h -                               - man-db.timer                 man-db.service
Sun 2024-12-22 14:28:43 CET           22h Sat 2024-12-21 14:28:43 CET 1h 10min ago systemd-tmpfiles-clean.timer systemd-tmpfiles-clean.service
Mon 2024-12-23 00:25:06 CET     1 day 8h Sat 2024-12-21 14:15:06 CET           - fstrim.timer                 fstrim.service
Sun 2025-01-05 05:09:08 CET 2 weeks 0 days -                               - mdcheck_start.timer          mdcheck_start.service
```

image.png

Chercher la ligne apt-daily.timer

10. **Log et dépannage :**

1. Consultez les logs pour vérifier les mises à jour réalisées :

```
cat /var/log/unattended-upgrades/unattended-upgrades.log
```

2. Si apt-daily.timer n'apparait pas dans la liste des services activé fait la commande :

```
sudo systemctl list-timers --all
```

Cette commande permet d'afficher les services non activés aussi.

---

3. Automatiser les mises à jour de sécurité via l'interface graphique

Si vous préférez une solution visuelle, Linux Mint offre une interface intuitive pour configurer les mises à jour automatiques.

1. Cliquez sur le logo **Linux Mint** *(1)* en bas à gauche puis accédez à **Administration** *(2)* > **Gestionnaire de mise à jour**. *(3)*

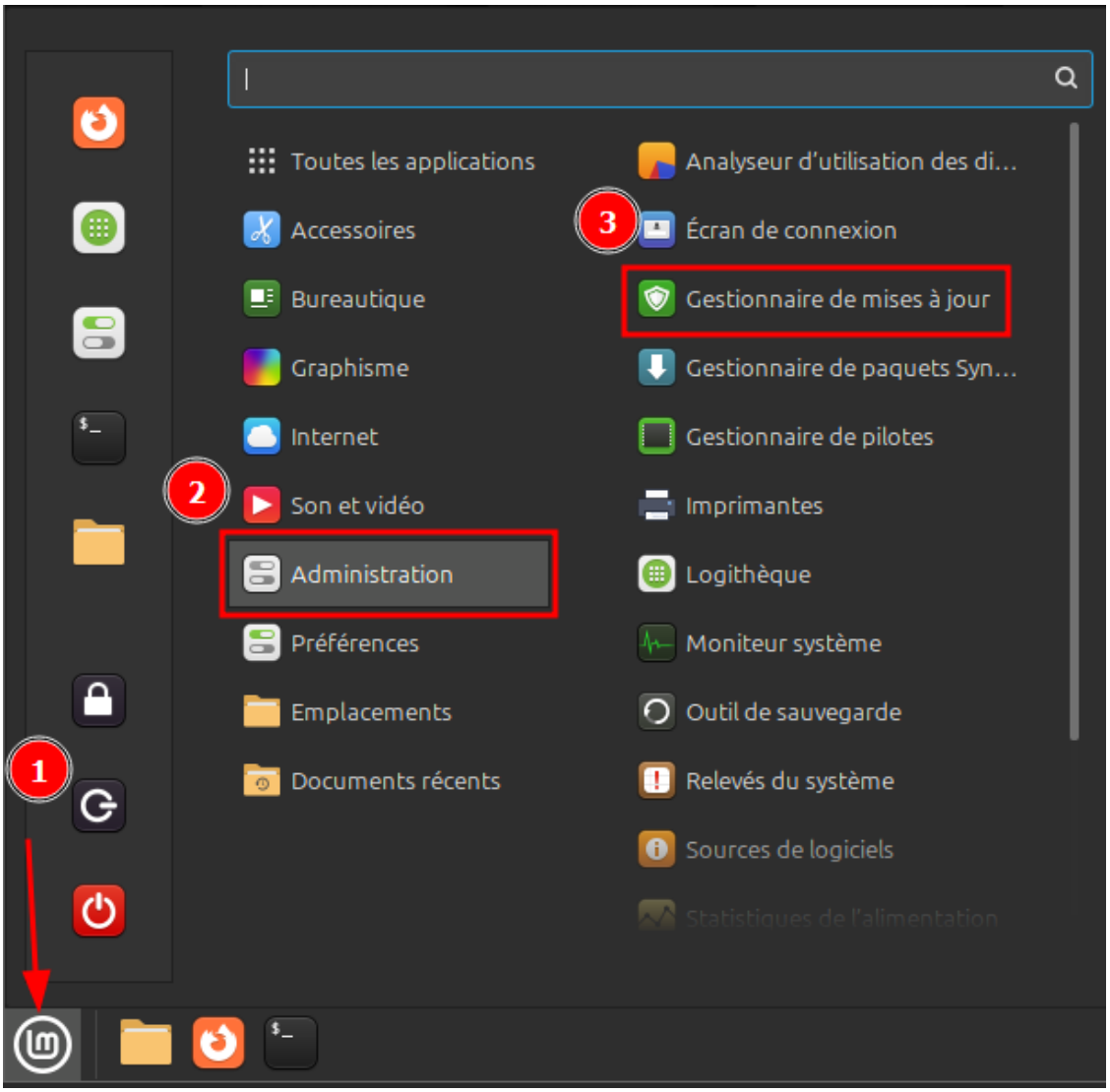


image.png

2. Cliquez sur **Valider** *(1)* **puis** sur **Édition.** *(2)*

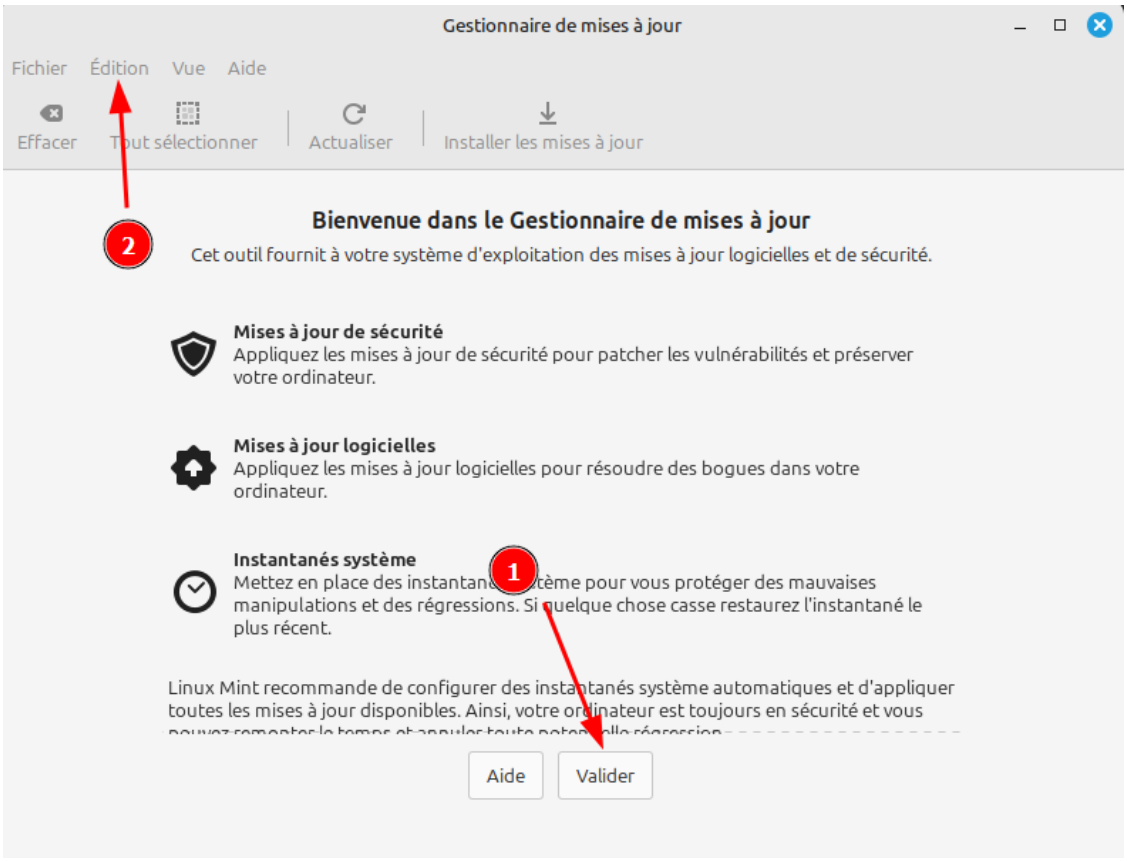


image.png

3. Cliquez sur **Préférences**. *(1)*

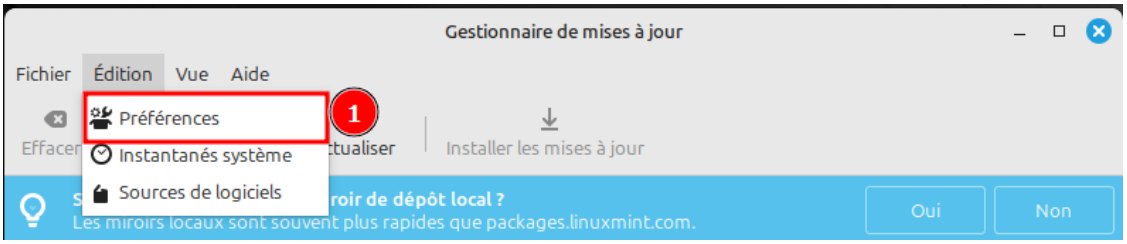


image.png

4. Allez dans la rubrique **Automatisation**. *(1)*

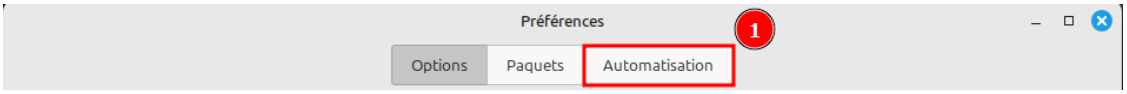


image.png

5. Cochez les 4 options suivantes puis entrez votre mot de passe :

   - **Appliquer les mises à jour automatiquement** *(1)* : Télécharge et installe les mises à jour sans intervention.
   - **Mettre à jour les composants Cinnamon automatiquement** *(2)* : Assure la stabilité et la sécurité de l'environnement graphique.

- **Mettre à jour les Flatpaks automatiquement** *(3)* : Garde les applications Flatpak à jour.
- **Retirer les noyaux obsolètes et leurs dépendances** *(4)* : Libère de l'espace disque en supprimant les anciens noyaux inutiles tout en conservant un noyau de secours.

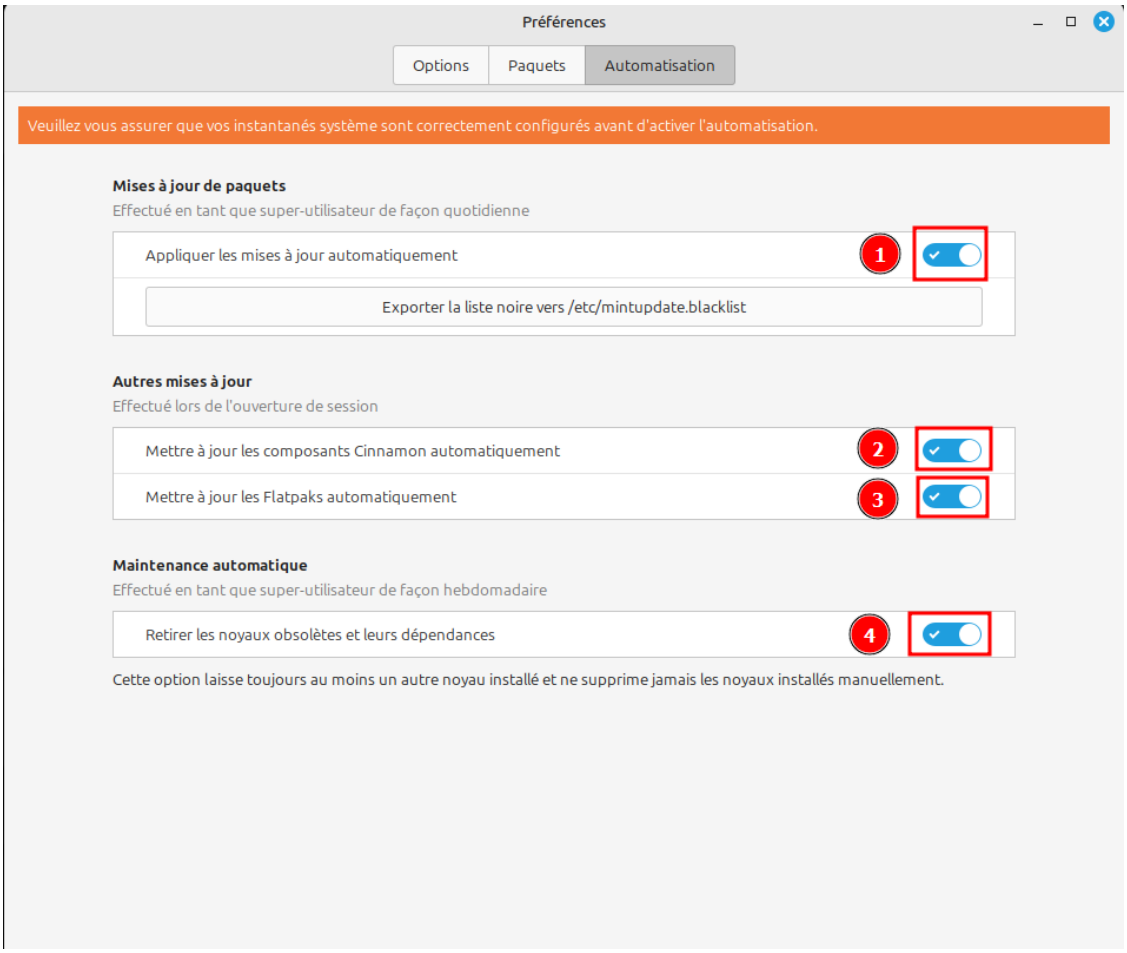


image.png

Points importants :

- Si vous configurez `unattended-upgrades`, il n'est pas nécessaire d'activer les options graphiques.

---

5. Pourquoi ces étapes sont importantes ?

- **Mises à jour régulières** : Elles corrigent des vulnérabilités de sécurité et améliorent la stabilité du système.
- **Automatisation** : Réduit les risques d'erreur humaine et garantit que les mises à jour critiques sont appliquées à temps.

- **Logs et dépannage** : Permettent de tracer les actions effectuées et d'identifier les problèmes rapidement.

---

2. Desactivation des Services Non Necessaires

0. Introduction

La désactivation des services inutiles est une étape essentielle pour améliorer la sécurité et les performances d'un système Linux. Chaque service actif représente une surface d'attaque potentielle. Par exemple, un service réseau inutilisé mais actif pourrait permettre à un attaquant de scanner le système pour trouver des failles exploitables, augmentant ainsi le risque d'intrusion. En limitant le nombre de services en cours d'exécution, on réduit les opportunités d'exploitation par des attaquants tout en économisant des ressources système.

---

1. Services Bluetooth

bluetooth.service / blueman-mechanism.service

- **Raison** : Si aucun périphérique Bluetooth n'est utilisé dans le cadre du projet, ces services peuvent être désactivés.
- **Commandes** :

```
sudo systemctl stop bluetooth.service
sudo systemctl stop blueman-mechanism.service
sudo systemctl disable bluetooth.service
sudo systemctl disable blueman-mechanism.service
sudo systemctl status bluetooth.service
sudo systemctl status blueman-mechanism.service
```

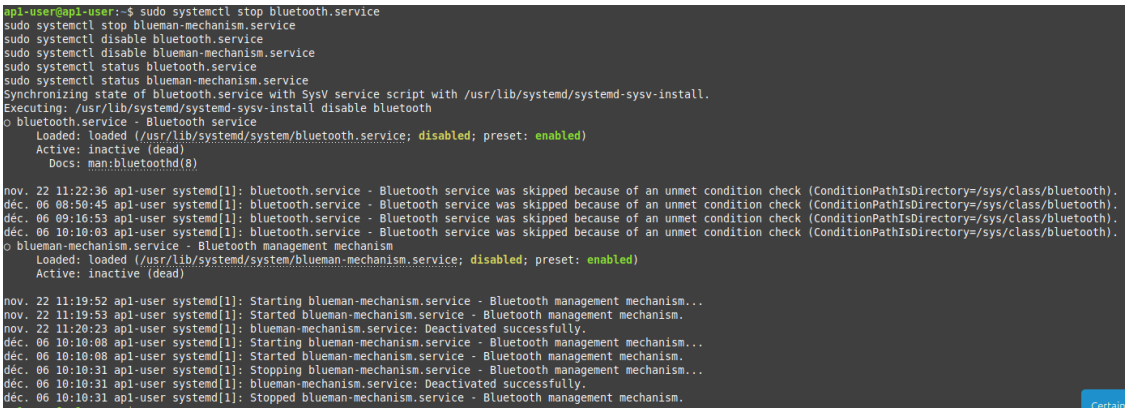


image.png

Ces commandes arrêtent immédiatement les services et empêchent leur démarrage automatique à l'avenir. Si ces services restent actifs inutilement, ils peuvent consommer des ressources système, exposer des vulnérabilités inutiles et augmenter la surface d'attaque du système.

---

2. Service ModemManager

ModemManager.service

- **Raison** : Si le projet ne nécessite pas l'utilisation d'un modem pour la connexion Internet, ce service peut être désactivé.
- **Commandes** :

```
sudo systemctl stop ModemManager.service
sudo systemctl disable ModemManager.service
sudo systemctl status ModemManager.service
```

```
ap1-user@ap1-user:~$ sudo systemctl stop ModemManager.service
ap1-user@ap1-user:~$ sudo systemctl status ModemManager.service
○ ModemManager.service - Modem Manager
     Loaded: loaded (/usr/lib/systemd/system/ModemManager.service; enabled; pre>
     Active: inactive (dead) since Fri 2024-12-06 10:05:18 CET; 7s ago
   Duration: 1w 6d 22h 45min 25.816s
    Process: 982 ExecStart=/usr/sbin/ModemManager (code=exited, status=0/SUCCES>
   Main PID: 982 (code=exited, status=0/SUCCESS)
        CPU: 91ms

nov. 22 11:19:52 ap1-user systemd[1]: Starting ModemManager.service - Modem Man>
nov. 22 11:19:52 ap1-user ModemManager[982]: <msg> ModemManager (version 1.23.4>
nov. 22 11:19:53 ap1-user systemd[1]: Started ModemManager.service - Modem Mana>
nov. 22 11:19:57 ap1-user ModemManager[982]: <msg> [base-manager] couldn't chec>
déc. 06 10:05:18 ap1-user systemd[1]: Stopping ModemManager.service - Modem Man>
déc. 06 10:05:18 ap1-user ModemManager[982]: <msg> caught signal, shutting down>
déc. 06 10:05:18 ap1-user ModemManager[982]: <msg> ModemManager is shut down
déc. 06 10:05:18 ap1-user systemd[1]: ModemManager.service: Deactivated success>
déc. 06 10:05:18 ap1-user systemd[1]: Stopped ModemManager.service - Modem Mana>

ap1-user@ap1-user:~$ sudo systemctl disable ModemManager.service
Removed "/etc/systemd/system/multi-user.target.wants/ModemManager.service".
Removed "/etc/systemd/system/dbus-org.freedesktop.ModemManager1.service".
```

image.png

Ces actions permettent d'éliminer tout accès potentiel à ce service non nécessaire. ModemManager est souvent activé par défaut car il gère les connexions des modems mobiles, ce qui peut être utile pour les utilisateurs qui se connectent à Internet via des clés USB 3G/4G ou des modems embarqués. Toutefois, si ces équipements ne sont pas utilisés, il est préférable de le désactiver pour réduire les risques de sécurité.

---

3. Autres Services Inutiles à Désactiver (facultatif)

cups.service (Service d'impression)

- **Raison** : Désactiver si l'impression locale n'est pas requise.
- **Commandes** :

```
sudo systemctl stop cups.service
sudo systemctl disable cups.service
sudo systemctl status cups.service
```

- **Impact** : Après désactivation, les imprimantes locales ne fonctionneront plus, mais les impressions via un réseau sécurisé peuvent être envisagées.

avahi-daemon.service (Découverte réseau)

- **Raison** : Désactiver pour éviter l'exposition à des requêtes de découverte réseau non nécessaires.
- **Commandes** :

```
sudo systemctl stop avahi-daemon.service
sudo systemctl disable avahi-daemon.service
sudo systemctl status avahi-daemon.service
```

- **Impact** : Les fonctionnalités de découverte automatique des appareils réseau seront désactivées.

rpcbind.service (Services liés à NFS)

- **Raison** : Désactiver si NFS (Network File System) n'est pas utilisé.
- **Commandes** :

```
sudo systemctl stop rpcbind.service
sudo systemctl disable rpcbind.service
sudo systemctl status rpcbind.service
```

- **Impact** : Les partages réseau basés sur NFS ne seront plus accessibles.

4.Options Avancées (facultatif)

Pour des environnements nécessitant un contrôle strict des services, désactiver les services suivants selon les besoins :

- **snapd.service** (Gestion des packages Snap) : Désactiver si Snap n'est pas utilisé.
- **NetworkManager-wait-online.service** : Désactiver si un démarrage rapide est prioritaire et que les connexions réseau ne sont pas critiques au démarrage.

Commandes Générales pour ces services :

```
sudo systemctl stop [nom_du_service]
sudo systemctl disable [nom_du_service]
sudo systemctl status [nom_du_service]
```

---

5. Vérification de la Désactivation

Pour confirmer que les services sont bien désactivés, exécutez la commande suivante : examinez si le statut indique « inactive (dead) » ou un état similaire, confirmant que le service est arrêté.

```
sudo systemctl status [nom_du_service]
```

- Exemple :

```
sudo systemctl status bluetooth.service
sudo systemctl status ModemManager.service
```

6. Tableau Récapitulatif des Services

Service	Utilité	Statut Recommandé	Impact de la Désactivation
bluetooth.service	Bluetooth	Désactivé	Aucun appareil Bluetooth ne pourra être utilisé.
blueman-mechanism.service	Bluetooth Manager	Désactivé	Gestion des périphériques Bluetooth non disponible.
ModemManager.service	Modem mobile	Désactivé	Aucune connexion via modem mobile ne sera possible.
cups.service	Impression locale	Activé si nécessaire	Les imprimantes locales ne fonctionneront plus.
avahi-daemon.service	Découverte réseau	Désactivé	Découverte automatique des appareils réseau désactivée.
rpcbind.service	NFS (Network File System)	Désactivé	Partages réseau NFS non accessibles.
snapd.service	Gestion des packages Snap	Désactivé si inutile	Impossible d'installer ou de gérer des applications Snap.
NetworkManager-wait-online.service	Attente de connexion réseau	Désactivé si rapide	Réduction du temps de démarrage, mais connexion non garantie.

7. Pourquoi ces étapes sont importantes ?

- **Réduction des risques** : Désactiver les services inutiles limite les vulnérabilités exploitables par des attaquants.
- **Optimisation des performances** : Libère des ressources système en arrêtant les services non nécessaires.
- **Conformité au besoin** : Assure une configuration adaptée aux objectifs spécifiques du projet.

3. Activation de l'Audit Système

0. Introduction

L'activation de l'audit système est une étape essentielle pour surveiller et consigner les activités sur un système Linux. Elle permet d'identifier des comportements anormaux, de répondre aux exigences de conformité et de renforcer la sécurité globale. Ce guide présente une méthode structurée pour installer, configurer et exploiter l'outil d'audit `auditd` sur un environnement Linux.

---

1. Installation de `auditd`

Objectif :

`auditd` est le démon responsable de la surveillance et de l'enregistrement des événements d'audit.

Étapes :

1. Installez `auditd` et ses plugins associés :

   ```
   sudo apt install auditd audispd-plugins -y
   ```

   ```
   ap1-linux@ap1linux:/etc$ sudo apt install auditd audispd-plugins -y
   ```

   image.png

   Vérifiez que tous les paquets installés sont nécessaires pour éviter des dépendances inutiles.

2. Vérifiez l'installation :

   ```
   sudo auditctl -v
   ```

```
ap1-linux@ap1linux:/etc$ sudo auditctl -v
auditctl version 3.1.2
```

image.png

Une version devrait s'afficher pour confirmer le succès de l'installation.

---

2. Vérification et Activation du Service

Vérifiez le statut du service `auditd` démarrez-le et activez-le au démarrage:

```
sudo systemctl status auditd
sudo systemctl start auditd
sudo systemctl enable auditd
```

```
ap1-user@ap1user:~$ sudo systemctl status auditd
sudo systemctl start auditd
sudo systemctl enable auditd
● auditd.service - Security Auditing Service
     Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-01-19 00:08:18 CET; 1min 59s ago
       Docs: man:auditd(8)
             https://github.com/linux-audit/audit-documentation
   Main PID: 28846 (auditd)
      Tasks: 2 (limit: 4549)
     Memory: 536.0K (peak: 2.3M)
        CPU: 32ms
     CGroup: /system.slice/auditd.service
             └─28846 /sbin/auditd

janv. 19 00:08:18 ap1user augenrules[28861]: enabled 1
janv. 19 00:08:18 ap1user augenrules[28861]: failure 1
janv. 19 00:08:18 ap1user augenrules[28861]: pid 28846
janv. 19 00:08:18 ap1user augenrules[28861]: rate_limit 0
janv. 19 00:08:18 ap1user augenrules[28861]: backlog_limit 8192
janv. 19 00:08:18 ap1user augenrules[28861]: lost 0
janv. 19 00:08:18 ap1user augenrules[28861]: backlog 3
janv. 19 00:08:18 ap1user augenrules[28861]: backlog_wait_time 60000
janv. 19 00:08:18 ap1user augenrules[28861]: backlog_wait_time_actual 0
janv. 19 00:08:18 ap1user systemd[1]: Started auditd.service - Security Auditing Service.
Synchronizing state of auditd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable auditd
```

image.png

---

3. Configuration des Règles d'Audit

Objectif :

Les règles d'audit permettent de spécifier les fichiers, dossiers ou événements à surveiller.

Méthode :

1. Entrez la commande suivante dans un terminal :

```
cat <<EOL | sudo tee /etc/audit/rules.d/audit.rules
## Supprimer toutes les règles existantes
-D

## Taille des tampons
-b 8192
# Ajustez cette valeur en fonction des besoins spécifiques.

## Définitions des règles
-w /etc/passwd -p wa -k passwd_changes
-w /etc/shadow -p wa -k shadow_access
-a always,exit -F arch=b64 -S setuid -S setgid -k privilege_changes
-w /var/log/auth.log -p wa -k auth_changes
-w /boot/ -p wa -k boot_changes
EOL
```

L'utilisation de scripts permet d'automatiser la configuration des règles et de réduire les erreurs manuelles.

2. Appliquez les nouvelles règles :

```
sudo systemctl restart auditd
sudo systemctl status auditd
```

```
ap1-linux@ap1linux:~$ sudo systemctl restart auditd
sudo systemctl status auditd
● auditd.service - Security Auditing Service
     Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset: e>
     Active: active (running) since Sun 2024-12-08 16:17:45 CET; 15ms ago
       Docs: man:auditd(8)
             https://github.com/linux-audit/audit-documentation
    Process: 3864 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
    Process: 3869 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/>
   Main PID: 3866 (auditd)
      Tasks: 2 (limit: 4549)
     Memory: 532.0K (peak: 2.2M)
        CPU: 28ms
     CGroup: /system.slice/auditd.service
             └─3866 /sbin/auditd

déc. 08 16:17:45 ap1linux augenrules[3883]: enabled 1
déc. 08 16:17:45 ap1linux augenrules[3883]: failure 1
déc. 08 16:17:45 ap1linux augenrules[3883]: pid 3866
déc. 08 16:17:45 ap1linux augenrules[3883]: rate_limit 0
déc. 08 16:17:45 ap1linux augenrules[3883]: backlog_limit 8192
déc. 08 16:17:45 ap1linux augenrules[3883]: lost 0
déc. 08 16:17:45 ap1linux augenrules[3883]: backlog 3
déc. 08 16:17:45 ap1linux augenrules[3883]: backlog_wait_time 60000
déc. 08 16:17:45 ap1linux augenrules[3883]: backlog_wait_time_actual 0
lines 1-23...skipping...
```

image.png

4. Test des Règles

Vérifiez que les règles fonctionnent correctement :

1. Simulez une modification sur `/etc/passwd` :

   ```
   sudo nano /etc/passwd
   ```

2. Recherchez les événements dans les journaux :

   ```
   sudo ausearch -k passwd_changes
   ```

3. Affichez un rapport détaillé des événements :

   ```
   sudo aureport -k
   ```

```
ap1-user@ap1user:~$ sudo nano /etc/passwd
ap1-user@ap1user:~$ sudo ausearch -k passwd_changes
----
time->Sun Jan 19 00:13:03 2025
type=PROCTITLE msg=audit(1737241983.260:514): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F617
56469742E72756C6573
type=SYSCALL msg=audit(1737241983.260:514): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7ffd75583010 a2=43
c a3=0 items=0 ppid=29628 pid=29641 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none
) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1737241983.260:514): auid=4294967295 ses=4294967295 subj=unconfined op=add_rule key="pas
swd_changes" list=4 res=1
----
time->Sun Jan 19 00:14:08 2025
type=PROCTITLE msg=audit(1737242048.448:535): proctitle=6E616E6F002F6574632F706173737764
type=PATH msg=audit(1737242048.448:535): item=1 name="/etc/passwd" inode=342307 dev=fc:01 mode=0100644 ouid=0 ogid=0
rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1737242048.448:535): item=0 name="/etc/" inode=261121 dev=fc:01 mode=040755 ouid=0 ogid=0 rdev=00
:00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1737242048.448:535): cwd="/home/ap1-user"
type=SYSCALL msg=audit(1737242048.448:535): arch=c000003e syscall=257 success=yes exit=3 a0=ffffff9c a1=5709ffe10b60
a2=241 a3=1b6 items=2 ppid=29659 pid=29660 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1
 ses=2 comm="nano" exe="/usr/bin/nano" subj=unconfined key="passwd_changes"
ap1-user@ap1user:~$ sudo aureport -k

Key Report
===============================================
# date time key success exe auid event
===============================================
1. 19/01/2025 00:13:03 passwd_changes yes /usr/sbin/auditctl -1 514
2. 19/01/2025 00:13:03 shadow_access yes /usr/sbin/auditctl -1 515
3. 19/01/2025 00:13:03 privilege_changes yes /usr/sbin/auditctl -1 516
4. 19/01/2025 00:13:03 auth_changes yes /usr/sbin/auditctl -1 517
5. 19/01/2025 00:13:03 boot_changes yes /usr/sbin/auditctl -1 518
6. 19/01/2025 00:13:03 privilege_changes yes /usr/bin/sudo 1000 524
7. 19/01/2025 00:13:55 privilege_changes yes /usr/bin/sudo 1000 532
8. 19/01/2025 00:14:08 passwd_changes yes /usr/bin/nano 1000 535
9. 19/01/2025 00:14:13 privilege_changes yes /usr/bin/sudo 1000 540
10. 19/01/2025 00:14:24 privilege_changes yes /usr/bin/sudo 1000 548
```

image.png

Vérifiez régulièrement que les mots-clés définis (ex. passwd_changes) sont toujours pertinents.

---

5. Configuration pour un Démarrage Automatique

Étapes :

1. Modifiez le fichier GRUB pour forcer l'activation de l'audit au démarrage :

   ```
   sudo gedot /etc/default/grub
   ```

2. Ajoutez ou modifiez la ligne suivante :

   ```
   GRUB_CMDLINE_LINUX="audit=1"
   ```

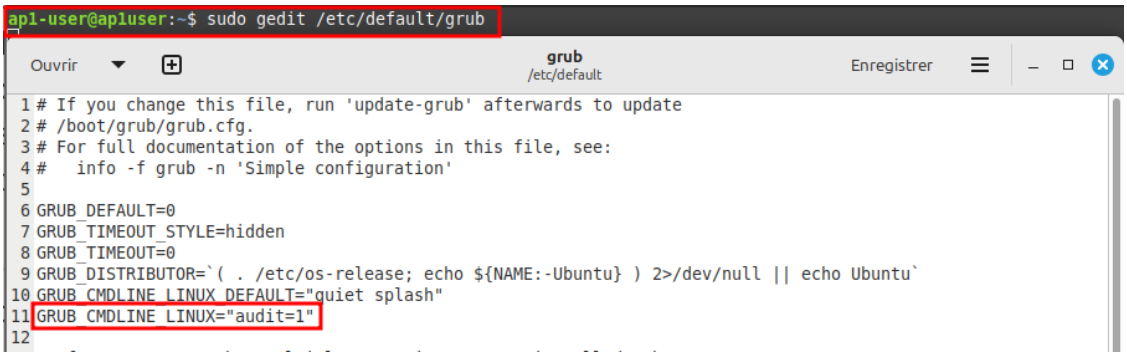


image.png

3. Mettez à jour GRUB et redémarrez :

   ```
   sudo update-grub
   sudo reboot
   ```

```
ap1-user@ap1user:~$ sudo nano /etc/default/grub
ap1-user@ap1user:~$ sudo update-grub
sudo reboot
Sourcing file `/etc/default/grub'
Sourcing file `/etc/default/grub.d/50_linuxmint.cfg'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-6.8.0-51-generic
Found initrd image: /boot/initrd.img-6.8.0-51-generic
Found linux image: /boot/vmlinuz-6.8.0-38-generic
Found initrd image: /boot/initrd.img-6.8.0-38-generic
Warning: os-prober will be executed to detect other bootable partitions.
Its output will be used to detect bootable binaries on them and create new boot entries.
Adding boot menu entry for UEFI Firmware Settings ...
done
```

image.png

---

6. Surveillance et Analyse

1. Affichez les journaux récents :

   ```
   sudo ausearch -i
   ```

2. Recherchez des événements spécifiques :

   ```
   sudo ausearch -k privilege_changes
   ```

3. Générer un rapport global :

```
sudo aureport
```

```
ap1-user@ap1user:~$ sudo aureport

Summary Report
======================
Range of time in logs: 19/01/2025 00:08:18.188 - 19/01/2025 00:18:36.300
Selected time for report: 19/01/2025 00:08:18 - 19/01/2025 00:18:36.300
Number of changes in configuration: 18
Number of changes to accounts, groups, or roles: 0
Number of logins: 0
Number of failed logins: 0
Number of authentications: 2
Number of failed authentications: 0
Number of users: 4
Number of terminals: 8
Number of host names: 1
Number of executables: 16
Number of commands: 18
Number of files: 10
Number of AVC's: 0
Number of MAC events: 2
Number of failed syscalls: 2
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of integrity events: 0
Number of virt events: 0
Number of keys: 5
Number of process IDs: 60
Number of events: 598
```

image.png

---

7. Pourquoi ces étapes sont importantes ?

- **Détection des activités suspectes** : L'audit système permet d'identifier les modifications ou comportements anormaux pour prévenir des intrusions.
- **Conformité et traçabilité** : Il répond aux exigences réglementaires en consignant les événements clés.
- **Réponse rapide aux incidents** : Les journaux d'audit facilitent l'analyse et la résolution des problèmes de sécurité.

4. Securisation de SSH

0. Introduction

La sécurisation de SSH (Secure Shell) est essentielle pour renforcer la protection des connexions distantes à un système Linux. Par exemple, les analyses de journaux de sécurité montrent que les attaques par force brute ciblent fréquemment les serveurs SSH non sécurisés, ce qui en fait une priorité pour les administrateurs système. En appliquant les bonnes pratiques décrites dans ce guide, vous pouvez minimiser les risques d'intrusion et garantir un environnement sécurisé.

---

1. Installation de SSH

1. Installez le service OpenSSH :

```
sudo apt install openssh-server -y
sudo apt install ssh -y
```

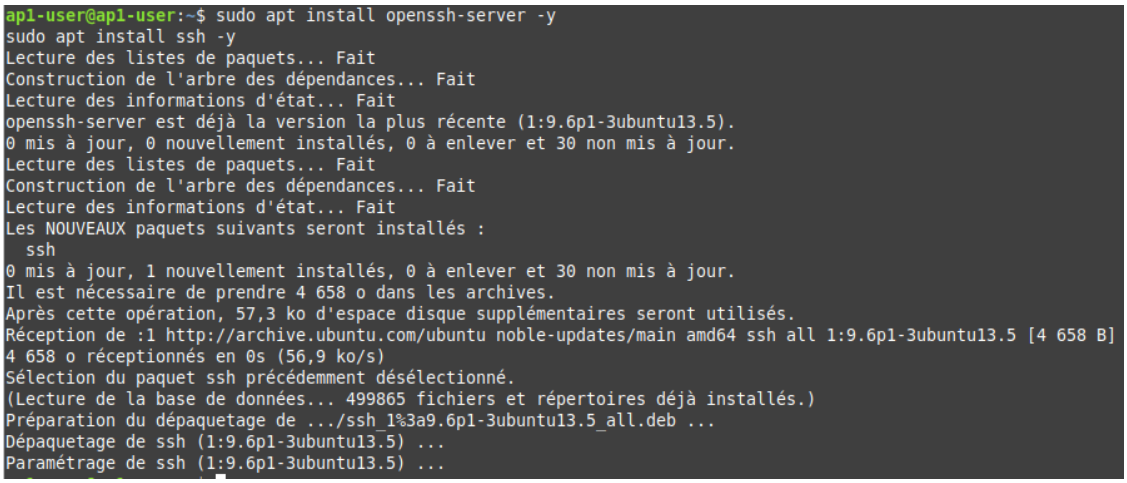


image.png

2. Activez et démarrez le service SSH :

```
sudo systemctl enable ssh
sudo systemctl start ssh
sudo systemctl status ssh
```

```
ap1-user@ap1-user:~$ sudo systemctl enable ssh
sudo systemctl start ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr/lib/systemd/system/ssh.service.
ap1-user@ap1-user:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Fri 2024-12-06 10:49:37 CET; 14s ago
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 33992 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 33993 (sshd)
      Tasks: 1 (limit: 4549)
     Memory: 1.2M (peak: 1.5M)
        CPU: 19ms
     CGroup: /system.slice/ssh.service
             └─33993 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

déc. 06 10:49:37 ap1-user systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
déc. 06 10:49:37 ap1-user sshd[33993]: Server listening on :: port 22.
déc. 06 10:49:37 ap1-user systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

image.png

3. Vérifiez l'état du service pour confirmer son fonctionnement.

---

2. Configuration de SSH

1. **Modifier les permissions sensibles** :

```
sudo chmod 700 /etc/ssh/sshd_config
sudo chmod 700 /etc/ssh/
```

```
ap1-user@ap1user:~$ sudo chmod 700 /etc/ssh/sshd_config
sudo chmod 700 /etc/ssh/
```

image.png

2. **Éditer le fichier de configuration** : Modifier les paramètres de `/etc/ssh/sshd_config` avec la commande suivante :

```
sudo gedit /etc/ssh/sshd_config
```

Modifiez les paramètres suivants pour améliorer la sécurité :

```
LoginGraceTime 2m
PermitRootLogin no
StrictModes yes
MaxAuthTries 3
MaxSessions 3

PubkeyAuthentication yes
```

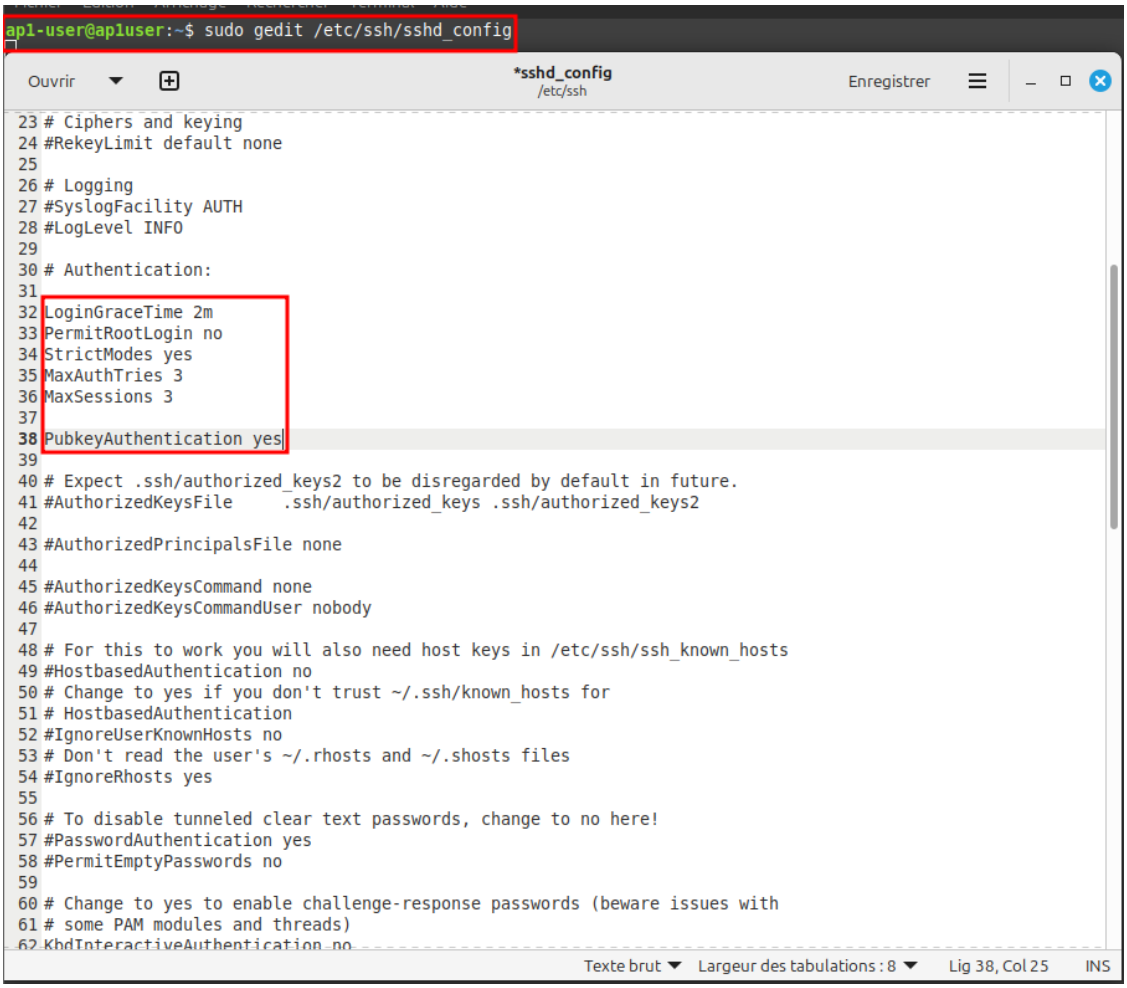


image.png

3. **Sauvegarder et appliquer les modifications** :

   - Sauvegardez le fichier et fermez l'éditeur.
   - Redémarrez le service SSH pour appliquer les changements :

```
sudo systemctl restart ssh
sudo systemctl status ssh
```

```
ap1-user@ap1-user:~$ sudo systemctl restart ssh
sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Fri 2024-12-06 11:19:30 CET; 15ms ago
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 34388 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 34389 (sshd)
      Tasks: 1 (limit: 4549)
     Memory: 1.2M (peak: 1.5M)
        CPU: 17ms
     CGroup: /system.slice/ssh.service
             └─34389 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

déc. 06 11:19:30 ap1-user systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
déc. 06 11:19:30 ap1-user sshd[34389]: Server listening on :: port 22.
déc. 06 11:19:30 ap1-user systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

image.png

- Explication des paramètres de configuration

1. **`LoginGraceTime 2m`** :
   - Définit le délai maximum pour saisir les informations d'authentification avant que la connexion ne soit interrompue.
2. **`PermitRootLogin no`** :
   - Désactive les connexions SSH en tant qu'utilisateur root, réduisant ainsi les risques liés aux attaques par force brute.
3. **`StrictModes yes`** :
   - Garantit que les permissions des fichiers et répertoires critiques sont correctement configurées.
4. **`MaxAuthTries 3`** :
   - Limite les tentatives d'authentification échouées à 3.
5. **`MaxSessions 3`** :
   - Réduit le nombre de sessions simultanées par utilisateur.
6. **`PubkeyAuthentication yes`** :
   - Active l'authentification par clé publique pour plus de sécurité.

---

3. Audit et suivi des connexions SSH

1. **Configuration des règles d'audit** : Ajoutez les règles suivantes dans le fichier `/etc/audit/rules.d/audit.rules` pour surveiller les modifications du fichier de configuration SSH et les connexions :

```
## Suivi des connexions SSH
-w /etc/ssh/sshd_config -p wa -k ssh_config_changes
-w /var/log/auth.log -p wa -k ssh_logins
```

```
ap1-user@ap1user:~$ sudo gedit /etc/audit/rules.d/audit.rules
```

Ouvrir — audit.rules — /etc/audit/rules.d — Enregistrer

```
1 ## Supprimer toutes les règles existantes
2 -D
3
4 ## Taille des tampons
5 -b 8192
6 # Ajustez cette valeur en fonction des besoins spécifiques.
7
8 ## Définitions des règles
9 -w /etc/passwd -p wa -k passwd_changes
10 -w /etc/shadow -p wa -k shadow_access
11 -a always,exit -F arch=b64 -S setuid -S setgid -k privilege_changes
12 -w /var/log/auth.log -p wa -k auth_changes
13 -w /boot/ -p wa -k boot_changes
14
15 ## Suivi des connexions SSH
16 -w /etc/ssh/sshd_config -p wa -k ssh_config_changes
17 -w /var/log/auth.log -p wa -k ssh_logins
```

image.png

2. **Redémarrage du service d'audit** : Appliquez les nouvelles règles en redémarrant `auditd` :

```
sudo systemctl restart auditd
sudo systemctl status auditd
```

```
ap1-user@ap1user:~$ sudo systemctl restart auditd
sudo systemctl status auditd
● auditd.service - Security Auditing Service
     Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-01-19 00:54:34 CET; 15ms ago
       Docs: man:auditd(8)
             https://github.com/linux-audit/audit-documentation
    Process: 4759 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
    Process: 4765 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/SUCCESS)
   Main PID: 4761 (auditd)
      Tasks: 2 (limit: 4549)
     Memory: 532.0K (peak: 2.3M)
        CPU: 26ms
     CGroup: /system.slice/auditd.service
             └─4761 /sbin/auditd

janv. 19 00:54:34 ap1user augenrules[4775]: enabled 1
janv. 19 00:54:34 ap1user augenrules[4775]: failure 1
janv. 19 00:54:34 ap1user augenrules[4775]: pid 4761
janv. 19 00:54:34 ap1user augenrules[4775]: rate_limit 0
janv. 19 00:54:34 ap1user augenrules[4775]: backlog_limit 8192
janv. 19 00:54:34 ap1user augenrules[4775]: lost 50
janv. 19 00:54:34 ap1user augenrules[4775]: backlog 1
janv. 19 00:54:34 ap1user augenrules[4775]: backlog_wait_time 60000
janv. 19 00:54:34 ap1user augenrules[4775]: backlog_wait_time_actual 0
janv. 19 00:54:34 ap1user systemd[1]: Started auditd.service - Security Auditing Service.
```

image.png

3. **Analyse des journaux d'audit** : Utilisez les commandes suivantes pour examiner les logs concernant SSH :

```
sudo ausearch -k ssh_logins
sudo aureport -x
```

```
ap1-user@ap1user:~$ sudo ausearch -k ssh_logins
sudo aureport -x
```

image.png

- `sudo ausearch -k ssh_logins` : Cette commande recherche les événements liés aux connexions SSH dans les journaux d'audit grâce à la clé `ssh_logins`.
- `sudo aureport -x` : Cette commande génère un rapport des commandes exécutées sur le système pour identifier toute activité suspecte.

4. **Dépannage :** Si vous rencontrez des problèmes, vérifiez que SSH écoute bien sur le port configuré avec :

   `sudo ss -l | grep ssh`

```
ap1-user@ap1user:~$ sudo ss -l | grep ssh
u_str LISTEN 0      5                                    /run/user/1000/gcr/ssh 20913                 * 0
u_str LISTEN 0      4096                 /run/user/1000/gnupg/S.gpg-agent.ssh 20952                 * 0
u_str LISTEN 0      10                           /run/user/1000/keyring/ssh 22837                 * 0
tcp   LISTEN 0      4096                                              *:ssh                       *:*
```

image.png

- **Explication** : Cette commande vérifie les ports sur lesquels SSH est en écoute pour s'assurer qu'il est opérationnel.

---

4. Pourquoi ces étapes sont importantes ?

- **Réduction des attaques par force brute** : Désactiver l'accès root et limiter les tentatives d'authentification renforcent la sécurité.
- **Sécurisation des connexions** : Activer l'authentification par clé publique et configurer des permissions strictes protègent contre les accès non autorisés.
- **Surveillance proactive** : Les audits et journaux permettent de détecter rapidement les activités suspectes et les modifications non autorisées.

5. Configuration du Pare-feu UFW

14. Introduction

Le pare-feu UFW (*Uncomplicated Firewall*) est un outil efficace et simple d'utilisation permettant de contrôler les connexions réseau entrantes et sortantes sur un système Linux. Par exemple, il peut être utilisé pour sécuriser un serveur web en autorisant uniquement les connexions HTTP (port 80) et HTTPS (port 443), tout en bloquant l'accès non autorisé à d'autres ports, comme Telnet ou SMB. Cette capacité à filtrer le trafic entrant et sortant

contribue à renforcer la sécurité réseau dans divers contextes. Une configuration adaptée est essentielle pour renforcer la sécurité des systèmes d'information.

---

15. 1. Vérification du statut du Pare-feu

Avant de configurer UFW, il est important de connaître son état actuel.

```
sudo ufw status
sudo ufw status verbose
sudo ufw status numbered
```

- **status** : Indique si le pare-feu est actif ou non.
- **verbose** : Fournit des détails supplémentaires.
- **numbered** : Affiche les règles avec un numéro unique.

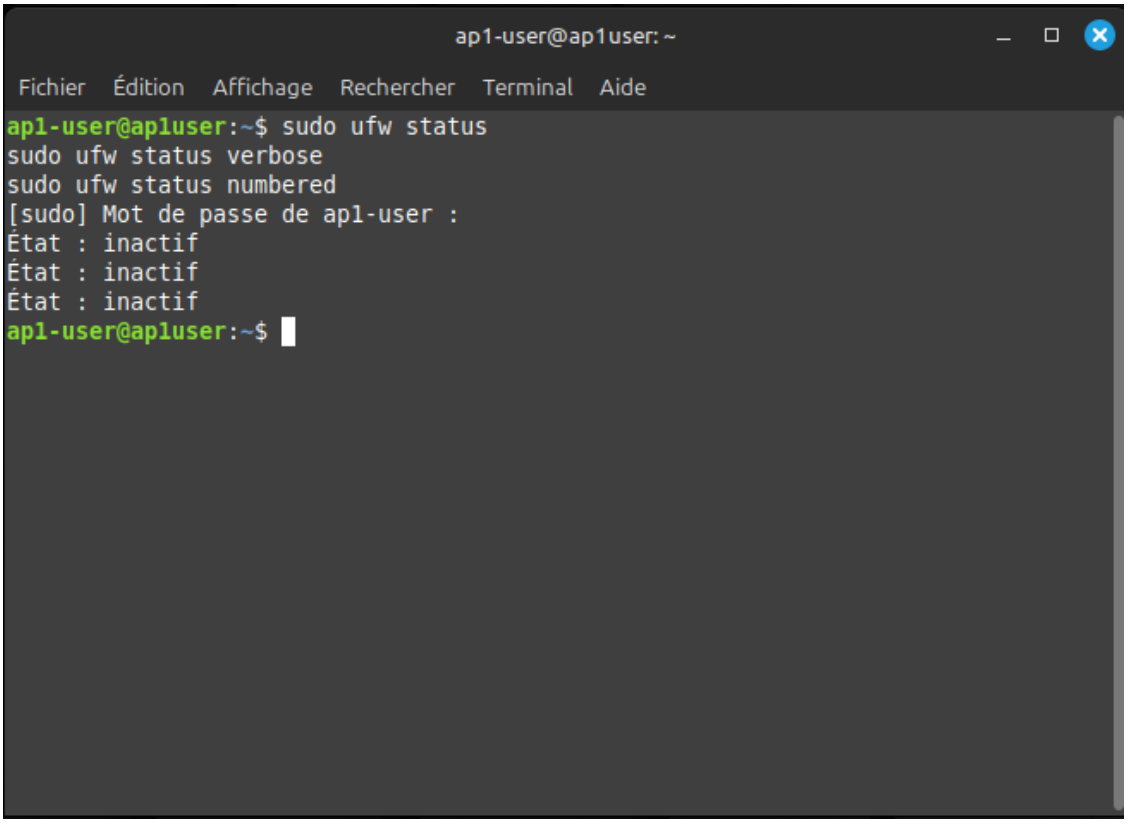


image.png

---

16. 2. Activation et Journalisation

Activer ou désactiver le pare-feu selon les besoins :

```
sudo ufw enable  # Activer UFW
# À utiliser lors de la mise en production pour assurer une sécurité de bas
e.
sudo ufw logging on  # Activer les logs
# Permet de surveiller les tentatives de connexion et d'analyser les compor
tements réseau.
sudo ufw disable # Désactiver UFW
# Utile lors de la maintenance pour éviter que le pare-feu bloque les opéra
tions nécessaires.
```

```
ap1-user@ap1user:~$ sudo ufw enable  # Activer UFW
sudo ufw logging on  # Activer les logs
Le pare-feu est actif et lancé au démarrage du système
Journalisation activée
```

image.png

> Remarque : La journalisation aide à suivre les événements du pare-feu pour une meilleure analyse.

---

3. Configuration des Règles Essentielles

Autoriser ou refuser l'accès à des services spécifiques :

Règles communes :

```
sudo ufw allow 22/tcp   # Autoriser SSH
sudo ufw allow 443/tcp  # Autoriser HTTPS
sudo ufw allow 80/tcp   # Autoriser HTTP
sudo ufw allow 631/tcp  # Autoriser CUPS (impression)
sudo ufw deny 23/tcp    # Refuser Telnet
sudo ufw deny 445/tcp   # Refuser SMB (Samba)
```

```
ap1-user@ap1user:~$ sudo ufw allow 22/tcp   # Autoriser SSH
sudo ufw allow 443/tcp  # Autoriser HTTPS
sudo ufw allow 80/tcp   # Autoriser HTTP
sudo ufw allow 631/tcp  # Autoriser CUPS (impression)
sudo ufw deny 23/tcp    # Refuser Telnet
sudo ufw deny 445/tcp   # Refuser SMB (Samba)
La règle a été ajoutée
La règle a été ajoutée (v6)
La règle a été ajoutée
La règle a été ajoutée (v6)
La règle a été ajoutée
La règle a été ajoutée (v6)
La règle a été ajoutée
La règle a été ajoutée (v6)
La règle a été ajoutée
La règle a été ajoutée (v6)
La règle a été ajoutée
La règle a été ajoutée (v6)
```

image.png

Options avancées :

```
sudo ufw allow out 161/udp  # Autoriser SNMP sortant
sudo ufw allow in 162/udp   # Autoriser SNMP entrant
sudo ufw allow 143/tcp      # Autoriser IMAP (messagerie)
sudo ufw allow 110/tcp      # Autoriser POP3
sudo ufw deny proto tcp from 10.0.0.0/8 to 192.168.0.1 port 25  # Refuser S
MTP spécifique
```

Règle par défaut :

```
sudo ufw default deny incoming  # Refuser tout trafic entrant par défaut
# Cette règle doit être accompagnée d'exceptions bien définies pour permett
re les connexions nécessaires, comme les ports 22 (SSH) ou 80/443 (HTTP/HTT
PS) dans le cas d'un serveur web.
```

---

4. Sauvegarde et Gestion des Règles

1. Sauvegarder les règles actuelles :

   ```
   sudo ufw status > ufw-rules-backup.txt
   cat ufw-rules-backup.txt
   ```

```
ap1-user@ap1user:~$ sudo ufw status > ufw-rules-backup.txt
cat ufw-rules-backup.txt
État : actif

Vers                       Action      De
----                       ------      --
22/tcp                     ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
631/tcp                    ALLOW       Anywhere
23/tcp                     DENY        Anywhere
445/tcp                    DENY        Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
443/tcp (v6)               ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
631/tcp (v6)               ALLOW       Anywhere (v6)
23/tcp (v6)                DENY        Anywhere (v6)
445/tcp (v6)               DENY        Anywhere (v6)
```

image.png

2. Afficher les services disponibles pour référence :

```
cat /etc/services
```

```
ap1-user@ap1user:~$ cat /etc/services
# Network services, Internet style
#
# Updated from https://www.iana.org/assignments/service-names-port-numbers/serv
#
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
```

image.png

5. Modifications des permissions des fichiers sensibles :

Appliquer des permissions restrictives :

```
sudo chmod 700 /etc/ufw/before.rules
```

```
ap1-user@ap1user:~$ sudo chmod 700 /etc/ufw/before.rules
```

image.png

---

6. Pourquoi ces étapes sont importantes ?

- **Renforcement de la sécurité réseau** : Bloquer les connexions non autorisées réduit le risque d'accès malveillant.
- **Contrôle précis du trafic** : UFW permet de définir des règles adaptées aux besoins spécifiques du projet.
- **Journalisation et audit** : Les logs facilitent l'analyse des tentatives d'intrusion et améliorent la gestion des incidents.

6. Configuration des Regles iptables

0. Introduction

`iptables` est un outil puissant pour gérer les règles de pare-feu sous Linux. Ce guide décrit les étapes pour installer, configurer, et gérer les règles `iptables`, avec des explications détaillées pour chaque commande et paramètre afin de renforcer la sécurité de votre système.

---

1. Installation d'iptables

Assurez-vous que `iptables` est installé sur votre système. Utilisez la commande suivante pour vérifier son installation avant de procéder :

```
iptables --version
```

Cette vérification évite une installation redondante.

---

2. Vérification des Règles Existantes

Avant de configurer de nouvelles règles, examinez les règles déjà en place :

```
sudo iptables -L -v
```

- L : Liste les règles actuelles.
- v : Affiche les détails supplémentaires.

---

3. Réinitialisation des Règles

Pour repartir sur une configuration propre, réinitialisez les règles existantes :

```
sudo iptables -F
```

⚠️ **Attention** : Cette commande supprime toutes les règles en cours, ce qui peut temporairement rendre votre système vulnérable. Assurez-vous d'appliquer immédiatement les nouvelles règles nécessaires après cette réinitialisation.

---

4. Configuration des Règles

1. Autoriser les connexions nécessaires :

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT # SSH
```

   - Le port **22** est utilisé pour le protocole SSH (Secure Shell), essentiel pour les connexions distantes sécurisées.

```
iptables -A INPUT -p tcp --dport 443 -j ACCEPT # HTTPS
```

   - Le port **443** permet les connexions HTTPS, garantissant des échanges chiffrés pour les sites web.

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT # HTTP
```

   - Le port **80** est utilisé pour les connexions HTTP, nécessaire si vous hébergez un serveur web non chiffré.

```
iptables -A INPUT -p tcp --dport 631 -j ACCEPT # CUPS (impression)
```

- Le port **631** est associé au service CUPS pour la gestion des impressions réseau.

2. Bloquer les connexions dangereuses :

```
iptables -A INPUT -p tcp --dport 23 -j REJECT # Telnet
```

- Le port **23** (Telnet) est obsolète et non sécurisé, souvent utilisé comme cible pour des attaques.

```
iptables -A INPUT -p tcp --dport 445 -j REJECT # SMB/SAMBA
```

- Le port **445** est lié au protocole SMB, fréquemment exploité par des logiciels malveillants.

3. Bloquer tout autre trafic entrant :

```
sudo iptables -A INPUT -j DROP
```

- `A INPUT` : Applique la règle aux paquets entrants.
- `p tcp` : Spécifie le protocole TCP.
- `-dport` : Définit le port concerné.
- `j` : Action à effectuer (ACCEPT, REJECT, DROP).

---

5. Gestion des Règles

1. Supprimer une Règle

   Pour supprimer une règle spécifique :

   1. Lister les règles avec leurs numéros :

      ```
      sudo iptables -L --line-numbers
      ```

   2. Supprimer la règle en fonction de son numéro :

      ```
      sudo iptables -D INPUT [NUMÉRO]
      ```

2. Sauvegarder les Règles

   Pour rendre les règles persistantes après redémarrage :

   ```
   sudo /sbin/iptables-save > /etc/iptables/rules.v4
   ```

   ⚠️ **Note** : Assurez-vous d'avoir les droits d'administrateur pour modifier le fichier `rules.v4`. Cela garantit que la commande fonctionne correctement et sauvegarde les règles sans erreur.

---

6. Tester les Règles

Utilisez nmap pour vérifier l'ouverture des ports :

```
nmap -p 22,80,443,23,445 [ADRESSE_IP]
```

⚠️ **Note** : Remplacez [ADRESSE_IP] par l'adresse réelle du système cible.

1. Limiter les Connexions pour Prévenir les Attaques DoS

   Ajoutez des règles pour limiter les connexions SSH :

   ```
   iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --set
   iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 60 --hitcount 4 -j DROP
   ```

   Cela limite les nouvelles connexions SSH à 3 par minute, réduisant les risques d'attaques par déni de service.

2. Journalisation des Paquets Bloqués

   Ajoutez une règle pour journaliser les paquets bloqués :

   ```
   iptables -A INPUT -j LOG --log-prefix "iptables-block: " --log-level 4
   ```

   Cela permet de surveiller les activités suspectes et de les analyser.

---

7. Alternatives Modernes

1. Introduction à nftables

   iptables est progressivement remplacé par nftables sur certaines distributions modernes. Pour les nouveaux systèmes, envisagez d'utiliser nftables, qui offre une syntaxe plus simple et des fonctionnalités avancées.

2. Distributions utilisant nftables par défaut

   - **Debian** : Depuis la version 10 (Buster), Debian utilise nftables comme backend par défaut pour iptables. Plus d'informations
   - **Red Hat Enterprise Linux (RHEL)** : À partir de RHEL 8, nftables est utilisé par défaut pour la gestion des pare-feu. Plus d'informations
   - **CentOS** : En tant que dérivé de RHEL, CentOS 8 et les versions ultérieures utilisent également nftables par défaut.

- **Fedora** : Fedora a migré vers `nftables` comme backend par défaut dans ses versions récentes.
- **Ubuntu** : Bien qu'Ubuntu continue d'utiliser `iptables` par défaut, les versions récentes incluent le support de `nftables`, et les utilisateurs peuvent choisir de l'utiliser pour la gestion des pare-feu.

Pour en savoir plus, consultez la documentation officielle.

---

8. Pourquoi ces étapes sont importantes ?

- **Contrôle précis du trafic** : `iptables` permet de gérer les connexions autorisées et de bloquer celles qui sont dangereuses, renforçant ainsi la sécurité réseau.
- **Prévention des attaques** : Limiter les connexions SSH et bloquer les ports vulnérables protège contre les attaques par force brute et autres intrusions.
- **Traçabilité** : Les règles de journalisation offrent une visibilité sur les activités suspectes et facilitent l'audit des événements réseau.

7. Installation de ClamAV et Lynis

1. Introduction

Dans ce guide, nous explorerons deux outils essentiels pour renforcer la sécurité des systèmes Linux : **Lynis** et **ClamAV**. Lynis est un outil d'audit de sécurité qui analyse votre système pour identifier les configurations sécurisées et les vulnérabilités potentielles. ClamAV, accompagné de son interface graphique ClamTK, offre une solution antivirus efficace pour détecter et éliminer les logiciels malveillants. Ce document détaille les étapes d'installation, de configuration et d'utilisation de ces outils pour garantir un système sécurisé et performant.

---

1. Installation de Lynis

1. **Installation de Lynis :**

   Lynis est un outil d'audit de sécurité utilisé pour évaluer les vulnérabilités potentielles d'un système.

   ```
   sudo apt-get install lynis -y
   ```

```
ap1-linux@ap1linux:/$ sudo apt-get install lynis -y
```

07%20Installation%20de%20ClamAV%20et%20Lynis%20182dbb723a2881ff915adc8046f6862a/image.png

Une fois installé, vérifiez la version de Lynis pour confirmer que l'installation s'est déroulée correctement :

```
lynis --version
```

```
ap1-user@ap1user:~$ lynis --version
3.0.9
```

image.png

2. **Exécution de l'audit système :**

   Lynis analyse le système pour identifier les configurations correctes et les améliorations possibles. Utilisez la commande suivante :

   ```
   sudo lynis audit system
   ```

   ```
   ap1-user@ap1user:~$ sudo lynis audit system
   ```

   image.png

   Cela génère un rapport complet des vulnérabilités et recommandations. Pour interpréter les résultats :

   - Les sections **[OK]** indiquent des configurations adéquates.
   - Les sections **[WARNING]** signalent des paramètres nécessitant une attention immédiate.
   - Les sections **[SUGGESTION]** fournissent des recommandations pour améliorer la sécurité ou les performances. Consultez la documentation officielle pour des détails spécifiques.

   Pour sauvegarder dans un fichier le résultat de la commande `sudo lynis audit system` vous pouvez utilisez la commande suivante :

   ```
   sudo lynis audit system > rapport_lynis.txt
   ```

   Puis utilisez par exemple gedit ou cat pour l'afficher :

   ```
   sudo cat rapport_lynis.txt
   # Ou
   sudo gedit rapport_lynis.txt
   ```

```
ap1-user@ap1user:~$ sudo lynis audit system > rapport_lynis.txt
pgrep: pattern that searches for process name longer than 15 characters will result in zero matches
Try `pgrep -f' option to match against the complete command line.
ap1-user@ap1user:~$ sudo gedit rapport_lynis.txt
ap1-user@ap1user:~$ sudo cat rapport_lynis.txt

[ Lynis 3.0.9 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]
  - Detecting language and localization                       [ fr ]

  ---------------------------------------------------
  Program version:           3.0.9
  Operating system:          Linux
  Operating system name:     Linux Mint
  Operating system version:  22
  Kernel version:            6.8.0
  Hardware platform:         x86_64
  Hostname:                  ap1user
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /etc/lynis/plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  fr
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                                  [ PAS DE MISE A JOUR ]
```

image.png

---

2. Installation de ClamAV

1. **Installation de ClamAV :**

   ClamAV est un antivirus open-source permettant d'identifier et de supprimer les logiciels malveillants sur un système Linux. Installez-le avec la commande suivante :

   ```
   sudo apt install clamav clamav-daemon -y
   ```

   ```
   ap1-linux@ap1linux:/usr/local/lynis/lynis$ sudo apt install clamav clamav-daemon
   ```

   07%20Installation%20de%20ClamAV%20et%20Lynis%20182dbb723a2881ff915adc8046f6862a/image%204.png

2. **Vérification de l'installation :**

   Vérifiez si ClamAV est correctement installé avec :

   ```
   clamscan --version
   ```

   Si aucune version n'apparaît, l'installation a échoué.

```
ap1-linux@ap1linux:/usr/local/lynis/lynis$ clamscan --version
ClamAV 1.0.7/27480/Sat Dec  7 10:42:16 2024
```

07%20Installation%20de%20ClamAV%20et%20Lynis%20182dbb723a2881ff915adc8046f6862a/image%205.png

3. **Mise à jour de la base de signatures :**

   ClamAV utilise une base de signatures pour identifier les menaces. Mettez-la à jour comme suit :

   - Arrêtez le service freshclam :

     ```
     sudo systemctl stop clamav-freshclam
     sudo systemctl status clamav-freshclam
     ```

```
ap1-linux@ap1linux:/usr/local/lynis/lynis$ sudo systemctl stop clamav-freshclam
ap1-linux@ap1linux:/usr/local/lynis/lynis$ sudo systemctl status clamav-freshclam
○ clamav-freshclam.service - ClamAV virus database updater
     Loaded: loaded (/usr/lib/systemd/system/clamav-freshclam.service; disabled; preset: en>
     Active: inactive (dead)
       Docs: man:freshclam(1)
             man:freshclam.conf(5)
             https://docs.clamav.net/

déc. 07 18:16:57 ap1linux freshclam[4601]: Sat Dec  7 18:16:57 2024 -> bytecode database av>
déc. 07 18:16:58 ap1linux freshclam[4601]: Testing database: '/var/lib/clamav/tmp.8a54039d3>
déc. 07 18:16:58 ap1linux freshclam[4601]: Database test passed.
déc. 07 18:16:58 ap1linux freshclam[4601]: Sat Dec  7 18:16:58 2024 -> bytecode.cvd updated>
déc. 07 18:16:58 ap1linux freshclam[4601]: WARNING: Clamd was NOT notified: Can't connect t>
déc. 07 18:29:14 ap1linux freshclam[4601]: Update process terminated
déc. 07 18:29:14 ap1linux systemd[1]: Stopping clamav-freshclam.service - ClamAV virus data>
déc. 07 18:29:14 ap1linux systemd[1]: clamav-freshclam.service: Deactivated successfully.
déc. 07 18:29:14 ap1linux systemd[1]: Stopped clamav-freshclam.service - ClamAV virus datab>
déc. 07 18:29:14 ap1linux systemd[1]: clamav-freshclam.service: Consumed 16.970s CPU time, >
lines 1-17/17 (END)
```

     07%20Installation%20de%20ClamAV%20et%20Lynis%20182dbb723a2881ff915adc8046f6862a/image%206.png

   - Lancez la mise à jour :

     ```
     sudo freshclam
     ```

     Note : Il est recommandé d'exécuter cette mise à jour régulièrement, idéalement quotidiennement, pour garantir une protection optimale contre les nouvelles menaces.

```
ap1-linux@ap1linux:/usr/local/lynis/lynis$ sudo freshclam
ClamAV update process started at Sat Dec  7 18:31:09 2024
Sat Dec  7 18:31:09 2024 -> daily.cvd database is up-to-date (version: 27480, sigs: 2069181,
 f-level: 90, builder: raynman)
Sat Dec  7 18:31:09 2024 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-l
evel: 90, builder: sigmgr)
Sat Dec  7 18:31:09 2024 -> bytecode.cvd database is up-to-date (version: 335, sigs: 86, f-l
evel: 90, builder: raynman)
```

image.png

- Relancez et activez le service freshclam :

```
sudo systemctl start clamav-freshclam
sudo systemctl enable clamav-freshclam
```

Activer automatiquement ce service garantit que les signatures sont toujours mises à jour, même en cas de redémarrage du système, renforçant ainsi la protection continue contre les menaces émergentes.

Vérifiez son statut :

```
sudo systemctl status clamav-freshclam
```

```
ap1-linux@ap1linux:/usr/local/lynis/lynis$ sudo systemctl start clamav-freshclam
sudo systemctl status clamav-freshclam
● clamav-freshclam.service - ClamAV virus database updater
     Loaded: loaded (/usr/lib/systemd/system/clamav-freshclam.service; disabled; preset: en>
     Active: active (running) since Sat 2024-12-07 18:33:53 CET; 17ms ago
       Docs: man:freshclam(1)
             man:freshclam.conf(5)
             https://docs.clamav.net/
   Main PID: 5424 (freshclam)
      Tasks: 1 (limit: 4549)
     Memory: 2.6M (peak: 2.8M)
        CPU: 9ms
     CGroup: /system.slice/clamav-freshclam.service
             └─5424 /usr/bin/freshclam -d --foreground=true

déc. 07 18:33:53 ap1linux systemd[1]: Started clamav-freshclam.service - ClamAV virus datab>
déc. 07 18:33:53 ap1linux freshclam[5424]: ClamAV update process started at Sat Dec  7 18:3>
```

07%20Installation%20de%20ClamAV%20et%20Lynis%20182dbb723a2881ff915adc8046f6862a/image%208.png

4. **Installation de ClamTK :**

ClamTK est une interface graphique pour ClamAV, simplifiant son utilisation :

```
sudo apt install clamtk -y
```

ClamTK ne nécessite généralement pas de permissions spécifiques pour fonctionner, mais pour effectuer des analyses approfondies, il peut être nécessaire de l'exécuter avec des droits administratifs. Aucune configuration supplémentaire n'est requise après l'installation.

```
ap1-linux@ap1linux:/usr/local/lynis/lynis$ sudo apt install clamtk -y
```

07%20Installation%20de%20ClamAV%20et%20Lynis%20182dbb723a2881ff915adc8046f6862a/image%209.png

5. **Lancer ClamTK :**

   Exécutez ClamTK pour une utilisation interactive :

   `clamtk`

```
ap1-linux@ap1linux:/usr/local/lynis/lynis$ clamtk
```

07%20Installation%20de%20ClamAV%20et%20Lynis%20182dbb723a2881ff915adc8046f6862a/image%2010.png

Une fenêtre graphique apparaîtra pour faciliter la gestion des analyses et des mises à jour.

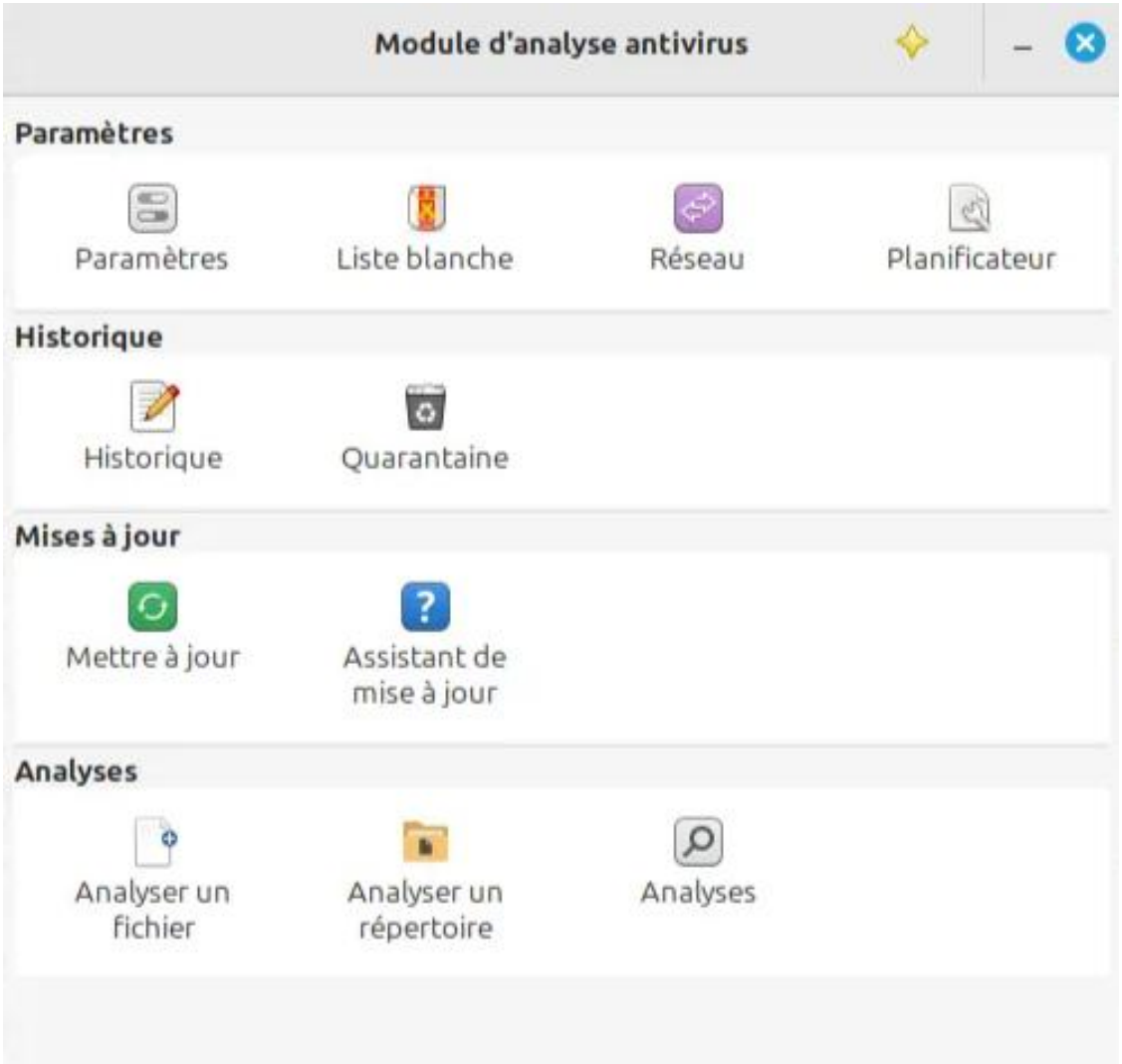


image.png

3. Pourquoi ces étapes sont importantes ?

- **Renforcement de la sécurité** : Lynis identifie les vulnérabilités et ClamAV détecte les logiciels malveillants, réduisant les risques d'attaques.
- **Audit et conformité** : Lynis aide à évaluer la sécurité du système et à se conformer aux meilleures pratiques.
- **Protection proactive** : Les mises à jour régulières de ClamAV assurent une défense continue contre les menaces émergentes.

8. Installation de fail2ban

0. Introduction

Fail2Ban est un outil essentiel pour sécuriser les serveurs Linux contre les attaques par force brute et autres tentatives d'intrusion. En surveillant les journaux d'accès, il peut bloquer automatiquement les adresses IP malveillantes en configurant des règles de pare-feu.

---

1. Installation de Fail2Ban

Pour installer Fail2Ban sur un système Linux, utilisez la commande suivante :

```
sudo apt install fail2ban -y
```

Cette commande installe le logiciel Fail2Ban à partir des dépôts officiels de votre distribution.

```
ap1-linux@ap1linux:/$ sudo apt install fail2ban -y
```

08%20Installation%20de%20fail2ban%20182dbb723a28812c80a6c47812741a74/image.png

---

2. Vérification du statut de Fail2Ban

Une fois l'installation terminée, vérifiez si le service Fail2Ban est actif avec la commande suivante :

```
systemctl status fail2ban.service
```

```
ap1-user@ap1user:~$ systemctl status fail2ban.service
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-01-19 01:57:30 CET; 1min 29s ago
       Docs: man:fail2ban(1)
   Main PID: 114588 (fail2ban-server)
      Tasks: 5 (limit: 4549)
     Memory: 19.6M (peak: 20.3M)
        CPU: 191ms
     CGroup: /system.slice/fail2ban.service
             └─114588 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

janv. 19 01:57:30 ap1user systemd[1]: Started fail2ban.service - Fail2Ban Service.
janv. 19 01:57:31 ap1user fail2ban-server[114588]: 2025-01-19 01:57:31,001 fail2ban.configreader   [114588]: WARNING>
janv. 19 01:57:31 ap1user fail2ban-server[114588]: Server ready
lines 1-14/14 (END)
```

image.png

Par défaut, le service est installé mais désactivé. Cette commande affiche son état actuel.

---

3. Activation et démarrage du service

Pour que Fail2Ban fonctionne en permanence, activez et démarrez le service :

```
sudo systemctl enable fail2ban
sudo systemctl start fail2ban
sudo systemctl status fail2ban
```

```
ap1-user@ap1user:~$ sudo systemctl enable fail2ban
sudo systemctl start fail2ban
sudo systemctl status fail2ban
Synchronizing state of fail2ban.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-01-19 01:57:30 CET; 2min 3s ago
       Docs: man:fail2ban(1)
   Main PID: 114588 (fail2ban-server)
      Tasks: 5 (limit: 4549)
     Memory: 19.6M (peak: 20.3M)
        CPU: 208ms
     CGroup: /system.slice/fail2ban.service
             └─114588 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

janv. 19 01:57:30 ap1user systemd[1]: Started fail2ban.service - Fail2Ban Service.
janv. 19 01:57:31 ap1user fail2ban-server[114588]: 2025-01-19 01:57:31,001 fail2ban.configreader   [114588]: WARNING>
janv. 19 01:57:31 ap1user fail2ban-server[114588]: Server ready
lines 1-14/14 (END)
```

image.png

Ces commandes assurent que le service Fail2Ban démarre automatiquement après chaque redémarrage du système.

---

4. Pourquoi ces étapes sont importantes ?

- **Protection contre les attaques** : Fail2Ban bloque automatiquement les adresses IP malveillantes, réduisant les risques d'intrusion.
- **Automatisation de la sécurité** : L'activation et le démarrage du service garantissent une défense continue sans intervention manuelle.
- **Surveillance proactive** : En analysant les journaux, Fail2Ban détecte rapidement les comportements suspects pour prévenir les attaques.

9. Desactivation de l'Execution de Scripts dans /tmp

0. Introduction

Le répertoire `/tmp` est couramment utilisé pour stocker des fichiers temporaires, y compris par des logiciels comme LibreOffice ou OnlyOffice qui nécessitent un accès exécutif pour certains de leurs processus. Cependant, ce répertoire peut devenir une cible pour des scripts malveillants. Cette documentation propose une approche sécurisée permettant de protéger le système tout en maintenant le fonctionnement normal des logiciels.

---

1. Vérification des Options de Montage Actuelles

Pour identifier les options actuelles de montage pour `/tmp`, exécutez la commande suivante :

```
sudo mount | grep /tmp
```

```
ap1-user@ap1user:~$ sudo mount | grep /tmp
ap1-user@ap1user:~$
```

image.png

Cela permet de savoir si des options comme `noexec`, `nosuid` ou `nodev` sont déjà activées. Les options actuelles sont listées dans la colonne "options".

---

2. Sécurisation du Répertoire /tmp

2.1 : Configuration Sécurisée de /tmp

Modifiez le fichier `/etc/fstab` pour désactiver l'exécution de scripts dans `/tmp` tout en maintenant son accessibilité pour les usages nécessaires :

```
sudo gedit /etc/fstab
```

Ajoutez ou modifiez la ligne suivante :

```
tmpfs /tmp tmpfs defaults,nosuid,nodev 0 0
```

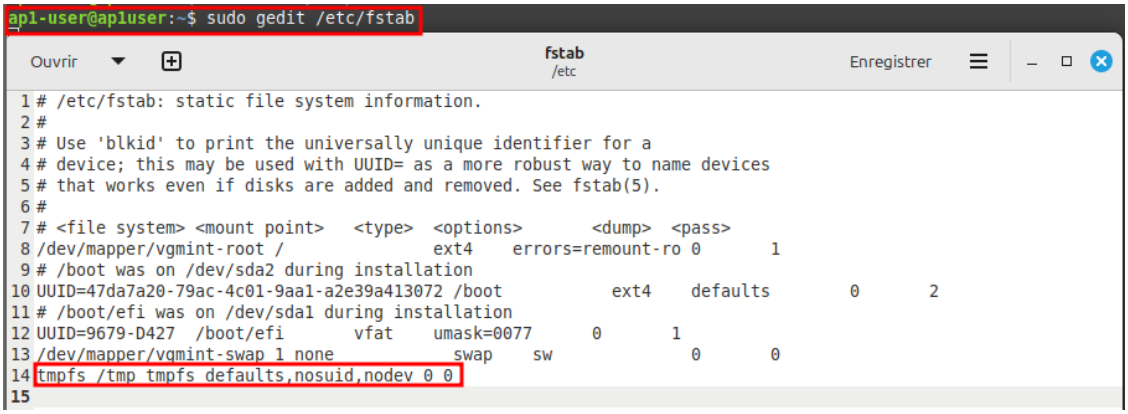


image.png

Cette configuration utilise `tmpfs` pour monter `/tmp` avec les options suivantes :

- `nosuid` : Désactive les privilèges `suid`.
- `nodev` : Interdit la création de périphériques spéciaux.

⚠️ **Note importante** : L'option `noexec` n'est pas utilisée ici pour éviter tout problème avec des logiciels nécessitant un accès exécutif temporaire.

2.2 : Appliquer les Changements

Rechargez les unités de montage de systemd pour que le système prenne en compte les modifications apportées à `/etc/fstab` :

```
sudo systemctl daemon-reload
```

Puis, appliquez les nouvelles options en remontant `/tmp` :

```
sudo mount -a
```

Vérifiez que les options de montage sont correctes :

```
mount | grep /tmp
```

Exemple de sortie attendue :

```
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,relatime,inode64)
```

```
ap1-user@ap1user:~$ sudo systemctl daemon-reload
ap1-user@ap1user:~$ sudo mount -a
ap1-user@ap1user:~$ mount | grep /tmp
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,relatime,inode64)
ap1-user@ap1user:~$
```

image.png

---

3. Tests de Fonctionnement

1. Test de nosuid
    1. Créez un binaire SUID :

        ```
        mkdir /tmp/suidtest
        cd /tmp/suidtest
        echo -e '#!/bin/bash\necho "UID: $(id -u)"' > test_suid.sh
        chmod +x test_suid.sh
        ```

        ```
        ap1-user@ap1user:~$ mkdir /tmp/suidtest
        cd /tmp/suidtest
        echo -e '#!/bin/bash\necho "UID: $(id -u)"' > test_suid.sh
        chmod +x test_suid.sh
        ```

        image.png

    2. Activez le bit SUID :

        ```
        sudo chown root:root test_suid.sh
        sudo chmod u+s test_suid.sh
        ls -l test_suid.sh
        ```

        Vous devriez voir un s dans les permissions, par exemple :

        ```
        -rwsr-xr-x 1 root root 34 jan 14 12:00 test_suid.sh
        ```

        ```
        ap1-user@ap1user:/tmp/suidtest$ sudo chown root:root test_suid.sh
        sudo chmod u+s test_suid.sh
        ls -l test_suid.sh
        -rwsrwxr-x 1 root root 33 janv. 19 02:06 test_suid.sh
        ```

        image.png

    3. Exécutez le script en tant qu'utilisateur non privilégié :

```
./test_suid.sh
```

```
ap1-user@ap1user:/tmp/suidtest$ ./test_suid.sh
UID: 1000
ap1-user@ap1user:/tmp/suidtest$ sudo ./test_suid.sh
UID: 0
```

image.png

Avec `nosuid`, il n'y aura pas d'élévation de privilèges (l'UID affiché sera celui de l'utilisateur courant).

2. Test de nodev
    1. Créez un fichier de périphérique :

    ```
    sudo mknod /tmp/test_dev b 7 0
    ls -l /tmp/test_dev
    ```

    Vous devriez voir :

    ```
    brw-r--r-- 1 root root 7, 0 jan 14 12:00 /tmp/test_dev
    ```

    ```
    ap1-user@ap1user:/tmp/suidtest$ sudo mknod /tmp/test_dev b 7 0
    ls -l /tmp/test_dev
    brw-r--r-- 1 root root 7, 0 janv. 19 02:09 /tmp/test_dev
    ```

    image.png

    2. Essayez d'utiliser ce pseudo-device :

    ```
    sudo mount /tmp/test_dev /mnt
    ```

    Si tout fonctionne vous obtiendrez une erreur.

    ```
    ap1-user@ap1user:/tmp/suidtest$ sudo mount /tmp/test_dev /mnt
    mount: /mnt: impossible de monter /tmp/test_dev en lecture seule.
           dmesg(1) may have more information after failed mount system call.
    ```

    image.png

    Ou :

    ```
    sudo losetup /dev/loop7 /tmp/test_dev
    ```

    Si tout fonctionne vous obtiendrez une erreur.

---

4. Pourquoi ces étapes sont importantes ?

- **Réduction des risques d'exploitation** : Désactiver l'exécution de scripts dans `/tmp` limite les possibilités d'exploiter ce répertoire pour des attaques.
- **Protection des privilèges système** : Les options `nosuid` et `nodev` renforcent la sécurité en empêchant l'élévation non autorisée des droits.
- **Maintien de la stabilité** : Ces modifications sécurisent le système tout en assurant le bon fonctionnement des applications nécessitant l'utilisation de `/tmp`.

10. Strategie de securite locale

1. Introduction

La mise en place d'une stratégie de sécurité locale pour les postes sous Linux Mint est essentielle pour garantir la protection des données et des systèmes de l'entreprise. Cette section décrit les étapes nécessaires pour configurer la sécurité locale, incluant la gestion des utilisateurs et la configuration des mots de passe.

---

1. Stratégie de mot de passe

1. **Installer les paquets requis** :

   ```
   sudo apt install libpam-pwquality libpwquality-tools -y
   ```

   ```
   ap1-user@ap1user:/tmp/suidtest$ sudo apt install libpam-pwquality libpwquality-tools -y
   ```

   image.png

2. **Modifier le fichier PAM commun** :

   ```
   sudo gedit /etc/pam.d/common-password
   ```

   Ajouter ou modifier les lignes suivantes :

   - **Première ligne à modifier** :

     ```
     password requisite pam_pwquality.so retry=3 minclass=4
     ```

   - **Deuxième ligne à modifier** :

     ```
     password [success=1 default=ignore] pam_unix.so obscure use_aut
     htok try_first_pass yescrypt minlen=12 remember=3
     ```

3. **Enregistrer les modifications** :

   - Appuyez sur `Ctrl+X` pour quitter, `O` pour enregistrer et `Entrée` pour confirmer.

```
#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords.  The default is pam_unix.

# Explanation of pam_unix options:
# The "yescrypt" option enables
#hashed passwords using the yescrypt algorithm, introduced in Debian
#11.  Without this option, the default is Unix crypt.  Prior releases
#used the option "sha512"; if a shadow password hash will be shared
#between Debian 11 and older releases replace "yescrypt" with "sha512"
#for compatibility .  The "obscure" option replaces the old
#`OBSCURE_CHECKS_ENAB' option in login.defs.  See the pam_unix manpage
#for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password        requisite                       pam_pwquality.so retry=3 minclass=4
password        [success=1 default=ignore]      pam_unix.so obscure use_authtok try_first_pass yescrypt minlen=12 remember=3
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
password        optional        pam_gnome_keyring.so
password        optional        pam_ecryptfs.so
# end of pam-auth-update config
```

image.png

Explications des paramètres configurés

- **`pam_pwquality.so`** : Ce module impose des exigences de qualité pour les mots de passe :
  - `retry=3` : Permet trois tentatives avant de renvoyer une erreur.
  - `minclass=4` : Exige que le mot de passe contienne au moins 4 classes de caractères différentes (majuscules, minuscules, chiffres, caractères spéciaux).
- **`pam_unix.so`** : Ce module gère l'authentification Unix traditionnelle :
  - `obscure` : Implique des vérifications supplémentaires pour garantir la complexité des mots de passe.
  - `use_authtok` : Réutilise le jeton d'authentification déjà saisi (par exemple, pour confirmer le mot de passe).
  - `try_first_pass` : Tente d'utiliser le mot de passe saisi pour éviter de le redemander.
  - `yescrypt` : Définit l'algorithme de chiffrement utilisé pour stocker les mots de passe, offrant une meilleure sécurité que les anciens algorithmes.
  - `minlen=12` : Impose une longueur minimale de 12 caractères pour les mots de passe.
  - `remember=3` : Retient les trois derniers mots de passe pour empêcher leur réutilisation.

---

2. Création d'un utilisateur standard

1. **Accéder à la gestion des utilisateurs**

   - Cliquez sur le logo Mint en bas à gauche de l'écran. *(1)*
   - Recherchez "Utilisateurs et groupes" dans la barre de recherche *(2)* et ouvrez l'application. *(3)* Entrez ensuite votre mot de passe.

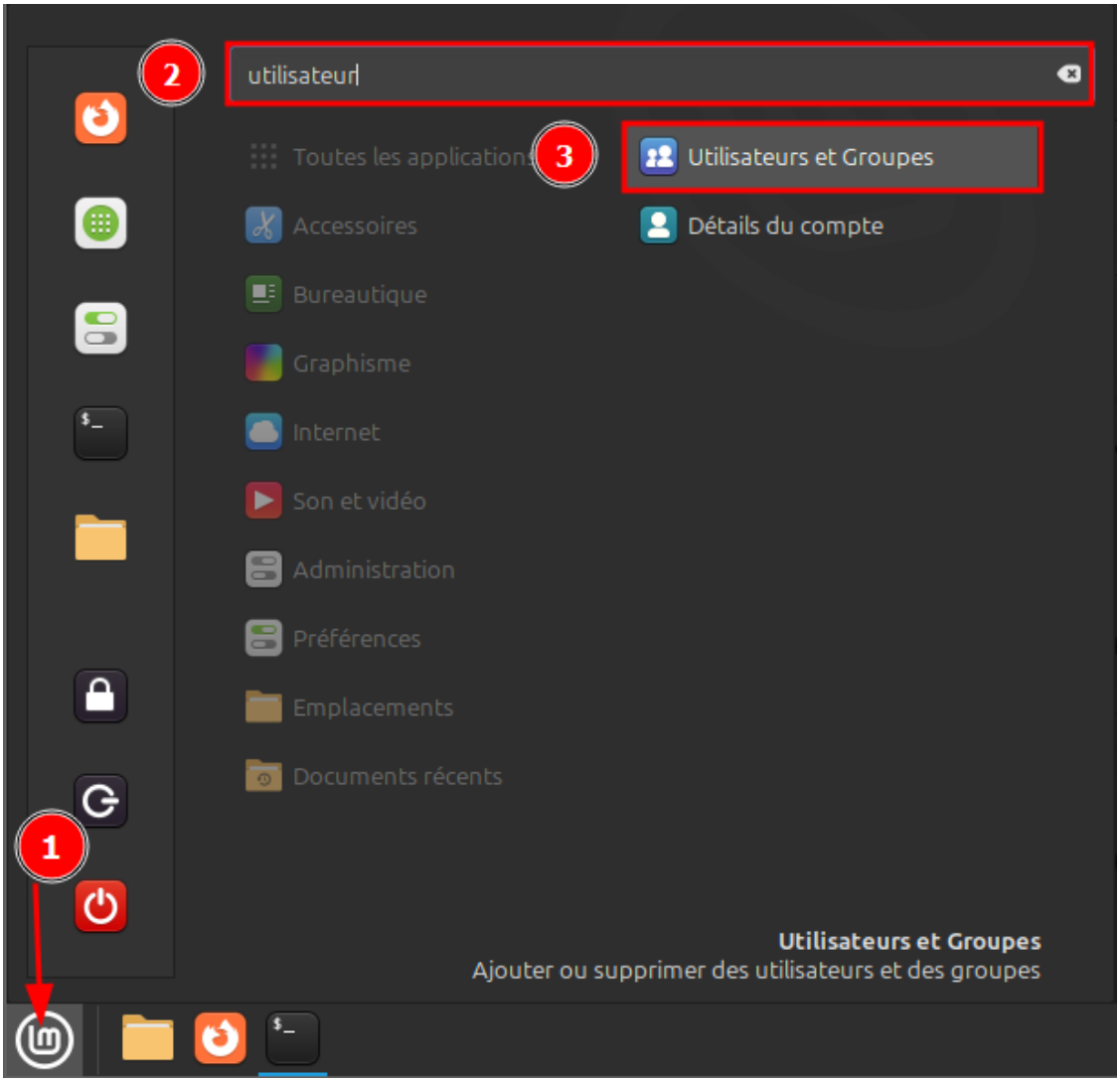


image.png

2. **Ajout d'un utilisateur**

   - Dans la fenêtre "Utilisateurs et groupes", cliquez sur "Ajouter".*(1)*
   - Remplissez le nom complet *(2)* ainsi que le nom d'utilisateur *(3)*
   - Cliquez sur "Ajouter" pour finaliser. *(4)*

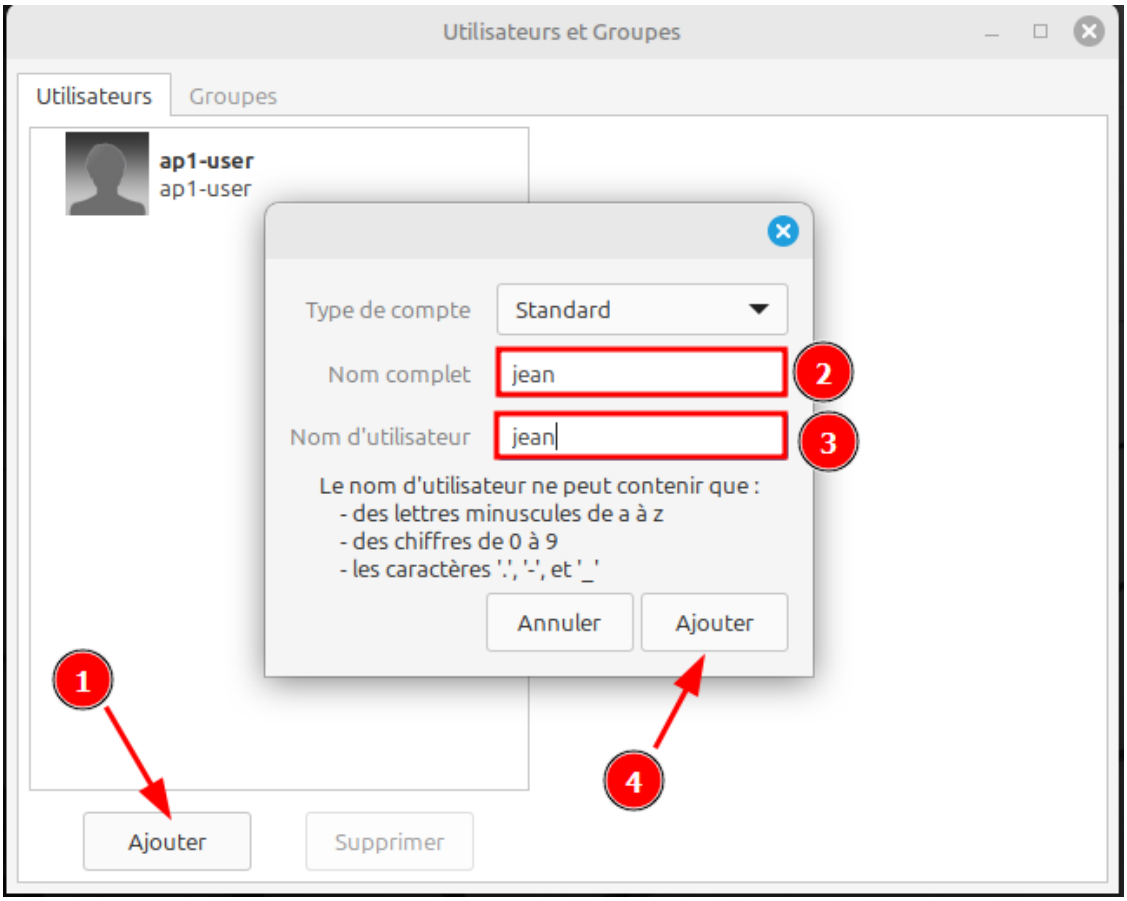


image.png

- Sélectionnez ensuite votre nouvel utilisateur.*(1)*
- Cliquez sur le champ Mot de passe*(2)*
- Entrez un mot de passe*(3)* puis confirmez le.*(4)* (Ce mot de passe est le mot de passe que jean devra entrer pour créer son mot de passe)
- Cliquez sur Modifier. *(5)*

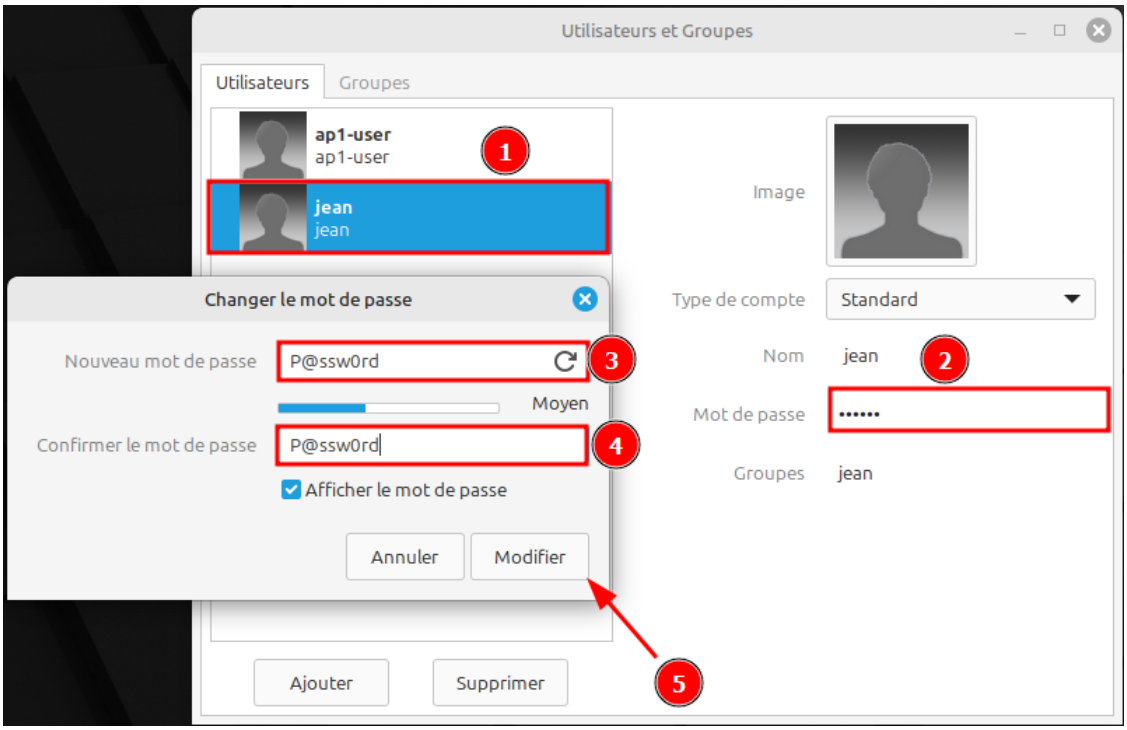


image.png

3. **Configurer une expiration de 90 jours** :

```
sudo chage -M 90 <nom_utilisateur>
```

Pour vérifier la configuration vous pouvez utiliser la commande :

```
sudo chage -l <nom_utilisateur>
```

```
apl-user@apluser:~$ sudo chage -l jean
Dernière modification du mot de passe                                : janv. 19, 2025
Le mot de passe expire                                               : avril 19, 2025
Mot de passe inactif                                                 : jamais
Le compte expire                                                     : jamais
Nombre minimal de jours entre deux changements de mot de passe       : 0
Nombre maximal de jours entre deux changements du mot de passe       : 90
Nombre de jours d'avertissements avant que le mot de passe n'expire  : 7
```

image.png

4. **Forcer une modification du mot de passe lors de la première connexion** :

```
sudo passwd --expire <nom_utilisateur>
```

Pour vérifier la configuration vous pouvez utiliser la commande :

```
sudo chage -l <nom_utilisateur>
```

```
ap1-user@ap1user:~$ sudo passwd --expire jean
passwd : mot de passe changé.
ap1-user@ap1user:~$ sudo chage -l jean
Dernière modification du mot de passe                                : le mot de passe doit être changé
Le mot de passe expire                                    : le mot de passe doit être changé
Mot de passe inactif                                      : le mot de passe doit être changé
Le compte expire                                                  : jamais
Nombre minimal de jours entre deux changements de mot de passe          : 0
Nombre maximal de jours entre deux changements du mot de passe          : 90
Nombre de jours d'avertissements avant que le mot de passe n'expire     : 7
```

image.png

5. Vérification de la configuration :

    1. Déconnectez-vous de votre session en cours en utilisant le menu utilisateur.

       Pour cela cliquez sur le logo Linux Mint en bas à gauche *(1)* puis cliquez sur le logo **Cadenas**. *(2)*

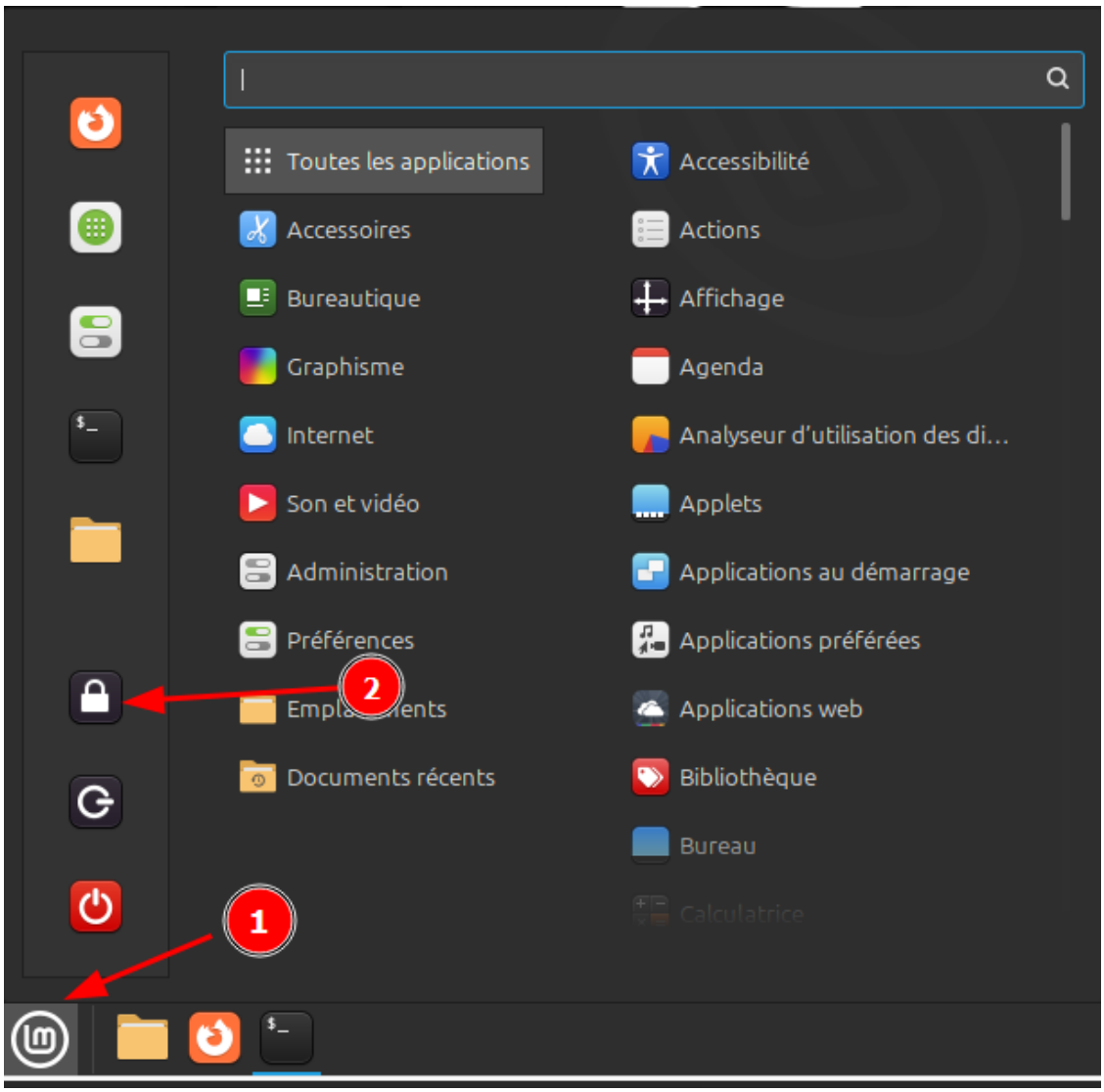


image.png

Pour finir cliquez sur **Se déconnecter** *(1)*

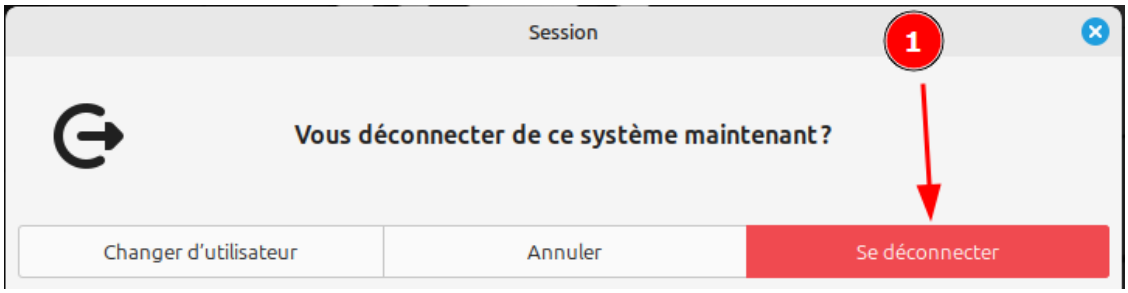


image.png

2. Revenez à l'écran de connexion.

image.png

3. Lors de la reconnexion, entrez le mot de passe actuel de l'utilisateur créé précédemment

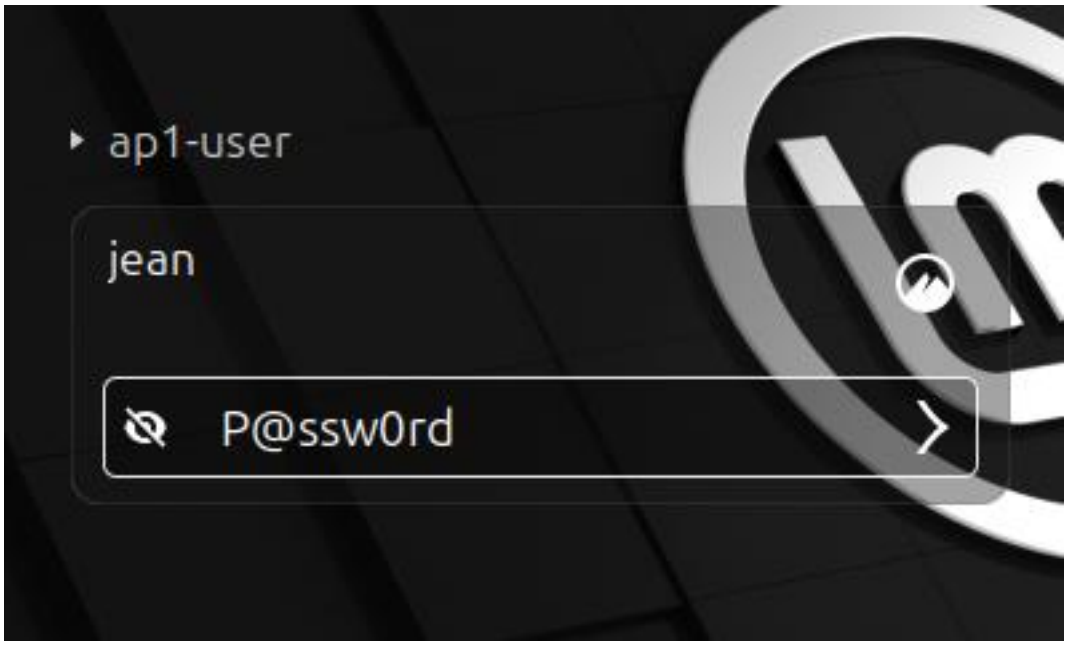


image.png

4. Saisissez d'abord l'ancien mot de passe, puis le nouveau mot de passe en suivant les règles de complexité définies.

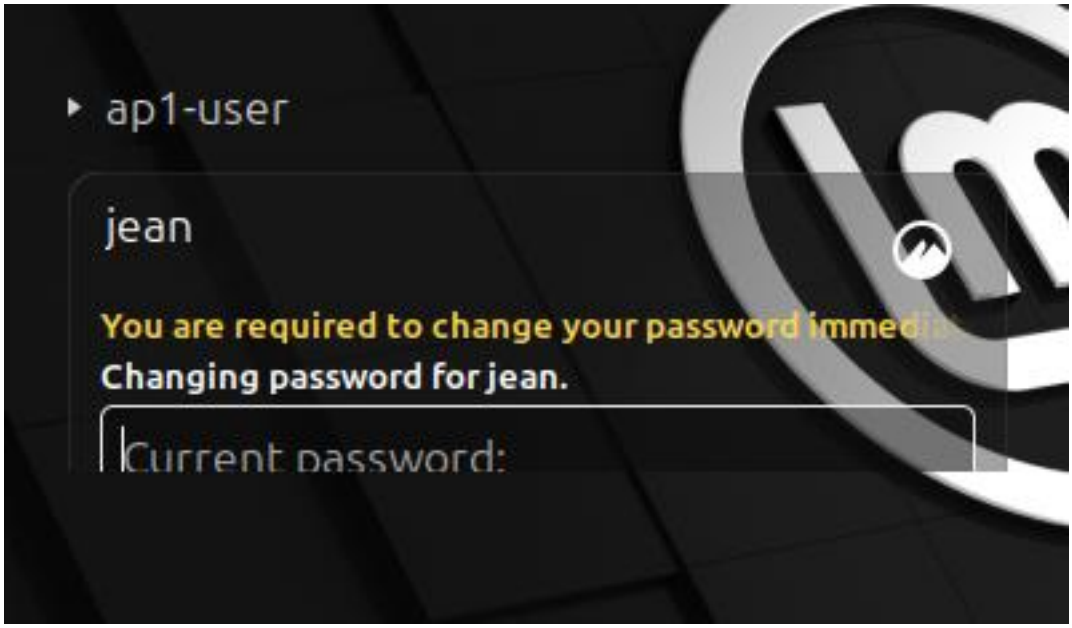


image.png

5. Essayez d'entrer un mot de passe non conforme (ex. : `azertyuiop`) pour vérifier que le système le refuse.

image.png

6. Testez ensuite avec un mot de passe conforme (ex. : `Ap1linuxunix!`), et assurez-vous qu'il est accepté.

---

3. Pourquoi ces étapes sont importantes ?

- **Renforcement de la sécurité** : Imposer des règles strictes pour les mots de passe et limiter leur réutilisation protège contre les accès non autorisés.
- **Gestion utilisateur contrôlée** : Créer des utilisateurs standards avec expiration des mots de passe réduit les risques liés à l'usage d'accès administrateurs non sécurisés.
- **Conformité aux bonnes pratiques** : Forcer la modification initiale des mots de passe et leur renouvellement périodique garantit un système aligné sur les standards de sécurité.

11. Restriction d'Acces aux Journaux Système

0. Introduction

La sécurité des journaux système est une composante essentielle de l'administration des systèmes Linux. Ces journaux contiennent des informations sensibles sur les événements du

système, les activités des utilisateurs, et les accès aux ressources. Une mauvaise gestion ou une exposition non contrôlée de ces fichiers peut conduire à des failles de sécurité exploitables par des attaquants. Ce guide explique étape par étape comment restreindre l'accès aux journaux système, configurer des permissions par défaut, surveiller les accès, et automatiser la gestion des journaux pour renforcer la sécurité de votre système.

---

1. Restreindre les permissions des journaux

1. Appliquer des permissions générales :

   Avant de restreindre les permissions, vérifiez leur état actuel :

   ```
   ls -ld /var/log/*
   ```

   ```
   ap1-user@ap1user:~$ ls -ld /var/log/*
   ```

   image.png

   Restreindre les permissions globales :

   ```
   sudo chmod -R go-rwx /var/log/*
   ```

   ```
   ap1-linux@ap1linux:~$ sudo chmod -R go-rwx /var/log/*
   [sudo] Mot de passe de ap1-linux :
   ```

   11%20Restriction%20d'Acces%20aux%20Journaux%20Systeme%20182dbb723a2881 2a94ccfdacf79b16d8/image%201.png

   Explication :

   - g : groupe.
   - o : autres (non propriétaires).
   - rwx : retire les droits de lecture, écriture et exécution.

2. Attribuer un propriétaire et un groupe spécifiques :

   Vérifiez les groupes disponibles :

   ```
   groups
   ```

   ```
   ap1-linux@ap1linux:~$ groups
   ap1-linux adm cdrom sudo dip plugdev users lpadmin sambashare
   ```

   11%20Restriction%20d'Acces%20aux%20Journaux%20Systeme%20182dbb723a2881 2a94ccfdacf79b16d8/image%202.png

   Assurez-vous que `root` est le propriétaire principal et que le groupe associé est `adm` :

```
sudo chown -R root:adm /var/log/*
```

```
ap1-linux@ap1linux:~$ sudo chown -R root:adm /var/log/*
[sudo] Mot de passe de ap1-linux :
```

11%20Restriction%20d'Acces%20aux%20Journaux%20Systeme%20182dbb723a28812a94ccfdacf79b16d8/image%203.png

Cette commande :

- Définit `root` comme propriétaire.
- Définit `adm` comme groupe associé pour tous les fichiers et sous-répertoires dans `/var/log`.

3. Vérifier les permissions après modification :

```
ls -l /var/log/
```

```
ap1-linux@ap1linux:~$ ls -l /var/log
total 4548
-rw-------  1 root adm       0 déc.   7 17:44 alternatives.log
-rw-------  1 root adm    6819 nov.  25 22:13 alternatives.log.1
drwx------  2 root adm    4096 déc.   7 18:55 apt
-rw-------  1 root adm   22517 déc.   7 20:46 auth.log
-rw-------  1 root adm   74598 déc.   7 17:44 auth.log.1
-rw-------  1 root adm    3084 déc.   7 17:44 boot.log
-rw-------  1 root adm   26372 déc.   7 17:44 boot.log.1
-rw-------  1 root adm   20276 nov.  26 20:08 boot.log.2
-rw-------  1 root adm       0 juil. 21 14:46 bootstrap.log
```

11%20Restriction%20d'Acces%20aux%20Journaux%20Systeme%20182dbb723a28812a94ccfdacf79b16d8/image%204.png

---

3. Configurer des permissions par défaut dans `rsyslog`

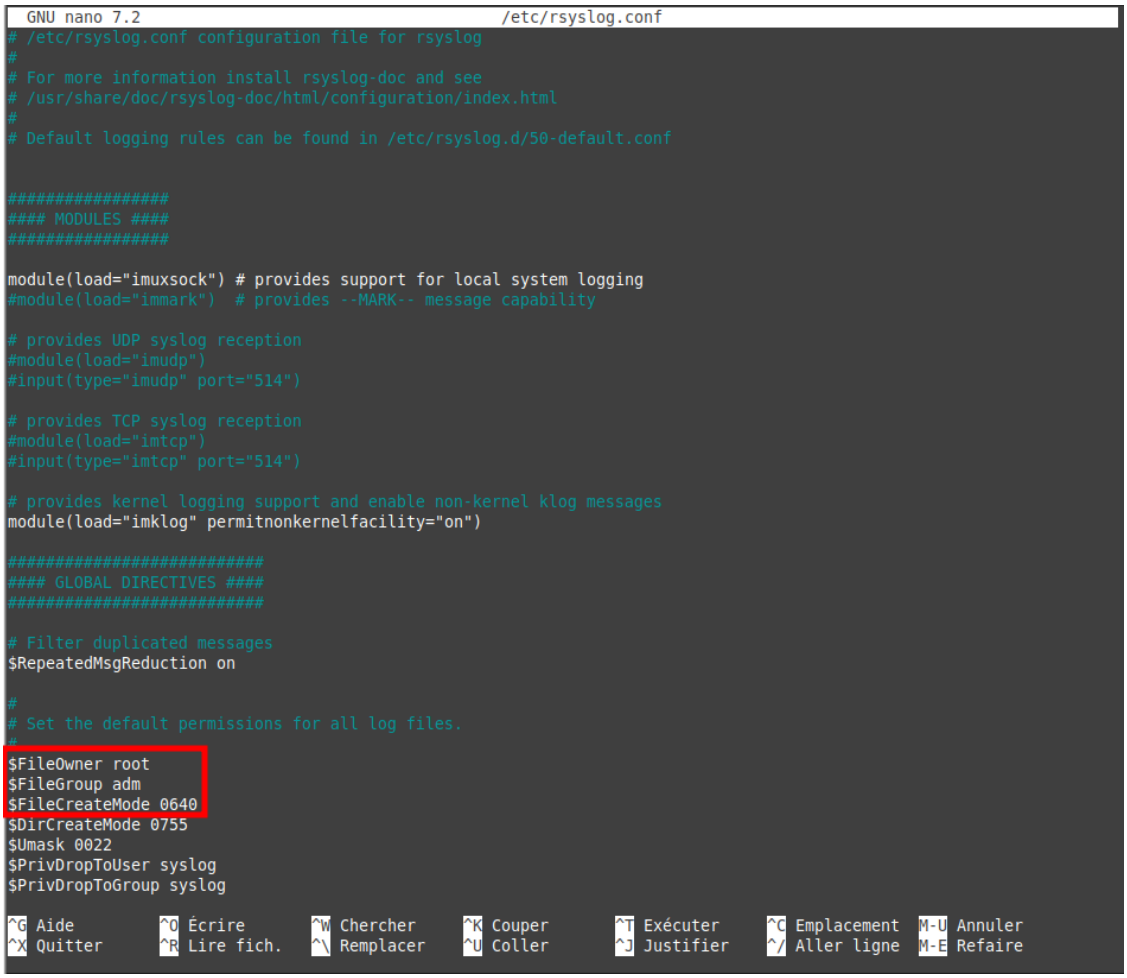
Pour s'assurer que les nouveaux fichiers journaux créés ont les permissions correctes, configurez les options dans `/etc/rsyslog.conf` ou `/etc/rsyslog.d/*.conf`.

1. Éditer le fichier principal de configuration `rsyslog` :

```
sudo nano /etc/rsyslog.conf
```

2. Ajouter ou modifier les lignes suivantes pour définir les permissions par défaut :

```
$FileOwner root
$FileGroup adm
$FileCreateMode 0640
```



11%20Restriction%20d'Acces%20aux%20Journaux%20Systeme%20182dbb723a2881 2a94ccfdacf79b16d8/image%205.png

Explication :

- **`$FileOwner root`** : Le propriétaire des fichiers journaux sera `root`.
- **`$FileGroup adm`** : Le groupe associé sera `adm`.
- **`$FileCreateMode 0640`** :
  - 6 : Lecture et écriture pour le propriétaire.
  - 4 : Lecture pour les groupes.
  - 0 : Aucun accès pour "autres".

3. Vérifier la syntaxe avant de redémarrer `rsyslog` :

```
sudo rsyslogd -N1
```

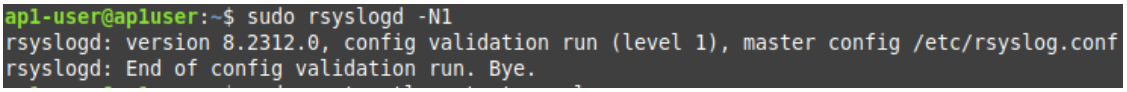
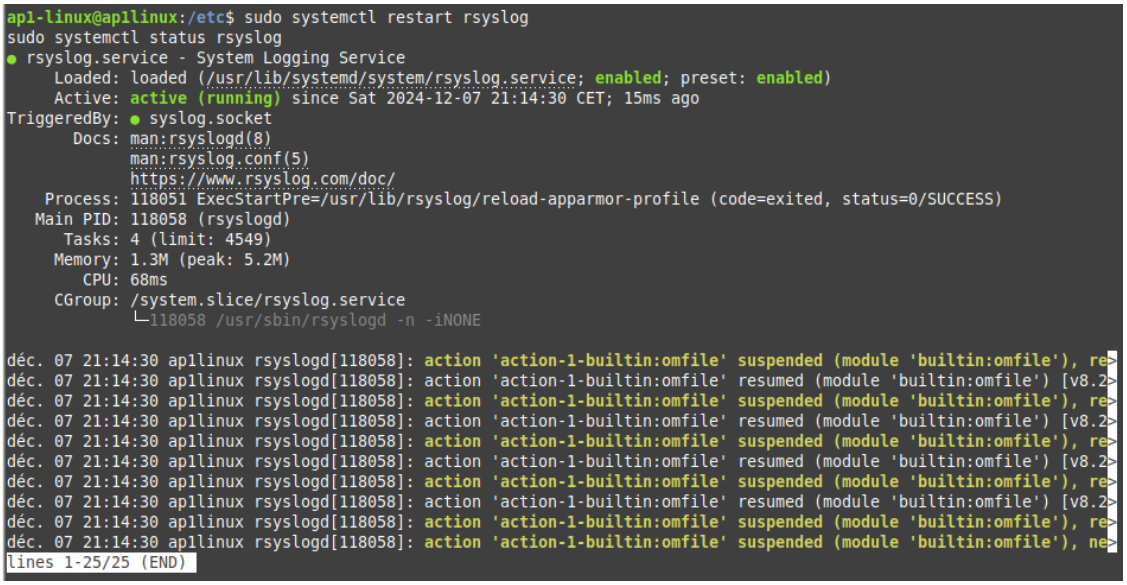


image.png

Cette commande permet de valider la syntaxe des fichiers de configuration avant de redémarrer le service. Si aucune erreur n'est signalée, redémarrez le service :

```
sudo systemctl restart rsyslog
sudo systemctl status rsyslog
```



11%20Restriction%20d'Acces%20aux%20Journaux%20Systeme%20182dbb723a28812a94ccfdacf79b16d8/image%207.png

---

4. Surveiller les accès aux journaux

Configurez l'audit système pour surveiller les tentatives d'accès non autorisées à des fichiers journaux critiques comme `/var/log/auth.log`.

1. Ajouter une règle d'audit pour `/var/log/auth.log` :

   Ajoutez une règle dans `/etc/audit/rules.d/audit.rules` pour qu'elle soit persistante :

   ```
   sudo gedit /etc/audit/rules.d/audit.rules
   ```

   Ajouter les lignes suivantes :

   ```
   ## Surveiller les accès aux journaux
   -w /var/log/auth.log -p wa -k auth_access
   ```

```
ap1-user@ap1user:~$ sudo gedit /etc/audit/rules.d/audit.rules
```

Ouvrir — *audit.rules — /etc/audit/rules.d

```
1  ## Supprimer toutes les règles existantes
2  -D
3
4  ## Taille des tampons
5  -b 8192
6  # Ajustez cette valeur en fonction des besoins spécifiques.
7
8  ## Définitions des règles
9  -w /etc/passwd -p wa -k passwd_changes
10 -w /etc/shadow -p wa -k shadow_access
11 -a always,exit -F arch=b64 -S setuid -S setgid -k privilege_changes
12 -w /var/log/auth.log -p wa -k auth_changes
13 -w /boot/ -p wa -k boot_changes
14
15 ## Suivi des connexions SSH
16 -w /etc/ssh/sshd_config -p wa -k ssh_config_changes
17 -w /var/log/auth.log -p wa -k ssh_logins
18
19 ## Surveiller les accès aux journaux
20 -w /var/log/auth.log -p wa -k auth_access
```

image.png

Explication :

- **w** : Surveille le fichier spécifié.
- **p wa** : Enregistre les tentatives d'écriture et d'attributs.
- **k auth_access** : Attribue un mot-clé pour identifier ces événements dans les logs d'audit.

Appliquez les nouvelles règles :

```
sudo augenrules --Load
```

```
ap1-user@ap1user:~$ sudo augenrules --load
No rules
enabled 1
failure 1
pid 4761
rate_limit 0
backlog_limit 8192
lost 50
backlog 3
backlog_wait_time 60000
backlog_wait_time_actual 0
```

image.png

2. Redémarrer le service `auditd` :

```
sudo systemctl restart auditd
sudo systemctl status auditd
```

```
ap1-linux@ap1linux:/etc$ sudo systemctl restart auditd
sudo systemctl status auditd
● auditd.service - Security Auditing Service
     Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset: enabled)
     Active: active (running) since Sat 2024-12-07 21:37:10 CET; 15ms ago
       Docs: man:auditd(8)
             https://github.com/linux-audit/audit-documentation
    Process: 118827 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
    Process: 118834 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/SUCCESS)
   Main PID: 118830 (auditd)
      Tasks: 2 (limit: 4549)
     Memory: 516.0K (peak: 2.3M)
        CPU: 26ms
     CGroup: /system.slice/auditd.service
             └─118830 /sbin/auditd

déc. 07 21:37:10 ap1linux augenrules[118845]: enabled 1
déc. 07 21:37:10 ap1linux augenrules[118845]: failure 1
déc. 07 21:37:10 ap1linux augenrules[118845]: pid 118830
déc. 07 21:37:10 ap1linux augenrules[118845]: rate_limit 0
déc. 07 21:37:10 ap1linux augenrules[118845]: backlog_limit 8192
déc. 07 21:37:10 ap1linux augenrules[118845]: lost 0
déc. 07 21:37:10 ap1linux augenrules[118845]: backlog 0
déc. 07 21:37:10 ap1linux augenrules[118845]: backlog_wait_time 60000
déc. 07 21:37:10 ap1linux augenrules[118845]: backlog_wait_time_actual 0
déc. 07 21:37:10 ap1linux systemd[1]: Started auditd.service - Security Auditing Service.
```

11%20Restriction%20d'Acces%20aux%20Journaux%20Systeme%20182dbb723a2881 2a94ccfdacf79b16d8/image%2010.png

3. Analyser les journaux d'audit pour détecter les accès :

   Pour vérifier les accès au fichier `/var/log/auth.log`, utilisez :

```
sudo ausearch -k auth_access
```

```
ap1-user@ap1user:~$ sudo ausearch -k auth_access
----
time->Sun Jan 19 14:18:31 2025
type=PROCTITLE msg=audit(1737292711.182:2349): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61
756469742E72756C6573
type=PATH msg=audit(1737292711.182:2349): item=0 name="/var/log/" inode=743570 dev=fc:01 mode=040775 ouid=0 ogid=102
rdev=00:00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1737292711.182:2349): cwd="/home/ap1-user"
type=SOCKADDR msg=audit(1737292711.182:2349): saddr=100000000000000000000000
type=SYSCALL msg=audit(1737292711.182:2349): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7ffd1e444f00 a2=4
3c a3=0 items=1 ppid=118526 pid=118539 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses
=2 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1737292711.182:2349): auid=1000 ses=2 subj=unconfined op=add_rule key="auth_access" list
=4 res=1
----
time->Sun Jan 19 14:19:00 2025
type=PROCTITLE msg=audit(1737292740.325:2378): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61
756469742E72756C6573
type=SOCKADDR msg=audit(1737292740.325:2378): saddr=100000000000000000000000
type=SYSCALL msg=audit(1737292740.325:2378): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7ffc134de2d0 a2=4
3c a3=0 items=0 ppid=118556 pid=118567 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(n
one) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1737292740.325:2378): auid=4294967295 ses=4294967295 subj=unconfined op=remove_rule key=
"auth_access" list=4 res=1
----
time->Sun Jan 19 14:19:00 2025
type=PROCTITLE msg=audit(1737292740.326:2387): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61
756469742E72756C6573
type=PATH msg=audit(1737292740.326:2387): item=0 name="/var/log/" inode=743570 dev=fc:01 mode=040775 ouid=0 ogid=102
rdev=00:00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1737292740.326:2387): cwd="/"
type=SOCKADDR msg=audit(1737292740.326:2387): saddr=100000000000000000000000
type=SYSCALL msg=audit(1737292740.326:2387): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7ffc134e0770 a2=4
3c a3=0 items=1 ppid=118556 pid=118567 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(n
one) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1737292740.326:2387): auid=4294967295 ses=4294967295 subj=unconfined op=add_rule key="au
th_access" list=4 res=1
```

image.png

---

5. Pourquoi ces étapes sont importantes ?

- **Protection des données sensibles** : Restreindre l'accès aux journaux empêche les utilisateurs non autorisés d'obtenir des informations critiques sur le système.
- **Conformité et traçabilité** : Configurer des permissions par défaut et surveiller les accès garantit une gestion sécurisée des fichiers journaux.
- **Détection proactive des intrusions** : L'audit des accès non autorisés aide à identifier et prévenir les activités malveillantes.

12. Restriction des Droits sur les Fichiers Sensibles

0. Introduction

Les fichiers sensibles sur un système Linux jouent un rôle crucial dans la stabilité et la sécurité de l'ensemble du système. Leur exposition ou modification non autorisée peut entraîner des failles exploitables, voire la compromission totale de l'environnement. Ce

guide présente les meilleures pratiques pour identifier et restreindre l'accès à ces fichiers, assurant ainsi un haut niveau de protection contre les menaces potentielles.

---

1. Identification des fichiers sensibles

Les fichiers sensibles incluent :

- **Fichiers systèmes critiques** : `/etc/passwd` et `/etc/shadow`.
- **Clés privées** : Fichiers dans `/etc/ssl/private/`.
- **Journaux système** : Contenus dans `/var/log/`.

Vérifiez les permissions actuelles :

```
sudo ls -l /etc/passwd /etc/shadow
sudo ls -l /etc/ssl/private/
sudo ls -l /var/log/
```

Résultats attendus :

- `/etc/passwd` doit être lisible par tous (`rw-r--r--`), mais modifiable uniquement par `root`.
- `/etc/shadow` doit être accessible uniquement par `root` (`rw-r-----`).
- Les fichiers dans `/etc/ssl/private/` doivent être accessibles uniquement par `root`.

```
ap1-linux@ap1linux:~$ sudo ls -l /etc/passwd /etc/shadow
sudo ls -l /etc/ssl/private/
sudo ls -l /var/log/
-rw-r--r-- 1 root root   2891 déc.   8 16:20 /etc/passwd
-rw-r----- 1 root shadow 1297 déc.   7 18:16 /etc/shadow
total 4
-rw-r----- 1 root ssl-cert 1708 nov.  24 15:16 ssl-cert-snakeoil.key
total 4044
```

image.png

---

2. Modification des permissions des fichiers sensibles

a. Fichiers systèmes critiques :

- Assurez-vous que les permissions sont correctement configurées pour empêcher les accès non autorisés.

Commandes :

```
sudo chmod 644 /etc/passwd
sudo chmod 640 /etc/shadow
```

```
ap1-user@ap1user:~$ sudo chmod 644 /etc/passwd
sudo chmod 640 /etc/shadow
```

image.png

Explications :

- `644` pour `/etc/passwd` : Lecture pour tous, écriture uniquement pour `root`.
- `640` pour `/etc/shadow` : Lecture et écriture pour `root`, aucune permission pour d'autres utilisateurs.

---

b. Clés privées :

- Les fichiers de `/etc/ssl/private/` doivent être protégés contre toute lecture ou écriture non autorisée.

Commandes :

```
sudo chmod 600 /etc/ssl/private/ssl-cert-snakeoil.key
sudo chown root:root /etc/ssl/private/ssl-cert-snakeoil.key
```

```
ap1-user@ap1user:~$ sudo chmod 600 /etc/ssl/private/ssl-cert-snakeoil.key
sudo chown root:root /etc/ssl/private/ssl-cert-snakeoil.key
```

image.png

Explications :

- `600` : Lecture et écriture uniquement pour `root`.
- `root:root` : Le propriétaire et le groupe des fichiers sont définis comme `root`.

---

c. Journaux système :

- Les journaux contiennent des informations sensibles sur l'activité du système et doivent être protégés.

Commandes :

```
sudo chmod -R go-rwx /var/log/*
sudo chown -R root:adm /var/log/
```

```
ap1-user@ap1user:~$ sudo chmod -R go-rwx /var/log/*
sudo chown -R root:adm /var/log/
```

image.png

Explications :

- `go-rwx` : Supprime toutes les permissions pour les groupes et autres utilisateurs.
- `root:adm` : Attribue les fichiers à `root` et au groupe `adm`, permettant un accès contrôlé.

---

3. Vérifications finales

Commandes :

- Vérifiez les permissions des fichiers sensibles :

```
sudo ls -l /etc/passwd /etc/shadow
sudo ls -l /etc/ssl/private/
sudo ls -l /var/log/
```

```
ap1-user@ap1user:~$ sudo ls -l /etc/passwd /etc/shadow
sudo ls -l /etc/ssl/private/
sudo ls -l /var/log/
-rw-r--r-- 1 root root   2980 janv. 19 03:14 /etc/passwd
-rw-r----- 1 root shadow 1410 janv. 19 03:32 /etc/shadow
total 4
-rw------- 1 root root 1704 janv. 18 22:22 ssl-cert-snakeoil.key
total 3168
-rw-------  1 root adm   7175 janv. 18 23:29 alternatives.log
drwx------  2 root adm   4096 janv. 19 03:07 apt
drwx------  2 root adm   4096 janv. 19 00:08 audit
drwx------  2 root adm   4096 janv. 19 00:45 audit_reports
-rw-------  1 root adm  93230 janv. 19 14:17 auth.log
-rw-------  1 root adm  19549 janv. 19 00:17 boot.log
-rw-------  1 root adm      0 juil. 21 14:46 bootstrap.log
-rw-------  1 root adm    768 janv. 19 03:34 btmp
drwx------  2 root adm   4096 janv. 19 01:43 clamav
drwx------  2 root adm   4096 janv. 18 23:29 cups
drwx------  2 root adm   4096 juil. 21 14:46 cups-browsed
-rw-------  1 root adm 153280 janv. 19 00:17 dmesg
-rw-------  1 root adm 150729 janv. 18 22:33 dmesg.0
-rw-------  1 root adm 280592 janv. 19 03:07 dpkg.log
```

image.png

- Simulez un accès non autorisé avec un utilisateur standard :

```
sudo -u nobody cat /etc/shadow
sudo -u nobody ls /etc/ssl/private/
```

Résultat attendu :

- Les commandes doivent afficher des messages d'erreur indiquant un accès refusé.

```
ap1-linux@ap1linux:/$ sudo -u nobody cat /etc/shadow
sudo -u nobody ls /etc/ssl/private/
cat: /etc/shadow: Permission non accordée
ls: impossible d'ouvrir le répertoire '/etc/ssl/private/': Permission non accordée
```

image.png

---

4. Pourquoi ces étapes sont importantes ?

- **Protection des données critiques** : Restreindre l'accès aux fichiers sensibles comme `/etc/shadow` ou les clés privées empêche les modifications ou consultations non autorisées.
- **Réduction des risques de compromission** : En sécurisant les journaux et les permissions système, vous limitez les informations exploitables par des attaquants.
- **Conformité aux bonnes pratiques** : Garantir des permissions strictes répond aux exigences de sécurité pour les environnements sensibles.

13. Deploiement de logiciel

0. Introduction

Ce guide explique comment automatiser le déploiement de plusieurs logiciels essentiels sur un système Linux. Les instructions incluent l'écriture d'un script bash, son exécution et des explications pour ajouter des outils supplémentaires si nécessaire.

---

1. Écriture du Script

1. Créez un fichier bash pour regrouper les commandes d'installation :

```
cd Bureau/
sudo gedit Installations_Logiciels.sh
```

```
ap1-user@ap1user:~$ cd Bureau/
sudo gedit Installations_Logiciels.sh
```

image.png

2. Collez le contenu suivant dans le fichier :

```
#!/bin/bash

# Définir les couleurs pour un affichage clair
bold=$(tput bold)
green=$(tput setaf 2)
yellow=$(tput setaf 3)
red=$(tput setaf 1)
reset=$(tput sgr0)

echo "${bold}${green}=== Début de l'installation des logiciels requis ===${reset}"

# Mise à jour et mise à niveau du système
echo "${bold}${yellow}Mise à jour des dépôts et mise à niveau des paquets en cours...${reset}"
sudo apt update -y > /dev/null 2>&1
sudo apt upgrade -y > /dev/null 2>&1
echo "${bold}${green}Mise à jour et mise à niveau terminées avec succès.${reset}"

# Étapes préalable avant installation de OnlyOffice
echo "${bold}${yellow}Étape 1 : Installation de OnlyOffice en cours...${reset}"
mkdir -p -m 700 ~/.gnupg > /dev/null 2>&1
echo "${bold}${green}Dossier GNUPG sécurisé créé avec succès.${reset}"
gpg --no-default-keyring --keyring gnupg-ring:/tmp/onlyoffice.gpg --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys CB2DE8E5 > /dev/null 2>&1
echo "${bold}${green}Clé GPG de OnlyOffice récupérée avec succès.${reset}"
chmod 644 /tmp/onlyoffice.gpg > /dev/null 2>&1
sudo chown root:root /tmp/onlyoffice.gpg > /dev/null 2>&1
sudo mv /tmp/onlyoffice.gpg /usr/share/keyrings/onlyoffice.gpg > /dev/null 2>&1
echo "${bold}${green}Clé GPG déplacée et sécurisée dans le répertoire système.${reset}"

echo "${bold}${yellow}Ajout du dépôt OnlyOffice à la liste des sources...${reset}"
echo 'deb [signed-by=/usr/share/keyrings/onlyoffice.gpg] https://download.onlyoffice.com/repo/debian squeeze main' | sudo tee /etc/apt/sources.list.d/onlyoffice.list > /dev/null
echo "${bold}${yellow}Mise à jour du cache des paquets...${reset}"
sudo apt-get update > /dev/null 2>&1

# Pré-accepter l'EULA pour éviter l'interruption interactive
echo "${bold}${yellow}Pré-acceptation des termes EULA...${reset}"
echo "ttf-mscorefonts-installer msttcorefonts/accepted-mscorefonts-eula select true" | sudo debconf-set-selections

# Installation de OnlyOffice
```

```
echo "${bold}${yellow}Installation du logiciel OnlyOffice Desktop Edi
tors...${reset}"
sudo apt-get install -y onlyoffice-desktopeditors > /dev/null
echo "${bold}${green}Installation de OnlyOffice terminée avec succès.
${reset}"

# Ajouter un raccourci sur le bureau
echo "${bold}${yellow}Ajout d'un raccourci OnlyOffice sur le bureau..
.${reset}"
cp /usr/share/applications/onlyoffice-desktopeditors.desktop ~/Bureau
/ > /dev/null 2>&1
chmod +x ~/Bureau/onlyoffice-desktopeditors.desktop > /dev/null 2>&1
echo "${bold}${green}Raccourci ajouté sur le bureau avec succès.${res
et}"

# Installation de VLC
echo "${bold}${yellow}Étape 2 : Installation de VLC en cours...${rese
t}"
sudo apt install -y vlc > /dev/null 2>&1
echo "${bold}${green}Installation de VLC terminée avec succès.${reset
}"

# Installation de Okular
echo "${bold}${yellow}Étape 3 : Installation de Okular en cours...${r
eset}"
sudo apt install -y okular > /dev/null 2>&1
echo "${bold}${green}Installation de Okular terminée avec succès.${re
set}"

# Vérification des installations
echo "${bold}${yellow}Vérification des logiciels installés...${reset}
"

# Fonction de vérification
check_installation() {
    if command -v $1 &> /dev/null; then
        echo "${bold}${green}$1 est correctement installé.${reset}"
    else
        echo "${bold}${red}$1 n'est pas installé ou ne fonctionne pas
correctement.${reset}"
    fi
}

check_installation "onlyoffice-desktopeditors"
check_installation "vlc"
check_installation "okular"

# Suppression automatique du script
script_path=~/Bureau/Installations_Logiciels.sh
if [ -f "$script_path" ]; then
    echo "${bold}${yellow}Suppression du fichier $script_path...${res
et}"
```

```
    rm -f "$script_path"
    echo "${bold}${green}Le fichier $script_path a été supprimé avec succès.${reset}"
else
    echo "${bold}${red}Le fichier $script_path est introuvable. Rien à supprimer.${reset}"
fi

# Installation terminée.
echo "${bold}${green}=== Toutes les installations sont terminées avec succès ! ===${reset}"
```

3. Rendez le fichier exécutable :

```
sudo chmod +x Installations_Logiciels.sh
```

```
ap1-user@ap1user:~/Bureau$ sudo chmod +x Installations_Logiciels.sh
```

image.png

4. Exécutez le script :

```
./Installations_Logiciels.sh
```

```
=== Début de l'installation des logiciels requis ===
Mise à jour des dépôts et mise à niveau des paquets en cours...
Mise à jour et mise à niveau terminées avec succès.
Étape 1 : Installation de OnlyOffice en cours...
Dossier GNUPG sécurisé créé avec succès.
Clé GPG de OnlyOffice récupérée avec succès.
Clé GPG déplacée et sécurisée dans le répertoire système.
Ajout du dépôt OnlyOffice à la liste des sources...
Mise à jour du cache des paquets...
Pré-acceptation des termes EULA...
Installation du logiciel OnlyOffice Desktop Editors...
Installation de OnlyOffice terminée avec succès.
Ajout d'un raccourci OnlyOffice sur le bureau...
Raccourci ajouté sur le bureau avec succès.
Étape 2 : Installation de VLC en cours...
Installation de VLC terminée avec succès.
Étape 3 : Installation de Okular en cours...
Installation de Okular terminée avec succès.
Vérification des logiciels installés...
onlyoffice-desktopeditors est correctement installé.
vlc est correctement installé.
okular est correctement installé.
Suppression du fichier /home/ap1-user/Bureau/Installations_Logiciels.sh...
Le fichier /home/ap1-user/Bureau/Installations_Logiciels.sh a été supprimé avec succès.
=== Toutes les installations sont terminées avec succès ! ===
```

image.png

---

2. Pourquoi ces étapes sont importantes ?

- **Automatisation efficace** : Un script centralise l'installation de plusieurs logiciels, économisant du temps et minimisant les erreurs manuelles.
- **Conformité et contrôle** : La configuration des dépôts et des clés garantit une installation sécurisée et fiable des logiciels nécessaires.
- **Gestion simplifiée** : Vérifier les installations et nettoyer les fichiers inutiles optimise la gestion du système après le déploiement.

14. Masterisation du poste Linux

0. Introduction

La masterisation d'un poste Windows 10 consiste à créer une image de sauvegarde d'un système configuré, que l'on peut ensuite restaurer ou cloner sur d'autres machines. Cette procédure est essentielle pour garantir une installation cohérente et standardisée des postes de travail, tout en facilitant la gestion des systèmes en cas de panne ou de besoin de déploiement rapide. L'outil Rescuezilla est utilisé dans ce guide pour sa simplicité d'utilisation et ses capacités à gérer les sauvegardes et restaurations. Une configuration précise et documentée est nécessaire pour minimiser les risques d'erreurs et assurer une continuité dans la gestion des systèmes

---

1. Préalables

- Un support de stockage pour la sauvegarde (USB, SSD, HDD, etc.).
- Un système à sauvegarder et à cloner.

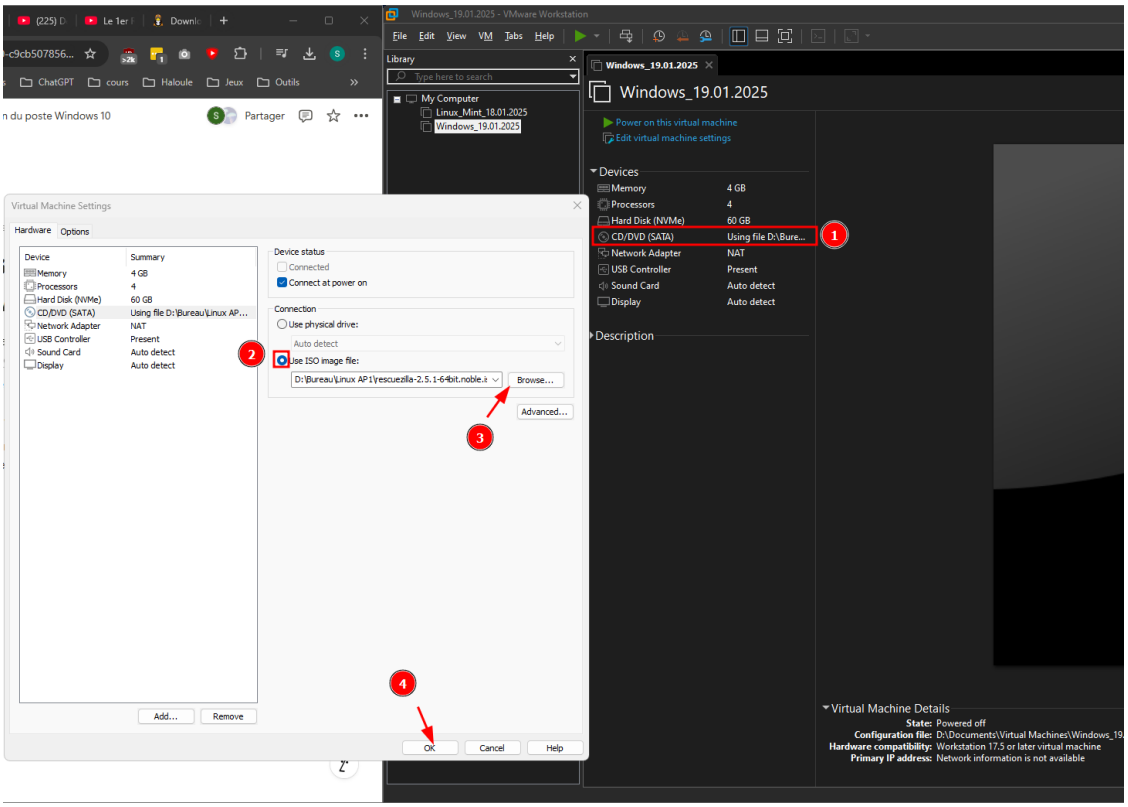
Rendez-vous sur ce site pour télécharger l'ISO de Rescuezilla : [Rescuezilla - Téléchargement]

---

2. Configuration initiale

1. **Sélection de l'ISO dans VMware**

   Sélectionnez votre VM sur VMware, cliquez sur CD/DVD (SATA). Cochez « Use ISO image file », puis cliquez sur le bouton `Browse...` et sélectionnez `rescuezilla.iso` que vous venez de télécharger. Cliquez ensuite sur OK.

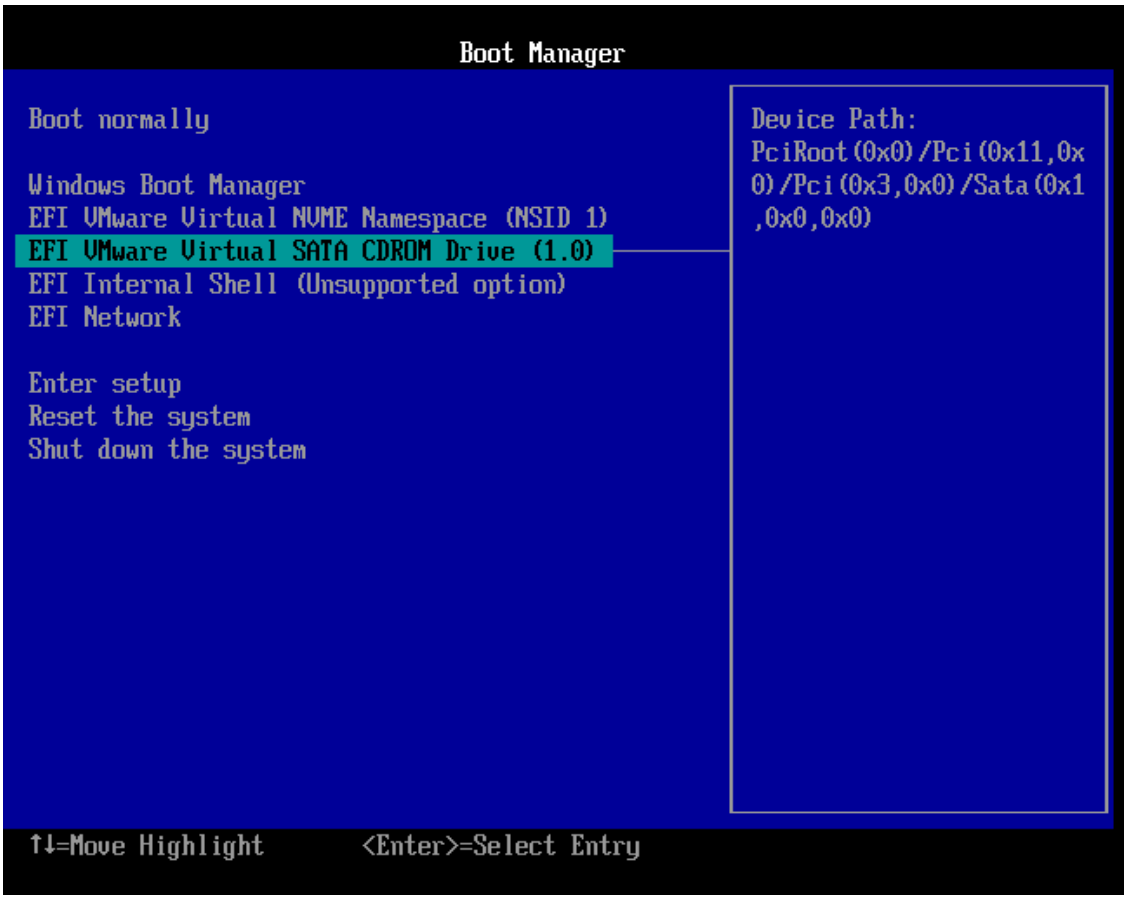


14%20Masterisation%20du%20poste%20Linux%20182dbb723a2881a19dbedb5f8020d02e/image.png

2. **Démarrage de la VM et accès au BIOS**

   Lancez la VM et, lorsque la fenêtre se lance, cliquez sur la touche F2 de votre clavier pour entrer dans l'UEFI.

   Une fois dans le BIOS, descendez avec les flèches directionnelles jusqu'à sélectionner `EFI VMware Virtual SATA CDROM Drive (1.0)` et appuyez sur `Entrée`.



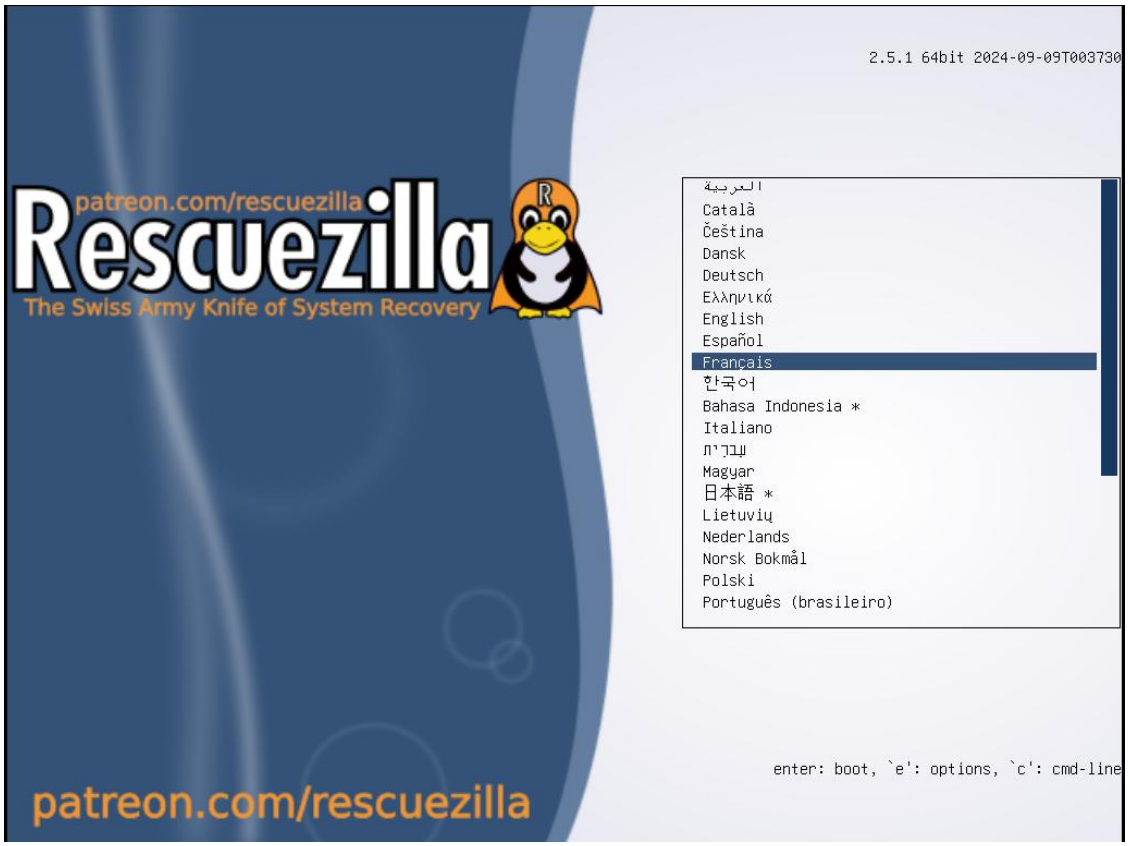
14%20Masterisation%20du%20poste%20Linux%20182dbb723a2881a19dbedb5f8020d02e/image%201.png

---

3. Utilisation de Rescuezilla

1. **Sélection de la langue**

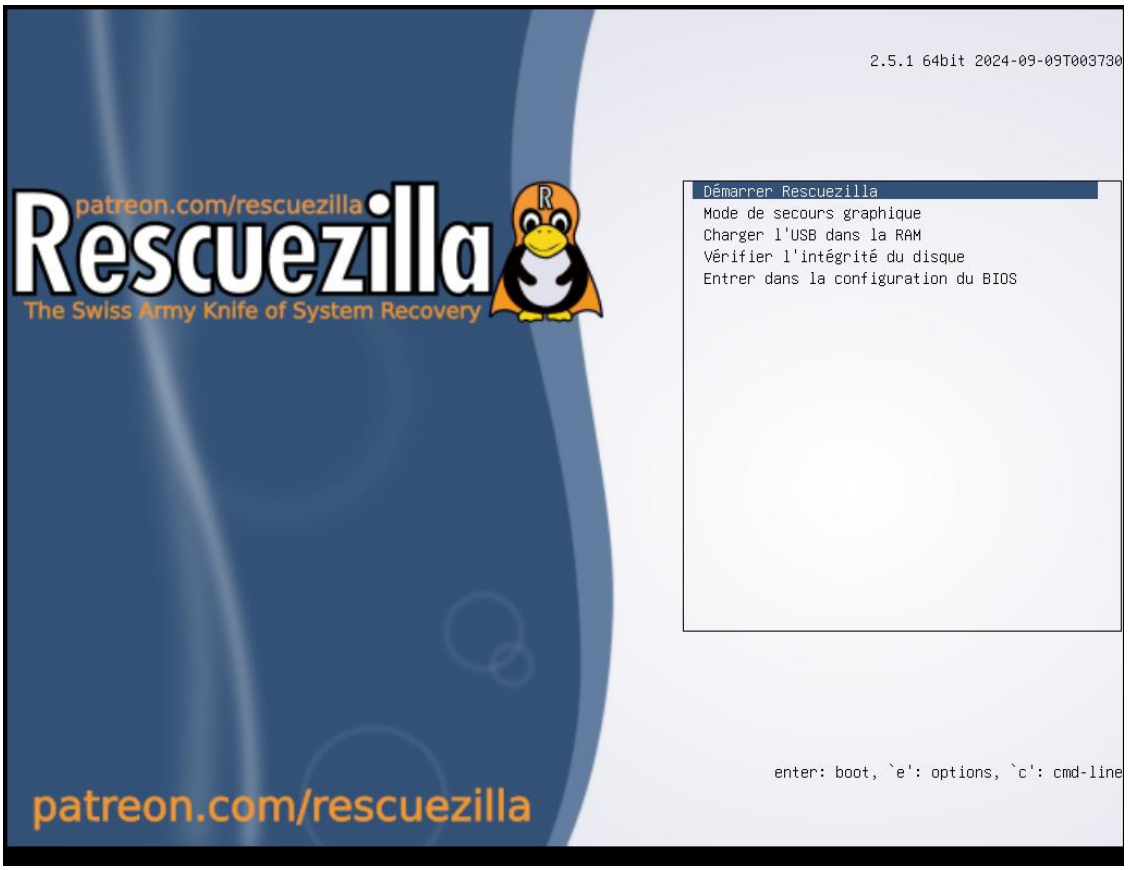
   Une fois dans Rescuezilla, sélectionnez votre langue en utilisant les flèches puis appuyez sur `Entrée`. Pour ce guide, nous choisirons le français.



14%20Masterisation%20du%20poste%20Linux%20182dbb723a2881a19dbedb5f8020d02e/image%202.png

2. **Démarrage de Rescuezilla**

   Sélectionnez « Démarrer Rescuezilla » en utilisant les flèches puis appuyez sur `Entrée`.



14%20Masterisation%20du%20poste%20Linux%20182dbb723a2881a19dbedb5f8020d02e/image%203.png

---

4. Sauvegarde du système

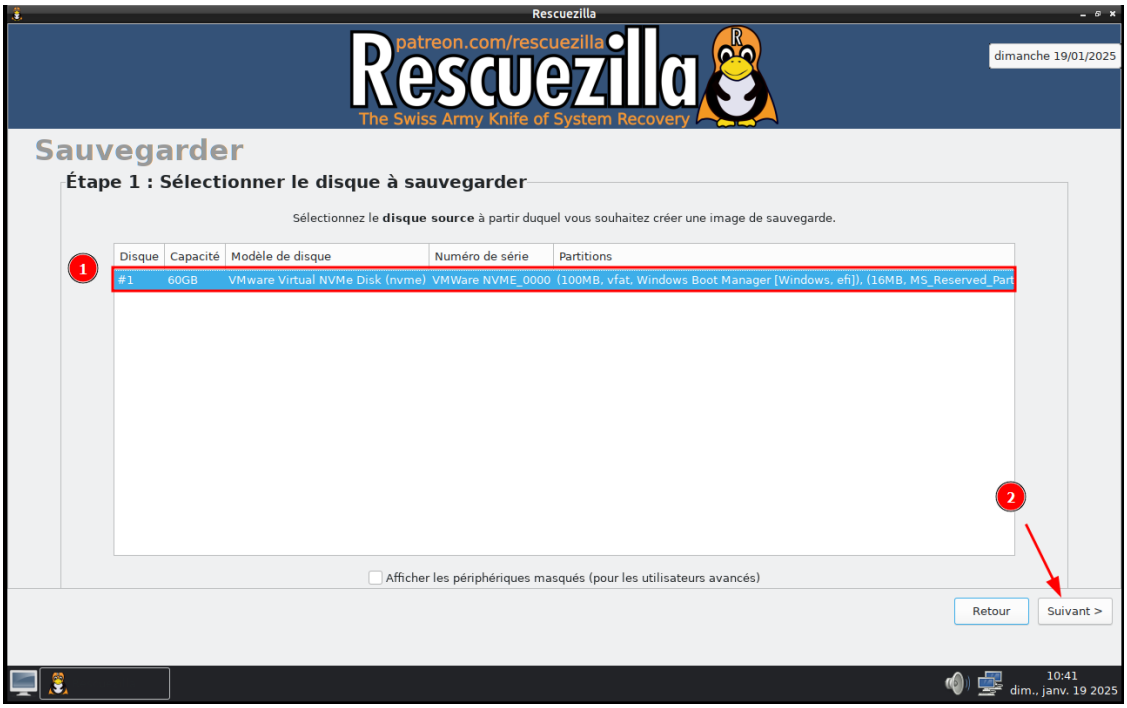
1. **Lancement de la sauvegarde**

   Cliquez sur Sauvegarder.

14%20Masterisation%20du%20poste%20Linux%20182dbb723a2881a19dbedb5f8020d02e/image%204.png

2. **Sélection du disque**

Sélectionnez le disque à sauvegarder puis cliquez sur `Suivant`.

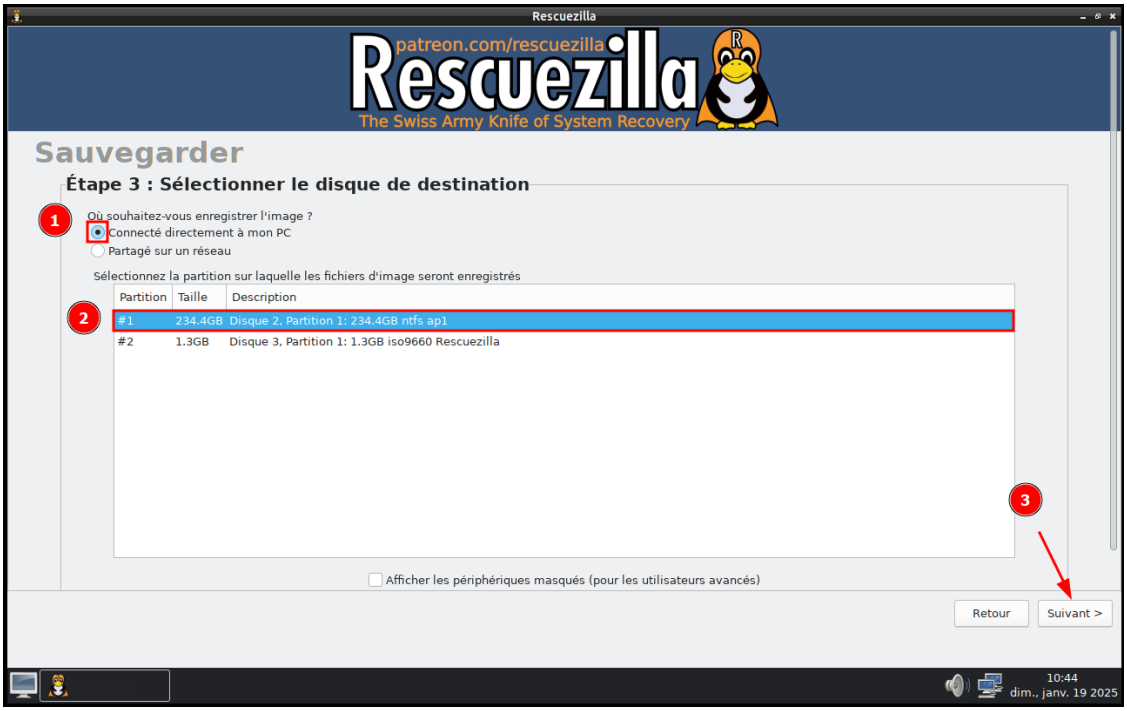


14%20Masterisation%20du%20poste%20Linux%20182dbb723a2881a19dbedb5f8020d02e/image%205.png

3. **Configuration de la sauvegarde**

   Laissez cocher « Connecté directement à mon PC ».

   Sélectionnez le support sur lequel sera effectuée la sauvegarde et cliquez sur `Suivant`.



14%20Masterisation%20du%20poste%20Linux%20182dbb723a2881a19dbedb5f8020d02e/image%206.png

4. **Démarrage de la sauvegarde**

   Renommez la sauvegarde si nécessaire, puis cliquez sur `Suivant` pour lancer la sauvegarde.

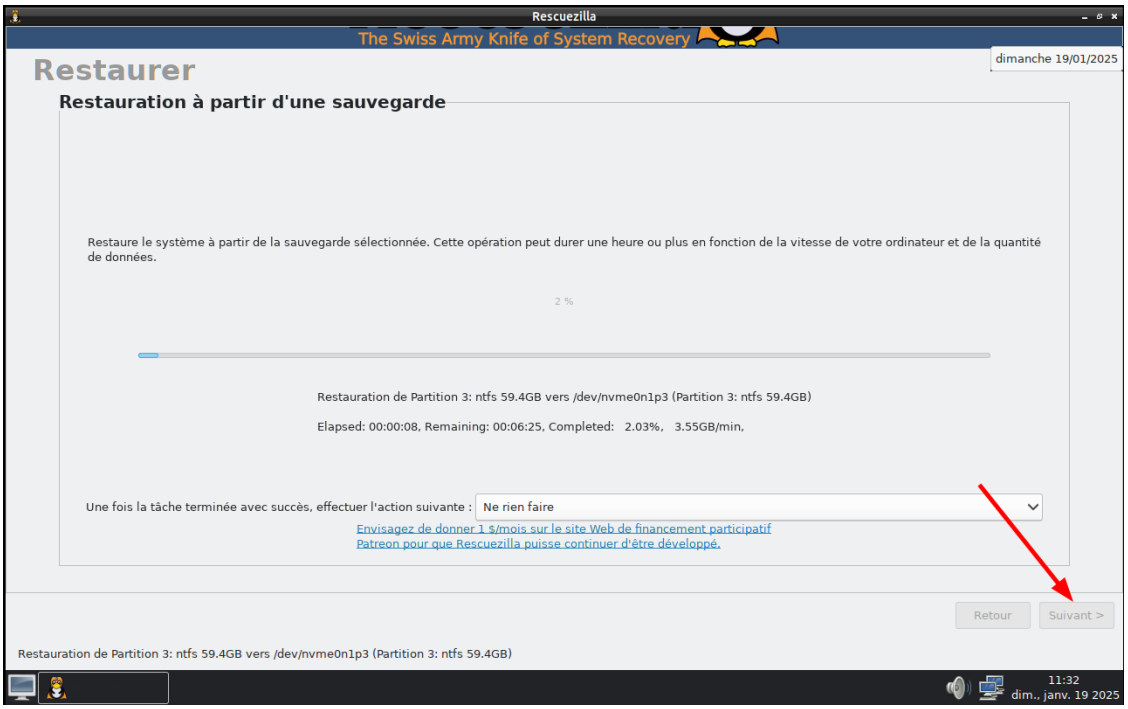
14%20Masterisation%20du%20poste%20Linux%20182dbb723a2881a19dbedb5f8020d02e/image%207.png

14%20Masterisation%20du%20poste%20Linux%20182dbb723a2881a19dbedb5f8020d02e/image%208.png

Une barre de progression indique l'avancement de la sauvegarde. Une fois terminée, cliquez sur `Suivant`.

5. **Arrêt de la VM**

Une fois de retour à l'accueil, vous pouvez éteindre la VM.



14%20Masterisation%20du%20poste%20Linux%20182dbb723a2881a19dbedb5f8020d02e/image%209.png

---

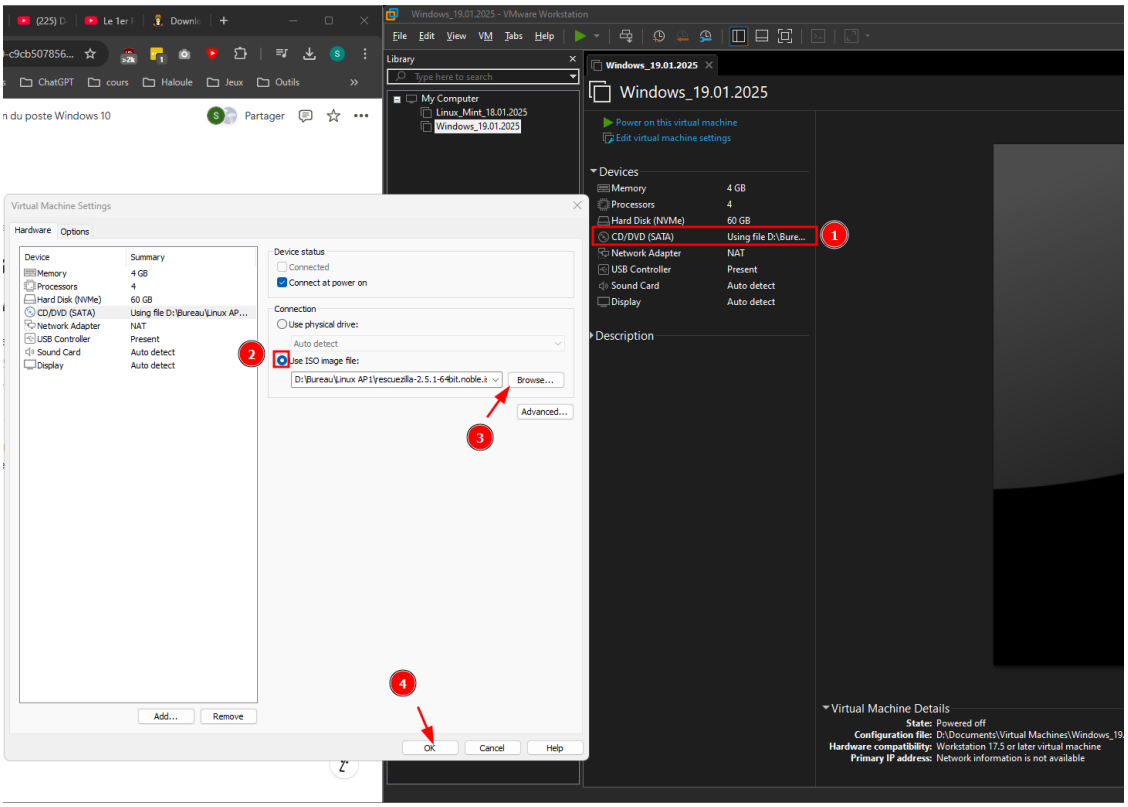
5. Restauration du système

1. **Création d'une nouvelle VM**

   Pour restaurer un système, créez une nouvelle VM. Vous pouvez suivre le guide « 00. Création d'une machine virtuelle (VM) dans VMware » si besoin.

2. **Chargement de l'ISO Rescuezilla**

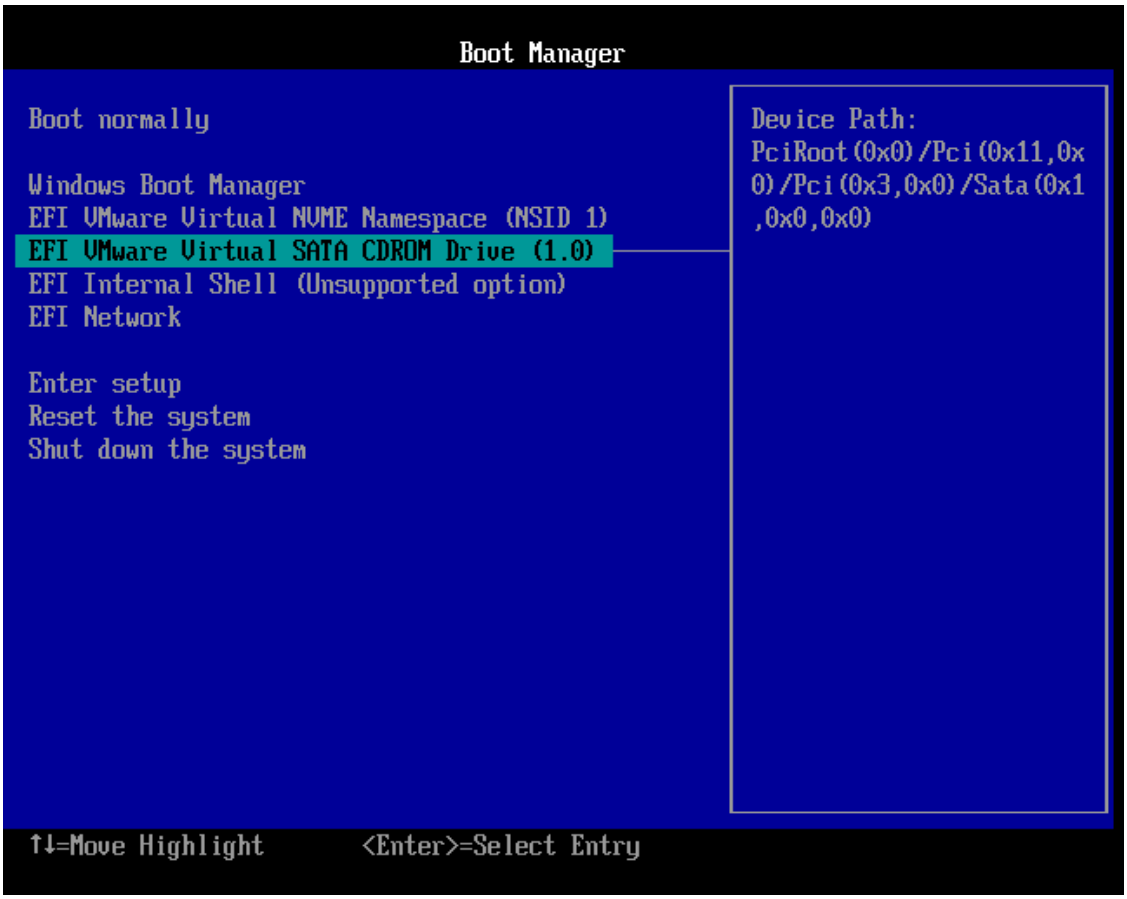
   Répétez la configuration initiale en sélectionnant « Use ISO image file » et en choisissant `rescuezilla.iso`.



14%20Masterisation%20du%20poste%20Linux%20182dbb723a2881a19dbedb5f8020d02e/image.png

3. **Accès au BIOS et démarrage Rescuezilla**

   Suivez les mêmes étapes que pour la sauvegarde afin de lancer Rescuezilla.



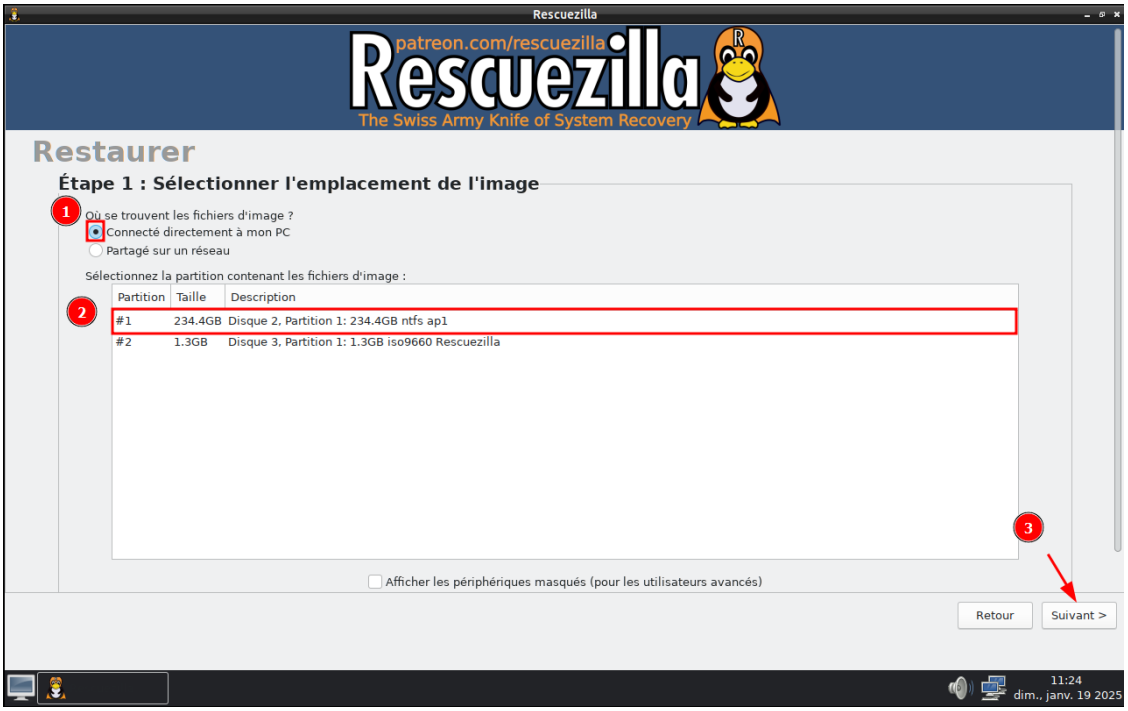
14%20Masterisation%20du%20poste%20Linux%20182dbb723a2881a19dbedb5f8020d02e/image%201.png

4. **Lancement de la restauration**

   Cliquez sur `Restaurer`.

14%20Masterisation%20du%20poste%20Linux%20182dbb723a2881a19dbedb5f8020d02e/image%2010.png

Sélectionnez le support contenant la sauvegarde et cliquez sur `Suivant`.



14%20Masterisation%20du%20poste%20Linux%20182dbb723a2881a19dbedb5f8020d02e/image%2011.png

5. **Finalisation**

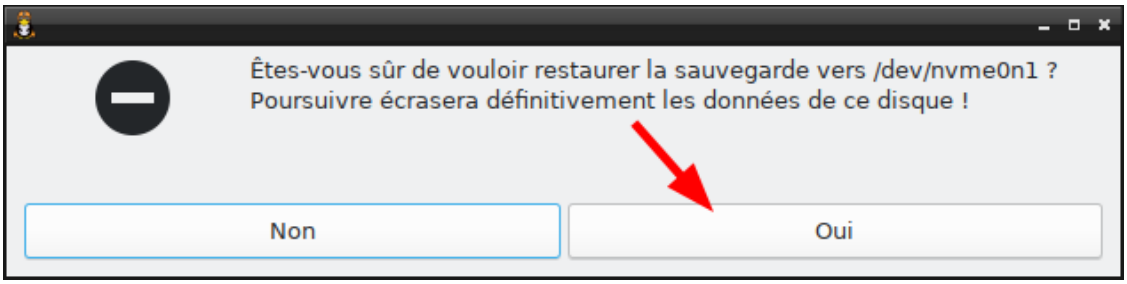
DOCUMENTATION D'INSTALLATION

Sélectionnez l'image à restaurer, la VM cible, puis suivez les instructions pour terminer la restauration.

14%20Masterisation%20du%20poste%20Linux%20182dbb723a2881a19dbedb5f8020d02e/image%2012.png

14%20Masterisation%20du%20poste%20Linux%20182dbb723a2881a19dbedb5f8020d02e/image%2013.png

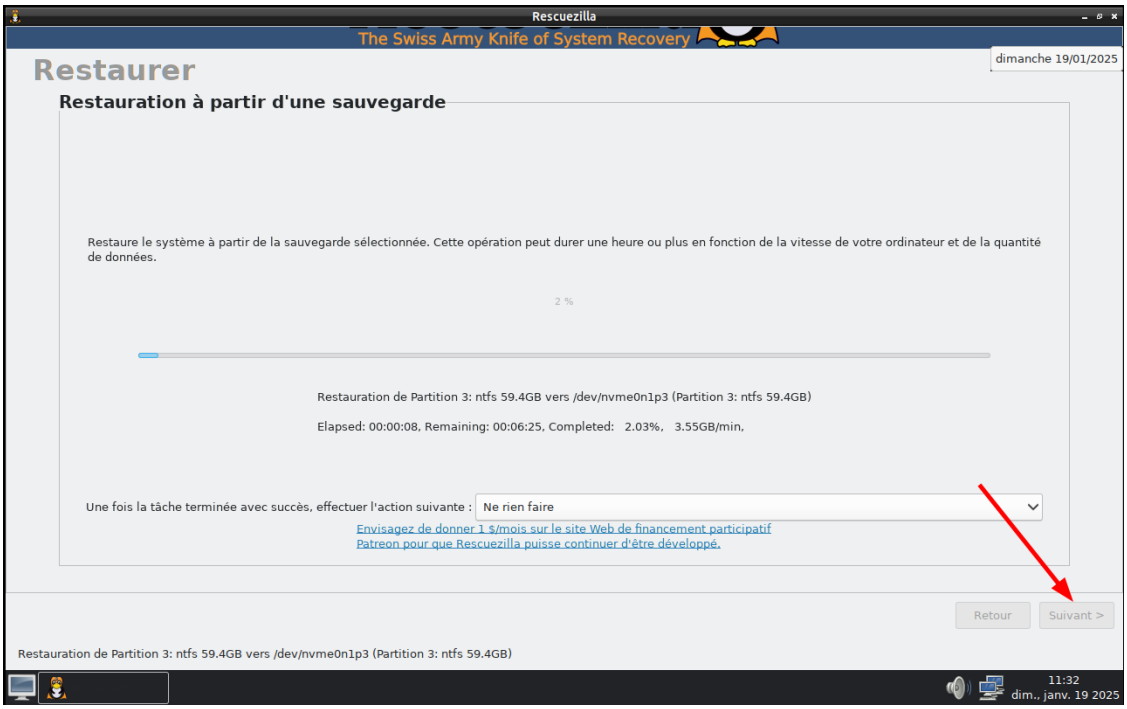
Cliquez sur `Oui` pour confirmer et démarrer la restauration.



14%20Masterisation%20du%20poste%20Linux%20182dbb723a2881a19dbedb5f8020d02e/image%2014.png

6. **Démarrage du système restauré**

   Une fois la restauration terminée, redémarrez la VM pour utiliser votre système restauré.



14%20Masterisation%20du%20poste%20Linux%20182dbb723a2881a19dbedb5f8020d02e/image%209.png

---

6. Pourquoi ces étapes sont importantes ?

- **Standardisation et cohérence** : La masterisation permet de garantir que tous les postes disposent de la même configuration et des mêmes outils, réduisant ainsi les variations et les problèmes de compatibilité.

- **Gain de temps et efficacité** : Les sauvegardes et restaurations rapides avec Rescuezilla simplifient le déploiement et la maintenance des postes en cas de panne ou de mise à jour.
- **Sécurité renforcée** : Une image de sauvegarde configurée correctement assure un environnement maîtrisé et limite les risques liés aux erreurs de configuration ou aux intrusions.

Bibliographie

Pour renforcer la sécurité de votre système Linux, voici une liste d'actions recommandées avec leurs tutoriels et aides détaillés.

---

1. Chiffrement du Disque avec LVM :

- Le chiffrement protège vos données en cas de vol ou de perte du matériel.
  - Aide 1 : https://www.youtube.com/watch?v=AT_hM-j4xmA&t=910s

2. Mise à Jour du Système :

- Maintenir votre système à jour est essentiel pour corriger les vulnérabilités connues.
  - Aide 1 : https://www.fosslinux.com/132214/how-to-set-up-automatic-updates-in-linux-mint.htm
  - Aide 2 : https://linuxiac.com/how-to-configure-linux-mint-21-automatic-updates/
  - Aide 3 : https://sites.google.com/site/installationubuntu/raspberry-pi/unattended-upgrades
  - Aide 4 : https://forum-francophone-linuxmint.fr/
  - Aide 5 : https://www.thegeekdiary.com/
  - Aide 6 : https://forums.linuxmint.com/
  - Aide 7 : https://community.linuxmint.com/

3. Configuration du Pare-feu UFW :

- UFW (Uncomplicated Firewall) simplifie la gestion des règles de pare-feu sous Linux.
  - Aide 1 : https://doc.ubuntu-fr.org/ufw
  - Aide 2 : https://www.ionos.fr/digitalguide/serveur/know-how/ports-tcpet-udp/

- Aide 3 : https://linuxhandbook.com/ufw-logs/
- Aide 4 : https://www.linuxbabe.com/security/ufw-firewall-debian-ubuntu-linux-mint-server
- Aide 5 : https://chmodcommand.com/

4. Désactivation des Services Non Nécessaires :

- Réduire le nombre de services actifs limite les points d'entrée potentiels pour les attaquants.
  - Aide 1 : https://www.linuxtricks.fr/wiki/optimiser-linux-pour-un-pc-portable
  - Aide 2 : https://grawok.wordpress.com/2011/12/16/desactiver-les-services-inutiles-sous-linux/
  - Aide 3 : https://easylinuxtipsproject.blogspot.com/p/speed-mint.html#ID1.1
  - Aide 4 : https://github.com/samderkaoui/systemd-service-hardening

5. Sécurisation de SSH :

- Sécuriser SSH est essentiel pour protéger les accès distants à votre système.
  - Aide 1 : https://www.malekal.com/activer-ssh-linux/
  - Aide 2 : https://www.ionos.fr/assistance/infrastructures-serveurs-et-cloud/premiers-pas/informations-importantes-sur-la-securite-de-votre-serveur/desactiver-la-connexion-root-ssh/
  - Aide 3 : https://thkernel.medium.com/comment-activer-ou-d%C3%A9sactiver-lauthentification-par-cl%C3%A9-publique-ssh-565b3558ef96

6. Installation de ClamAV et Lynis :

- ClamAV est un antivirus pour Linux, et Lynis est un outil d'audit de sécurité.
  - Aide 1 : https://community.time4vps.com/discussion/125/lynis-and-clamav-installation
  - Aide 2 : https://thesecmaster.com/blog/how-to-install-clamav-on-linux-mint
  - Aide 3 : https://www.it-connect.fr/scan-de-votre-systeme-unix-avec-lynis/

7. Restriction d'Accès aux Journaux Système :

- Limiter l'accès aux fichiers de logs protège la confidentialité et l'intégrité des informations.
  - Aide 1 : https://www.man7.org/linux/man-pages/man5/rsyslog.conf.5.html
  - Aide 2 : https://doc.ubuntu-fr.org/syslog-ng

- Aide 3 : https://docs.redhat.com/fr/documentation/red_hat_enterprise_linux/7/html/system_administrators_guide/s1-basic_configuration_of_rsyslog#s2-Filters
- Aide 4 : https://www.webhi.com/how-to/fr/comment-acceder-et-configurer-les-journaux-systeme-sur-ubuntu-et-debian/

8. Activation de l'Audit Système :

- L'audit système permet de surveiller les activités et de détecter les comportements suspects.
  - Aide 1 : https://www.it-connect.fr/linux-enregistrer-toutes-les-commandes-saisies-avec-auditd/
  - Aide 2 : https://www.webhi.com/how-to/fr/comment-acceder-et-configurer-les-journaux-systeme-sur-ubuntu-et-debian/

9. Configuration des Règles iptables :

- iptables est un outil puissant de filtrage réseau sous Linux.
  - Aide 1 : https://doc.ubuntu-fr.org/iptables

10. Désactivation de l'Exécution de Scripts dans /tmp :

- Bloquer l'exécution de scripts dans /tmp réduit les risques de code malveillant.
  - Aide 1 : https://docs.redhat.com/fr/documentation/red_hat_enterprise_linux/6/html/storage_administration_guide/sect-using_the_mount_command-mounting-options
  - Aide 2 : https://help.eset.com/efs/8.1/fr-FR/using-the-noexec-flag.html
  - Aide 3 : https://help.eset.com/essl/10.1/fr-FR/using_the_noexec_flag.html
  - Aide 4 : https://www.debian.org/doc/manuals/securing-debian-manual/ch04s10.fr.html

11. Restriction des Droits sur les Fichiers Sensibles :

- Une gestion stricte des permissions protège contre les accès non autorisés.

12. Installation de fail2ban :

- fail2ban bloque automatiquement les adresses IP suspectes.
    - Aide 1 : https://doc.ubuntu-fr.org/fail2ban

13. Deploiement de logiciel :

- Le déploiement de logiciel sous forme de script :
    - Aide 1 : https://doc.ubuntu-fr.org/apt
    - Aide 2 : https://helpcenter.onlyoffice.com/installation/desktop-install-ubuntu.aspx
    - Aide 3 : https://blog.stephane-robert.info/docs/admin-serveurs/linux/script-shell/
    - Aide 4 : https://askubuntu.com/questions/

Dépannage

0. Documentation de dépannage pour l'installation de Linux Mint sur VMware

Voici une documentation de dépannage adaptée au guide que vous avez fourni sur l'installation de Linux Mint dans un environnement VMware.

---

1. Problème : VMware ne démarre pas ou affiche une erreur

- **Symptôme** : VMware ne se lance pas, ou une erreur s'affiche comme "VMware Workstation Pro is not responding".
- **Solution** :
  1. Assurez-vous que VMware est installé correctement.
  2. Vérifiez que la virtualisation est activée dans le BIOS/UEFI de votre ordinateur.
     - Redémarrez votre ordinateur.
     - Accédez au BIOS (souvent via la touche **F2**, **DEL** ou **ESC** au démarrage).
     - Activez l'option **Intel VT-x** ou **AMD-V**.
  3. Redémarrez l'ordinateur et réessayez.

2. Problème : Impossible de créer une machine virtuelle

- **Symptôme** : Message d'erreur "Cannot open VM or create a new one".
- **Solution** :
  1. Vérifiez l'espace disque disponible.
  2. Exécutez VMware en tant qu'administrateur (clic droit sur l'icône > **Exécuter en tant qu'administrateur**).
  3. Supprimez les fichiers temporaires :
     - Sous Windows : `%temp%` dans la barre d'adresse de l'explorateur > Supprimer les fichiers.

3. Problème : Le fichier ISO de Linux Mint n'est pas détecté

- **Symptôme** : VMware affiche "No bootable medium found".
- **Solution** :
    1. Assurez-vous que le fichier ISO est valide :
        - Vérifiez le fichier avec une somme de contrôle SHA256 (commande : `sha256sum <nom_du_fichier>.iso` sous Linux).
    2. Vérifiez la configuration du lecteur CD/DVD :
        - Allez dans les **Settings** de la VM.
        - Sous l'onglet **CD/DVD (SATA)**, assurez-vous que l'option **Use ISO image file** est sélectionnée.

4. Problème : La VM démarre, mais Linux Mint reste bloqué sur l'écran de démarrage

- **Symptôme** : L'écran d'installation de Linux Mint ne charge pas.
- **Solution** :
    1. Augmentez la mémoire RAM allouée à la VM à au moins **4 Go** :
        - VMware > **Settings** > **Memory**.
    2. Activez l'option de virtualisation matérielle :
        - VMware > **Settings** > **Processors** > **Virtualize Intel VT-x/EPT or AMD-V**.
    3. Essayez un autre fichier ISO ou une version différente de Linux Mint.

5. Problème : Erreur lors de l'installation de Linux Mint

- **Symptôme** : Message d'erreur concernant le disque virtuel ou l'espace insuffisant.
- **Solution** :
    1. Assurez-vous que le disque virtuel a une taille suffisante (au moins **40 Go**).
        - VMware > **Settings** > **Hard Disk** > Ajustez la taille.
    2. Vérifiez que le type de disque est **SCSI** :
        - VMware > **Settings** > **Hard Disk** > **Type** > Sélectionnez **SCSI (Recommended)**.
    3. Redémarrez l'installation.

6. Problème : Impossible de se connecter au réseau dans la VM

- **Symptôme** : La VM n'a pas d'accès Internet.
- **Solution** :
    1. Vérifiez que l'adaptateur réseau est configuré en **NAT** :
        - VMware > **Settings** > **Network Adapter** > **NAT**.
    2. Redémarrez les services réseau de la VM :

- Sous Linux Mint, exécutez : `sudo systemctl restart network-manager`.

7. Problème : Clavier ou souris non détectés dans la VM

- **Symptôme** : Les périphériques d'entrée ne fonctionnent pas.
- **Solution** :
  1. Installez les VMware Tools pour Linux :
     - Menu VMware > **Install VMware Tools**.
     - Suivez les instructions pour installer les outils dans Linux Mint.
  2. Redémarrez la VM après l'installation.

8. Problème : Mot de passe oublié pour l'utilisateur Linux Mint

- **Symptôme** : Impossible de se connecter à la session utilisateur.
- **Solution** :
  1. Redémarrez la VM et sélectionnez **Recovery Mode** dans le menu GRUB.
  2. Accédez à une session root :
     - Tapez : `passwd <nom_utilisateur>` pour réinitialiser le mot de passe.
     - Redémarrez la VM.

9. Annexes

1. **Commandes Linux utiles** :
   - Vérifier l'espace disque : `df -h`.
   - Redémarrer le gestionnaire de services : `sudo systemctl restart <service>`.
   - Forcer une mise à jour du système : `sudo apt-get dist-upgrade`.
2. **Ressources supplémentaires** :
   - Documentation officielle de Linux Mint : https://linuxmint.com/documentation.php.
   - Forum VMware : https://communities.vmware.com/.

DOCUMENTATION D'INSTALLATION

1. Documentation de dépannage pour les mises à jour du système sous Linux Mint

Voici une documentation de dépannage détaillée pour répondre aux problèmes éventuels liés à la mise à jour du système et à l'automatisation des correctifs avec **unattended-upgrades**.

---

1. Problème : La commande `sudo apt update` retourne des erreurs

- **Symptôme** : Messages d'erreur du type "Failed to fetch" ou "Hash Sum mismatch".
- **Solution** :
  1. Mettez à jour les sources des dépôts :

     ```
     sudo rm -rf /var/lib/apt/lists/*
     sudo apt update
     ```

  2. Vérifiez le fichier `/etc/apt/sources.list` pour détecter des dépôts corrompus ou obsolètes.

  3. Si les erreurs persistent, changez de serveur miroir :

     - **Ouvrir le gestionnaire de mise à jour** > **Édition** > **Sources de logiciels** > Sélectionnez un autre miroir.

2. Problème : La commande `sudo apt upgrade` est interrompue

- **Symptôme** : Le processus de mise à jour s'arrête avec des erreurs concernant dpkg.
- **Solution** :
  1. Réparez les paquets cassés :

     ```
     sudo apt --fix-broken install
     ```

  2. Réinitialisez les configurations des paquets problématiques :

     ```
     sudo dpkg --configure -a
     ```

3. Problème : Les mises à jour automatiques ne fonctionnent pas

- **Symptôme** : `unattended-upgrades` n'applique pas les correctifs.

- **Solution** :
  1. Vérifiez que le service est actif :

     ```
     sudo systemctl status unattended-upgrades.service
     ```

     - Si le service est inactif, redémarrez-le :

       ```
       sudo systemctl restart unattended-upgrades.service
       ```

  2. Vérifiez les logs des mises à jour automatiques :

     ```
     cat /var/log/unattended-upgrades/unattended-upgrades.log
     ```

  3. Exécutez un test à blanc pour détecter les erreurs :

     ```
     sudo unattended-upgrades --dry-run
     ```

4. Problème : Les paquets spécifiques ne se mettent pas à jour

- **Symptôme** : Certains paquets restent bloqués dans une ancienne version.
- **Solution** :
  1. Supprimez le verrouillage des paquets :

     ```
     sudo apt-mark unhold <nom_du_paquet>
     ```

  2. Forcez la mise à jour :

     ```
     sudo apt install --only-upgrade <nom_du_paquet>
     ```

5. Problème : Erreur liée à `chmod` lors de la configuration

- **Symptôme** : Les fichiers de configuration de `unattended-upgrades` ne sont pas modifiables.
- **Solution** :
  1. Ajustez les permissions des fichiers concernés :

     ```
     sudo chmod 644 /etc/apt/apt.conf.d/50unattended-upgrades
     sudo chmod 644 /etc/apt/apt.conf.d/20auto-upgrades
     ```

  2. Vérifiez les permissions globales du répertoire :

     ```
     ls -l /etc/apt/apt.conf.d/
     ```

6. Problème : Notifications ou alertes d'erreurs dans le journal

- **Symptôme** : Les logs affichent des erreurs du type "Failed to lock /var/cache/apt/archives/lock".
- **Solution** :
  1. Libérez les verrous APT bloqués :

     ```
     sudo rm /var/lib/dpkg/lock-frontend
     sudo rm /var/lib/dpkg/lock
     sudo rm /var/cache/apt/archives/lock
     ```

  2. Reprenez l'opération interrompue :

     ```
     sudo dpkg --configure -a
     sudo apt update
     ```

7. Problème : L'interface graphique ne propose pas les mises à jour

- **Symptôme** : Le gestionnaire de mises à jour reste vide.
- **Solution** :
  1. Réinitialisez le gestionnaire de mise à jour :

     ```
     sudo mintupdate-cli refresh
     ```

  2. Réinstallez le gestionnaire :

     ```
     sudo apt install --reinstall mintupdate
     ```

8. Annexes

- **Commandes Linux utiles** :
  - Vérifier les mises à jour disponibles : `apt list --upgradable`.
  - Forcer la réinstallation d'un paquet : `sudo apt install --reinstall <nom_du_paquet>`.
- **Ressources supplémentaires** :
  - Documentation officielle d'APT : https://manpages.debian.org/apt.
  - Forum Linux Mint : https://forums.linuxmint.com/.

---

2. Documentation de dépannage pour la désactivation des services non nécessaires sous Linux

Voici une documentation de dépannage adaptée à la désactivation des services superflus, avec des solutions pour résoudre les éventuels problèmes.

---

1. Problème : Le service désactivé redémarre automatiquement

- **Symptôme** : Un service désactivé (ex. : `bluetooth.service`) redémarre après un redémarrage du système.
- **Solution** :

  1. Masquez le service pour empêcher tout redémarrage :

     ```
     sudo systemctl mask [nom_du_service]
     ```

  2. Vérifiez si le service est bien masqué :

  Le statut doit indiquer : `masked`.

  ```bash
  sudo systemctl status [nom_du_service]

  ```

2. Problème : Erreur "Failed to stop service"

- **Symptôme** : Message d'erreur lors de l'exécution de la commande `sudo systemctl stop`.
- **Solution** :
  1. Forcez l'arrêt du service :

     ```
     sudo systemctl kill [nom_du_service]
     sudo systemctl stop [nom_du_service]
     ```

  2. Si le service est essentiel à un autre processus, identifiez et arrêtez ce dernier :

     ```
     ps aux | grep [nom_du_service]
     kill -9 [PID]
     ```

3. Problème : La commande `systemctl disable` ne fonctionne pas

- **Symptôme** : Le service reste activé au démarrage malgré sa désactivation.
- **Solution** :
  1. Supprimez les fichiers de liens symboliques liés au service :

     ```
     sudo rm /etc/systemd/system/multi-user.target.wants/[nom_du_service].service
     sudo rm /etc/systemd/system/[nom_du_service].service
     ```

  2. Rechargez la configuration de `systemd` :

     ```
     sudo systemctl daemon-reload
     ```

4. Problème : Perte de fonctionnalité après la désactivation d'un service

- **Symptôme** : Une fonctionnalité clé du système devient inutilisable après la désactivation d'un service (ex. : pas d'accès réseau après désactivation de `NetworkManager`).
- **Solution** :
  1. Réactivez temporairement le service concerné pour restaurer la fonctionnalité :

     ```
     sudo systemctl start [nom_du_service]
     ```

  2. Analysez si le service est indispensable et réactivez-le au démarrage si nécessaire :

     ```
     sudo systemctl enable [nom_du_service]
     ```

5. Problème : Les services désactivés ne s'affichent pas dans `systemctl status`

- **Symptôme** : Les services désactivés ou arrêtés ne sont pas visibles avec `systemctl status`.
- **Solution** :
  1. Listez tous les services (actifs et inactifs) :

     ```
     sudo systemctl list-units --all
     ```

  2. Identifiez les services inactifs ou masqués :

     ```
     sudo systemctl list-units --state=inactive
     ```

6. Problème : Services réactivés après une mise à jour système

- **Symptôme** : Un service désactivé (ex. : `snapd.service`) se réactive après une mise à jour.
- **Solution** :
  1. Vérifiez les fichiers de configuration des services après la mise à jour.
  2. Remasquez les services problématiques :

     ```
     sudo systemctl mask [nom_du_service]
     ```

7. Problème : Erreur d'autorisation lors de la désactivation d'un service

- **Symptôme** : Message "Permission denied" avec les commandes `systemctl stop` ou `systemctl disable`.
- **Solution** :
  1. Exécutez les commandes avec des privilèges `sudo`.
  2. Vérifiez les permissions des fichiers de configuration du service :

     ```
     ls -l /etc/systemd/system/[nom_du_service].service
     ```

  3. Ajustez les permissions si nécessaire :

     ```
     sudo chmod 644 /etc/systemd/system/[nom_du_service].service
     ```

8. Annexes

- **Commandes utiles** :
  - Vérifier l'état d'un service : `sudo systemctl status [nom_du_service]`.
  - Redémarrer un service : `sudo systemctl restart [nom_du_service]`.
  - Lister tous les services : `sudo systemctl list-units --type=service`.
- **Documentation complémentaire** :
  - Guide officiel de systemd : https://www.freedesktop.org/wiki/Software/systemd/.

3. Documentation de dépannage pour l'activation de l'audit système avec `auditd` sous Linux

Voici une documentation détaillée pour résoudre les problèmes courants liés à l'installation, la configuration et l'utilisation de `auditd` sur un système Linux.

---

1. Problème : Erreur lors de l'installation de `auditd`

- **Symptôme** : Message "Unable to locate package auditd" ou "Package not found".
- **Solution** :
  1. Mettez à jour la liste des paquets :

     ```
     sudo apt update
     ```

  2. Vérifiez que les dépôts nécessaires sont activés dans `/etc/apt/sources.list`.
  3. Réessayez l'installation :

     ```
     sudo apt install auditd audispd-plugins -y
     ```

2. Problème : Le service `auditd` ne démarre pas

- **Symptôme** : Message "Failed to start auditd.service".
- **Solution** :
  1. Vérifiez les permissions et les dépendances :

     ```
     sudo journalctl -xe
     ```

  2. Réparez les fichiers de configuration si nécessaire :

  Réinitialisez le fichier de configuration par défaut.

  ```bash
  sudo cp /etc/audit/auditd.conf /etc/audit/auditd.conf.backup
  ```

  3. Redémarrez le service :

     ```
     sudo systemctl restart auditd
     ```

3. Problème : Les règles d'audit ne s'appliquent pas

- **Symptôme** : Les événements configurés dans les règles ne sont pas consignés.
- **Solution** :
  1. Vérifiez la syntaxe des règles :

     ```
     sudo auditctl -l
     ```

  2. Rechargez les règles :

     ```
     sudo systemctl restart auditd
     ```

  3. Vérifiez si le fichier `/etc/audit/rules.d/audit.rules` contient des erreurs de configuration.

4. Problème : L'audit ne capture pas les événements système spécifiques

- **Symptôme** : Les journaux ne montrent pas d'événements pour des fichiers ou des actions spécifiques (ex. : modification de `/etc/passwd`).
- **Solution** :
  1. Assurez-vous que le fichier ou l'action est bien surveillé dans les règles :

     ```
     sudo cat /etc/audit/rules.d/audit.rules
     ```

  2. Ajoutez une règle manuellement et rechargez :

     ```
     sudo auditctl -w /etc/passwd -p wa -k passwd_changes
     ```

5. Problème : Les journaux d'audit sont vides

- **Symptôme** : Le fichier `/var/log/audit/audit.log` ne contient pas de données.
- **Solution** :
  1. Vérifiez que le service est actif :

     ```
     sudo systemctl status auditd
     ```

  2. Assurez-vous que l'espace disque est suffisant pour les logs :

     ```
     df -h
     ```

  3. Relancez le service après nettoyage ou redémarrage :

     ```
     sudo systemctl restart auditd
     ```

6. Problème : Erreur lors de la mise à jour de GRUB pour activer l'audit au démarrage

- **Symptôme** : Message "update-grub command not found".
- **Solution** :
  1. Installez le paquet GRUB si nécessaire :

     ```
     sudo apt install grub2-common
     ```

  2. Relancez la commande :

     ```
     sudo update-grub
     ```

7. Problème : Les journaux d'audit se remplissent trop vite

- **Symptôme** : Le fichier `/var/log/audit/audit.log` occupe une grande quantité d'espace disque.
- **Solution** :
  1. Activez la rotation des journaux dans `/etc/audit/auditd.conf` :
     - Vérifiez ou modifiez les paramètres suivants :

       ```
       max_log_file = 10
       num_logs = 5
       ```

  2. Redémarrez le service pour appliquer les changements :

     ```
     sudo systemctl restart auditd
     ```

8. Annexes

- **Commandes utiles** :
  - Voir les règles actives : `sudo auditctl -l`.
  - Rechercher un événement spécifique : `sudo ausearch -k [clé]`.
  - Générer un rapport global : `sudo aureport`.
- **Ressources supplémentaires** :
  - Documentation officielle `auditd` : https://linux.die.net/man/8/auditd.

4. Documentation de dépannage pour la sécurisation de SSH sous Linux

Voici une documentation complète pour résoudre les problèmes courants liés à la configuration et à la sécurisation de SSH.

---

1. Problème : Impossible de démarrer le service SSH

- **Symptôme** : Le service SSH ne démarre pas ou retourne une erreur.
- **Solution** :
  1. Vérifiez les journaux pour diagnostiquer l'erreur :

     ```
     sudo journalctl -xe | grep ssh
     ```

  2. Testez la configuration de SSH :

  Corrigez toute erreur signalée dans le fichier `/etc/ssh/sshd_config`.

  ```bash
  sudo sshd -t

  ```

  3. Redémarrez le service :

     ```
     sudo systemctl restart ssh
     ```

2. Problème : Connexion SSH refusée

- **Symptôme** : L'accès distant via SSH est bloqué.
- **Solution** :
  1. Vérifiez si le service SSH est actif :

     ```
     sudo systemctl status ssh
     ```

  2. Confirmez que le port SSH est ouvert dans le pare-feu :

     ```
     sudo ufw allow 22
     sudo ufw status
     ```

  3. Testez la connexion localement :

```
ssh localhost
```

3. Problème : Accès root toujours possible malgré `PermitRootLogin no`

- **Symptôme** : Les connexions root sont autorisées même après configuration.
- **Solution** :
  1. Assurez-vous que la ligne suivante dans `/etc/ssh/sshd_config` n'est pas commentée :

     ```
     PermitRootLogin no
     ```

  2. Redémarrez SSH après modification :

     ```
     sudo systemctl restart ssh
     ```

4. Problème : Le port SSH personnalisé n'est pas fonctionnel

- **Symptôme** : Impossible de se connecter via un port SSH non standard.
- **Solution** :
  1. Modifiez le port SSH dans `/etc/ssh/sshd_config` :

     ```
     Port 2222
     ```

  2. Ouvrez le nouveau port dans le pare-feu :

     ```
     sudo ufw allow 2222
     ```

  3. Vérifiez si le service écoute sur ce port :

     ```
     sudo ss -l | grep 2222
     ```

5. Problème : L'authentification par clé publique ne fonctionne pas

- **Symptôme** : Les utilisateurs ne peuvent pas se connecter avec des clés SSH.
- **Solution** :
  1. Vérifiez les permissions du répertoire `.ssh` et des clés :

     ```
     chmod 700 ~/.ssh
     chmod 600 ~/.ssh/authorized_keys
     ```

  2. Assurez-vous que l'authentification par clé publique est activée dans `/etc/ssh/sshd_config` :

     ```
     PubkeyAuthentication yes
     ```

3. Redémarrez SSH et réessayez.

6. Problème : Détection d'activités suspectes dans les journaux SSH

- **Symptôme** : Les journaux montrent des tentatives d'accès non autorisées ou des activités suspectes.
- **Solution** :
  1. Recherchez les tentatives de connexion échouées :

     ```
     sudo grep "Failed password" /var/log/auth.log
     ```

  2. Bloquez les adresses IP suspectes avec `ufw` :

     ```
     sudo ufw deny from [IP]
     ```

  3. Installez et configurez `fail2ban` pour automatiser le blocage :

     ```
     sudo apt install fail2ban
     ```

7. Problème : Audit SSH non fonctionnel

- **Symptôme** : Les journaux d'audit ne capturent pas les événements SSH.
- **Solution** :
  1. Assurez-vous que les règles d'audit sont bien configurées :

     ```
     sudo cat /etc/audit/rules.d/audit.rules
     ```

  2. Rechargez le service d'audit :

     ```
     sudo systemctl restart auditd
     ```

8. Annexes

- **Commandes utiles** :
  - Tester la configuration SSH : `sudo sshd -t`.
  - Redémarrer SSH : `sudo systemctl restart ssh`.
  - Analyser les connexions : `sudo ausearch -k ssh_logins`.
- **Ressources supplémentaires** :
  - Documentation officielle OpenSSH : https://www.openssh.com/manual.html.

5. Documentation de dépannage pour la configuration du pare-feu UFW sous Linux

Voici une documentation pour résoudre les problèmes courants liés à l'installation, la configuration et la gestion du pare-feu UFW.

---

1. Problème : Le pare-feu UFW ne démarre pas ou ne s'active pas

- **Symptôme** : Message "UFW is not enabled" ou "Failed to enable UFW".
- **Solution** :
  1. Vérifiez le statut d'UFW :

     ```
     sudo ufw status
     ```

  2. Activez le pare-feu avec force si nécessaire :

     ```
     sudo ufw enable --force
     ```

  3. Si le problème persiste, vérifiez les logs pour diagnostiquer les erreurs :

     ```
     sudo journalctl -xe | grep ufw
     ```

2. Problème : Une règle UFW ne s'applique pas correctement

- **Symptôme** : Le trafic bloqué ou autorisé ne correspond pas aux règles configurées.
- **Solution** :
  1. Vérifiez la priorité des règles avec :

     ```
     sudo ufw status numbered
     ```

  2. Supprimez ou modifiez les règles conflictuelles :

     ```
     sudo ufw delete [numéro_de_règle]
     ```

  3. Redémarrez UFW pour appliquer les changements :

     ```
     sudo ufw reload
     ```

3. Problème : Impossible d'ajouter ou de modifier des règles

- **Symptôme** : Message "Permission denied" ou problème avec les fichiers de configuration.
- **Solution** :

1. Vérifiez les permissions des fichiers UFW :

Appliquez les permissions correctes si nécessaire :

```bash
ls -l /etc/ufw/
```

```bash
sudo chmod 700 /etc/ufw/before.rules
```

2. Vérifiez qu'UFW est actif avant d'ajouter des règles :

```
sudo ufw enable
```

4. Problème : Les journaux de trafic ne sont pas générés

- **Symptôme** : Aucun log n'apparaît malgré l'activation de la journalisation.
- **Solution** :
  1. Activez la journalisation si elle est désactivée :

     ```
     sudo ufw logging on
     ```

  2. Consultez les logs dans `/var/log/` :

     ```
     sudo tail -f /var/log/ufw.log
     ```

5. Problème : Le trafic autorisé par défaut bloque certaines connexions

- **Symptôme** : Des services autorisés (ex. : SSH) ne fonctionnent pas.
- **Solution** :
  1. Assurez-vous que les ports nécessaires sont explicitement ouverts :

     ```
     sudo ufw allow 22/tcp
     ```

  2. Modifiez la politique par défaut si nécessaire :

     ```
     sudo ufw default allow outgoing
     ```

6. Problème : Les règles ne sont pas persistantes après redémarrage

- **Symptôme** : Les règles configurées disparaissent après un redémarrage.
- **Solution** :
  1. Vérifiez que UFW est configuré pour démarrer automatiquement :

     ```
     sudo systemctl enable ufw
     ```

  2. Sauvegardez vos règles pour les restaurer si nécessaire :

     ```
     sudo ufw status > ufw-rules-backup.txt
     ```

7. Problème : Une connexion spécifique reste bloquée malgré les règles

- **Symptôme** : Une connexion autorisée par une règle reste inaccessible.
- **Solution** :
  1. Vérifiez si une règle plus restrictive est en conflit :

     ```
     sudo ufw status numbered
     ```

  2. Supprimez ou ajustez les règles bloquantes :

     ```
     sudo ufw delete [numéro_de_règle]
     ```

8. Annexes

- **Commandes utiles** :
  - Lister les règles avec numéros : `sudo ufw status numbered`.
  - Supprimer une règle spécifique : `sudo ufw delete [numéro_de_règle]`.
  - Réinitialiser UFW : `sudo ufw reset`.
- **Ressources supplémentaires** :
  - Documentation officielle UFW : https://wiki.ubuntu.com/UncomplicatedFirewall.

---

7. Documentation de dépannage pour l'installation de ClamAV et Lynis sous Linux

Voici une documentation complète pour résoudre les problèmes liés à l'installation, la configuration et l'utilisation de **ClamAV** et **Lynis**.

DOCUMENTATION D'INSTALLATION

1. Problème : Lynis ne s'installe pas ou retourne des erreurs

- **Symptôme** : Message "Unable to locate package lynis" ou erreur lors de l'installation.
- **Solution** :
    1. Mettez à jour les dépôts et réessayez :

       ```
       sudo apt update
       sudo apt-get install lynis -y
       ```

    2. Si le problème persiste, vérifiez si le dépôt officiel de Lynis est configuré :

       ```
       echo "deb http://packages.cisofy.com/community/lynis/deb/ stabl
       e main" | sudo tee /etc/apt/sources.list.d/lynis.list
       sudo apt update
       sudo apt install lynis -y
       ```

2. Problème : Lynis ne génère pas de rapport complet

- **Symptôme** : Certains paramètres ne sont pas analysés ou des avertissements apparaissent.
- **Solution** :
    1. Exécutez Lynis en tant que super-utilisateur pour un audit complet :

       ```
       sudo lynis audit system
       ```

    2. Vérifiez que les permissions des répertoires critiques sont accessibles :

       ```
       ls -ld /etc /var/log /tmp
       ```

3. Problème : ClamAV ne détecte pas les menaces malgré une base de signatures mise à jour

- **Symptôme** : Les scans de ClamAV ne trouvent aucune menace, même sur des fichiers test.
- **Solution** :
    1. Vérifiez que la base de signatures est à jour :

       ```
       sudo freshclam
       ```

    2. Testez la détection avec un fichier EICAR (fichier test non malveillant) :

       ```
       curl -o eicar.txt https://secure.eicar.org/eicar.com.txt
       clamscan eicar.txt
       ```

3. Si le fichier n'est pas détecté, redémarrez le service ClamAV :

```
sudo systemctl restart clamav-daemon
```

4. Problème : Erreur "freshclam: can't update database"

- **Symptôme** : ClamAV ne parvient pas à mettre à jour la base de signatures.
- **Solution** :
  1. Vérifiez les permissions du fichier de configuration :

```
sudo chmod 644 /etc/clamav/freshclam.conf
```

  2. Relancez la mise à jour après avoir arrêté le service freshclam :

```
sudo systemctl stop clamav-freshclam
sudo freshclam
sudo systemctl start clamav-freshclam
```

5. Problème : ClamTK ne démarre pas ou affiche une erreur

- **Symptôme** : L'interface graphique ClamTK ne s'ouvre pas.
- **Solution** :
  1. Assurez-vous que toutes les dépendances nécessaires sont installées :

```
sudo apt install clamtk -y
```

  2. Lancez ClamTK depuis un terminal pour détecter les éventuelles erreurs :

```
clamtk
```

6. Problème : ClamAV consomme trop de ressources pendant le scan

- **Symptôme** : Le système devient lent pendant un scan ClamAV.
- **Solution** :
  1. Effectuez un scan avec priorité réduite :

```
nice -n 19 clamscan -r /
```

  2. Excluez certains répertoires volumineux (ex. : sauvegardes) pour réduire la charge :

```
clamscan -r --exclude-dir=/backup /
```

7. Annexes

- **Commandes utiles** :
  - Mise à jour de ClamAV : `sudo freshclam`.
  - Audit système avec Lynis : `sudo lynis audit system`.
  - Vérification de la version de ClamAV : `clamscan --version`.
- **Ressources supplémentaires** :
  - Documentation officielle ClamAV : https://www.clamav.net/documentation.
  - Guide Lynis : https://cisofy.com/documentation/lynis/.

---

8. Documentation de dépannage pour l'installation et la configuration de Fail2Ban

Voici une documentation détaillée pour résoudre les problèmes courants liés à l'installation et à l'utilisation de **Fail2Ban**.

---

1. Problème : Le service Fail2Ban ne démarre pas

- **Symptôme** : La commande `systemctl start fail2ban` retourne une erreur ou le service ne démarre pas.
- **Solution** :
  1. Vérifiez les journaux pour identifier l'erreur :

     ```
     sudo journalctl -xe | grep fail2ban
     ```

  2. Testez la configuration de Fail2Ban pour détecter des erreurs dans les fichiers :

     ```
     sudo fail2ban-client -d
     ```

  3. Si une erreur est détectée, vérifiez le fichier `/etc/fail2ban/jail.local` ou `/etc/fail2ban/jail.conf` pour corriger la syntaxe.

2. Problème : Les adresses IP malveillantes ne sont pas bloquées

- **Symptôme** : Malgré des tentatives d'attaques visibles dans les journaux, aucune adresse IP n'est bloquée.
- **Solution** :

1. Assurez-vous que les règles Fail2Ban sont bien appliquées au pare-feu UFW :

Vérifiez si des règles comme "f2b-ssh" ou "f2b-apache" apparaissent.

```bash
sudo ufw status
```

2. Redémarrez le service pour appliquer les règles correctement :

```
sudo systemctl restart fail2ban
```

3. Consultez les logs pour vérifier l'activité de Fail2Ban :

```
sudo cat /var/log/fail2ban.log
```

3. Problème : Les règles personnalisées de jail.local ne fonctionnent pas

- **Symptôme** : Les paramètres définis dans `/etc/fail2ban/jail.local` ne sont pas pris en compte.
- **Solution** :

1. Assurez-vous que le fichier `jail.local` est correctement configuré :

Exemple de règle pour SSH :

```bash
sudo nano /etc/fail2ban/jail.local
```

```
[sshd]
enabled = true
port = ssh
logpath = /var/log/auth.log
maxretry = 5
bantime = 3600
```

2. Redémarrez Fail2Ban pour appliquer les modifications :

```
sudo systemctl restart fail2ban
```

4. Problème : Les journaux de Fail2Ban ne sont pas générés

- **Symptôme** : Le fichier `/var/log/fail2ban.log` est vide ou n'existe pas.
- **Solution** :
  1. Vérifiez si la journalisation est activée dans `/etc/fail2ban/fail2ban.conf` :

     ```
     logtarget = /var/log/fail2ban.log
     ```

  2. Corrigez les permissions si nécessaire :

     ```
     sudo chmod 644 /var/log/fail2ban.log
     ```

  3. Relancez le service pour recréer les logs :

     ```
     sudo systemctl restart fail2ban
     ```

5. Problème : Impossible de débloquer une adresse IP

- **Symptôme** : Une adresse IP est bloquée accidentellement et Fail2Ban continue de la bannir.
- **Solution** :
  1. Listez les adresses IP bannies :

     ```
     sudo fail2ban-client status sshd
     ```

  2. Débloquez l'adresse spécifique :

     ```
     sudo fail2ban-client unban <IP>
     ```

6. Problème : Trop de faux positifs

- **Symptôme** : Des utilisateurs légitimes sont bannis.
- **Solution** :
  1. Augmentez le nombre de tentatives autorisées dans `jail.local` :

     ```
     maxretry = 10
     ```

  2. Excluez des adresses IP spécifiques du bannissement en ajoutant une exception :

     ```
     ignoreip = 127.0.0.1/8 192.168.0.0/24
     ```

7. Annexes

- **Commandes utiles** :

- Vérifier le statut d'une jail : `sudo fail2ban-client status [nom_de_la_jail]`.
- Débloquer une adresse IP : `sudo fail2ban-client unban <IP>`.
- Redémarrer Fail2Ban : `sudo systemctl restart fail2ban`.

- **Ressources supplémentaires** :
  - Documentation officielle : https://www.fail2ban.org/.

---

9. Documentation de dépannage pour la désactivation de l'exécution de scripts dans `/tmp`

Voici une documentation complète pour résoudre les problèmes liés à la configuration et à la sécurisation du répertoire `/tmp`.

---

1. Problème : Les options de montage ne s'appliquent pas

- **Symptôme** : Après modification du fichier `/etc/fstab`, les options comme `nosuid` ou `nodev` ne semblent pas actives.
- **Solution** :
  1. Rechargez la configuration de montage :

     ```
     sudo systemctl daemon-reload
     sudo mount -a
     ```

  2. Vérifiez les options actuellement appliquées à `/tmp` :

     ```
     mount | grep /tmp
     ```

  3. Si les options ne sont pas appliquées, vérifiez le fichier `/etc/fstab` pour détecter des erreurs de syntaxe :

     ```
     cat /etc/fstab
     ```

2. Problème : Des applications cessent de fonctionner après la modification

- **Symptôme** : Des logiciels comme LibreOffice ou d'autres outils utilisant `/tmp` rencontrent des erreurs.
- **Solution** :
  1. Supprimez temporairement l'option problématique dans `/etc/fstab` (par ex. : `noexec`).

2. Ajoutez des exceptions pour les applications concernées en configurant leurs répertoires temporaires dans un autre emplacement. Exemple pour LibreOffice :

```
mkdir ~/temp
export TMPDIR=~/temp
```

3. Problème : Impossible de remonter `/tmp` après modification

- **Symptôme** : La commande `sudo mount -a` retourne une erreur.
- **Solution** :
  1. Vérifiez les logs pour identifier la source du problème :

     ```
     sudo journalctl -xe
     ```

  2. Assurez-vous que le répertoire `/tmp` existe et est vide avant de monter :

     ```
     sudo mkdir -p /tmp
     sudo umount /tmp
     ```

4. Problème : Échec des tests pour `nosuid` ou `nodev`

- **Symptôme** : Les scripts ou périphériques dans `/tmp` fonctionnent malgré les options de montage.
- **Solution** :
  1. Vérifiez les options appliquées :

     ```
     mount | grep /tmp
     ```

  2. Réappliquez les options correctes via un remontage :

     ```
     sudo mount -o remount,nosuid,nodev /tmp
     ```

  3. Refaites les tests avec les commandes suivantes :

     - Test pour `nosuid` :

     Le script ne doit pas exécuter avec des privilèges élevés.

     ```bash
     ./test_suid.sh
     ```

     - Test pour `nodev` :

     Ces actions doivent être bloquées.

```bash
sudo mknod /tmp/test_dev b 7 0
sudo losetup /dev/loop7 /tmp/test_dev

```

5. Problème : Performances réduites après configuration avec `tmpfs`

- **Symptôme** : Le système devient lent ou `/tmp` est saturé.
- **Solution** :
  1. Vérifiez l'espace disque alloué à `tmpfs` :

     ```
     df -h /tmp
     ```

  2. Augmentez la taille de `tmpfs` en ajustant l'entrée dans `/etc/fstab` :

     ```
     tmpfs /tmp tmpfs defaults,nosuid,nodev,size=1G 0 0
     ```

  3. Remontez `/tmp` avec la nouvelle taille :

     ```
     sudo mount -o remount /tmp
     ```

6. Annexes

- **Commandes utiles** :
  - Vérifier les options de montage : `mount | grep /tmp`.
  - Remonter `/tmp` avec des options spécifiques : `sudo mount -o remount,nosuid,nodev /tmp`.
  - Vérifier l'état de `/etc/fstab` : `cat /etc/fstab`.
- **Ressources supplémentaires** :
  - Documentation sur `fstab` : https://man7.org/linux/man-pages/man5/fstab.5.html.

---

10. Documentation de dépannage pour la stratégie de sécurité locale sous Linux Mint

Voici une documentation complète pour résoudre les problèmes courants liés à la mise en œuvre des politiques de sécurité locale, notamment la gestion des mots de passe et des utilisateurs.

---

1. Problème : Les règles de complexité des mots de passe ne sont pas appliquées

- **Symptôme** : Les utilisateurs peuvent définir des mots de passe faibles malgré les configurations dans `/etc/pam.d/common-password`.
- **Solution** :
  1. Vérifiez que le module `pam_pwquality` est bien installé :

     ```
     sudo apt install libpam-pwquality -y
     ```

  2. Assurez-vous que la ligne suivante est présente dans `/etc/pam.d/common-password` :

     ```
     password requisite pam_pwquality.so retry=3 minclass=4
     ```

  3. Redémarrez les sessions utilisateur pour appliquer les changements.

2. Problème : Les utilisateurs ne peuvent pas changer leur mot de passe

- **Symptôme** : Une erreur "Authentication token manipulation error" apparaît lors de la tentative de modification du mot de passe.
- **Solution** :

  1. Vérifiez les permissions des fichiers suivants :

  Les permissions doivent être :

  ```bash
  ls -l /etc/shadow /etc/passwd
  ```

  ```
  -rw-r--r-- 1 root root /etc/passwd
  -rw------- 1 root shadow /etc/shadow
  ```

  2. Corrigez les permissions si nécessaire :

     ```
     sudo chmod 644 /etc/passwd
     sudo chmod 600 /etc/shadow
     ```

3. Problème : La politique d'expiration des mots de passe ne fonctionne pas

- **Symptôme** : Les utilisateurs ne sont pas forcés de changer leur mot de passe après 90 jours.
- **Solution** :
    1. Vérifiez la configuration pour l'utilisateur concerné :

       ```
       sudo chage -l <nom_utilisateur>
       ```

    2. Appliquez une expiration de mot de passe manuellement :

       ```
       sudo chage -M 90 <nom_utilisateur>
       ```

4. Problème : L'utilisateur n'est pas invité à modifier son mot de passe à la première connexion

- **Symptôme** : L'utilisateur peut se connecter sans changer le mot de passe initial.
- **Solution** :

    1. Forcez l'expiration du mot de passe pour l'utilisateur :

       ```
       sudo passwd --expire <nom_utilisateur>
       ```

    2. Vérifiez la configuration :

    Assurez-vous que le mot de passe expire immédiatement.

    ```bash
    sudo chage -l <nom_utilisateur>

    ```

5. Problème : Création d'utilisateurs impossible via l'interface graphique

- **Symptôme** : Une erreur apparaît ou l'option "Ajouter" est grisée dans "Utilisateurs et groupes".
- **Solution** :
    1. Assurez-vous que l'utilisateur actuel dispose de privilèges administratifs.
    2. Lancez l'application "Utilisateurs et groupes" avec `sudo` :

       ```
       sudo users-admin
       ```

    3. Si le problème persiste, créez l'utilisateur via la ligne de commande :

       ```
       sudo adduser <nom_utilisateur>
       ```

6. Problème : Les mots de passe faibles sont acceptés même après configuration

- **Symptôme** : Des mots de passe ne respectant pas les critères (longueur, classes de caractères) sont acceptés.
- **Solution** :
  1. Testez la configuration de `pam_pwquality` avec un mot de passe non conforme pour vérifier qu'elle fonctionne :

     ```
     passwd <nom_utilisateur>
     ```

  2. Si le problème persiste, vérifiez que `libpwquality-tools` est installé et que les règles dans `/etc/security/pwquality.conf` sont correctement définies :

     ```
     minlen = 12
     minclass = 4
     retry = 3
     ```

7. Annexes

- **Commandes utiles** :
  - Vérifier la politique d'un utilisateur : `sudo chage -l <nom_utilisateur>`.
  - Modifier les paramètres PAM : `sudo nano /etc/pam.d/common-password`.
  - Liste des utilisateurs avec leurs politiques : `getent passwd`.
- **Ressources supplémentaires** :
  - Documentation PAM : https://linux-pam.org/.
  - Guide de sécurité Linux Mint : https://linuxmint.com/.

---

11. Documentation de dépannage pour la restriction d'accès aux journaux système sous Linux

Voici une documentation complète pour résoudre les problèmes courants liés à la gestion et à la sécurisation des journaux système.

---

1. Problème : Les permissions des journaux ne sont pas correctement appliquées

- **Symptôme** : Les utilisateurs non autorisés peuvent lire ou modifier les journaux dans `/var/log`.
- **Solution** :

1. Appliquez des permissions restreintes globales :

   ```
   sudo chmod -R go-rwx /var/log/*
   ```

2. Vérifiez les permissions :

   ```
   ls -l /var/log/
   ```

3. Assurez-vous que `root` et le groupe `adm` sont les propriétaires des fichiers :

   ```
   sudo chown -R root:adm /var/log/*
   ```

2. Problème : Les nouveaux fichiers journaux créés n'ont pas les bonnes permissions

- **Symptôme** : Les fichiers journaux nouvellement générés ne respectent pas les permissions par défaut définies.
- **Solution** :

1. Modifiez la configuration de `rsyslog` :

Ajoutez ou modifiez les lignes suivantes :

```bash
sudo nano /etc/rsyslog.conf

```

```
$FileOwner root
$FileGroup adm
$FileCreateMode 0640

```

2. Validez la configuration :

   ```
   sudo rsyslogd -N1
   ```

3. Redémarrez le service :

   ```
   sudo systemctl restart rsyslog
   ```

3. Problème : Les règles d'audit des journaux ne fonctionnent pas

- **Symptôme** : Les tentatives d'accès non autorisé aux journaux ne sont pas enregistrées.
- **Solution** :

1. Vérifiez le fichier des règles d'audit :

Assurez-vous qu'il contient :

```bash
sudo nano /etc/audit/rules.d/audit.rules

```

```
-w /var/log/auth.log -p wa -k auth_access

```

2. Chargez les nouvelles règles :

```
sudo augenrules --load
```

3. Redémarrez le service `auditd` :

```
sudo systemctl restart auditd
```

4. Problème : Les journaux critiques sont modifiés ou supprimés

- **Symptôme** : Les fichiers journaux dans `/var/log` sont altérés par des utilisateurs non autorisés.
- **Solution** :

1. Activez l'audit pour surveiller les modifications :

Ajoutez une règle pour chaque fichier critique, par exemple :

```bash
sudo nano /etc/audit/rules.d/audit.rules

```

```
-w /var/log/auth.log -p wa -k auth_modifications

```

2. Chargez les règles et surveillez les accès :

```
sudo augenrules --load
sudo ausearch -k auth_modifications
```

5. Problème : Les journaux deviennent inaccessibles après modification des permissions

- **Symptôme** : Les services système ne peuvent plus écrire dans les journaux.
- **Solution** :
  1. Assurez-vous que les propriétaires et groupes sont correctement configurés :

     ```
     sudo chown -R root:adm /var/log/*
     ```

  2. Vérifiez les permissions minimales requises :

     ```
     sudo chmod 640 /var/log/*
     ```

6. Annexes

- **Commandes utiles** :
  - Vérifier les permissions des journaux : `ls -l /var/log/`.
  - Rechercher les accès dans les journaux d'audit : `sudo ausearch -k auth_access`.
  - Redémarrer `rsyslog` après modification : `sudo systemctl restart rsyslog`.
- **Ressources supplémentaires** :
  - Documentation rsyslog : https://www.rsyslog.com/.
  - Guide sur auditd : https://linux.die.net/man/8/auditd.

---

12. Documentation de dépannage pour la restriction des droits sur les fichiers sensibles sous Linux

Voici une documentation complète pour résoudre les problèmes liés à la sécurisation des fichiers critiques sur le système.

---

1. Problème : Les permissions des fichiers sensibles sont incorrectes

- **Symptôme** : Les fichiers comme `/etc/passwd` ou `/etc/shadow` sont accessibles en écriture ou lecture à des utilisateurs non autorisés.
- **Solution** :
  1. Corrigez les permissions des fichiers :

```
sudo chmod 644 /etc/passwd
sudo chmod 640 /etc/shadow
```

2. Vérifiez les permissions :

Les résultats attendus :

```bash
ls -l /etc/passwd /etc/shadow

```

```
-rw-r--r-- 1 root root /etc/passwd
-rw-r----- 1 root shadow /etc/shadow

```

2. Problème : Les clés privées dans `/etc/ssl/private/` sont exposées

- **Symptôme** : Les clés privées sont accessibles à des utilisateurs non autorisés.
- **Solution** :

1. Modifiez les permissions des fichiers :

```
sudo chmod 600 /etc/ssl/private/ssl-cert-snakeoil.key
sudo chown root:root /etc/ssl/private/ssl-cert-snakeoil.key
```

2. Vérifiez les permissions :

Le résultat attendu :

```bash
ls -l /etc/ssl/private/

```

```
-rw------- 1 root root ssl-cert-snakeoil.key

```

3. Problème : Les journaux système sont accessibles à des utilisateurs non autorisés

- **Symptôme** : Les fichiers journaux dans `/var/log` peuvent être consultés ou modifiés par des utilisateurs non privilégiés.
- **Solution** :
  1. Appliquez des permissions restrictives :

     ```
     sudo chmod -R go-rwx /var/log/*
     sudo chown -R root:adm /var/log/
     ```

  2. Vérifiez les permissions :

     ```
     ls -ld /var/log/
     ```

4. Problème : Les modifications des permissions ne persistent pas après redémarrage

- **Symptôme** : Les permissions reviennent à un état par défaut après un redémarrage.
- **Solution** :
  1. Configurez les permissions par défaut dans les fichiers de configuration des services concernés :
     - Pour les journaux système, modifiez `/etc/rsyslog.conf` :

     Ajoutez ou modifiez :

     ```
     ```bash
     sudo nano /etc/rsyslog.conf

     ```

     ```
     $FileOwner root
     $FileGroup adm
     $FileCreateMode 0640

     ```
  2. Validez la configuration et redémarrez le service :

     ```
     sudo rsyslogd -N1
     sudo systemctl restart rsyslog
     ```

5. Problème : Un utilisateur standard peut toujours accéder aux fichiers sensibles

- **Symptôme** : Malgré les modifications, des utilisateurs non privilégiés peuvent consulter certains fichiers sensibles.
     ```

- **Solution** :

1. Simulez l'accès non autorisé avec un utilisateur standard :

Si l'accès est autorisé, vérifiez et corrigez les permissions :

```bash
sudo -u nobody cat /etc/shadow
```

```bash
sudo chmod 640 /etc/shadow
```

2. Vérifiez les appartenances aux groupes pour s'assurer qu'aucun utilisateur non autorisé ne fait partie du groupe `root` ou `adm` :

```
groups <nom_utilisateur>
```

---

14. Documentation de dépannage pour la masterisation du poste Linux avec Rescuezilla

Voici une documentation détaillée pour résoudre les problèmes courants liés à la sauvegarde et à la restauration de postes Linux à l'aide de Rescuezilla.

---

1. Problème : Impossible de démarrer sur Rescuezilla

- **Symptôme** : La VM ne démarre pas sur l'ISO de Rescuezilla.
- **Solution** :
  1. Assurez-vous que l'ISO est correctement attachée :

     ```
     VMware > Settings > CD/DVD (SATA) > Use ISO image file
     ```

  2. Vérifiez l'ordre de démarrage dans le BIOS :
     - Accédez au BIOS en appuyant sur F2 lors du démarrage.
     - Assurez-vous que `EFI VMware Virtual SATA CDROM Drive` est en premier dans l'ordre de démarrage.
  3. Si le problème persiste, téléchargez à nouveau l'ISO depuis Rescuezilla pour vérifier son intégrité.

2. Problème : La sauvegarde échoue

- **Symptôme** : Message d'erreur lors de la sauvegarde ou arrêt du processus.
- **Solution** :
    1. Vérifiez l'espace libre sur le support de sauvegarde :

       ```
       df -h
       ```

    2. Si l'espace est suffisant, testez le support avec la commande suivante :

    Remplacez `/dev/sdX` par le chemin du disque cible.

    ```bash
    sudo fsck /dev/sdX

    ```

    3. Relancez la sauvegarde après correction.

3. Problème : La restauration échoue

- **Symptôme** : L'image sauvegardée ne peut pas être restaurée sur une nouvelle VM.
- **Solution** :
    1. Vérifiez l'intégrité de l'image sauvegardée :
        - Depuis Rescuezilla, sélectionnez « Vérifier une sauvegarde » avant de la restaurer.
    2. Assurez-vous que la taille du disque cible est suffisante pour accueillir l'image.
    3. Relancez Rescuezilla et redémarrez la restauration.

4. Problème : La VM restaurée ne démarre pas

- **Symptôme** : La VM affiche une erreur ou reste bloquée après la restauration.
- **Solution** :
    1. Accédez au BIOS de la VM (F2) et vérifiez que le disque restauré est défini comme premier disque de démarrage.
    2. Si le problème persiste, redémarrez Rescuezilla et effectuez une vérification du disque cible avant de restaurer :

       ```
       sudo fsck /dev/sdX
       ```

    3. Recréez la VM avec les mêmes paramètres que celle utilisée pour créer la sauvegarde initiale.

5. Problème : La sauvegarde ou restauration est lente

- **Symptôme** : Le processus de sauvegarde ou de restauration prend plus de temps que prévu.
- **Solution** :
  1. Vérifiez les performances du support de stockage utilisé :

     ```
     sudo hdparm -Tt /dev/sdX
     ```

  2. Utilisez un support plus rapide (ex. : SSD) pour la sauvegarde/restauration.
  3. Limitez les processus actifs sur Rescuezilla pour allouer plus de ressources au processus.

6. Problème : Sauvegarde corrompue

- **Symptôme** : L'image restaurée contient des fichiers corrompus ou des erreurs système.
- **Solution** :
  1. Vérifiez l'intégrité du système avant la sauvegarde :

     ```
     sudo fsck -f /dev/sdX
     ```

  2. Assurez-vous que Rescuezilla termine correctement le processus de sauvegarde.
  3. Évitez de modifier la VM pendant le processus de sauvegarde.

7. Annexes

- **Commandes utiles** :
  - Vérifier l'espace disque : `df -h`.
  - Vérifier l'intégrité du disque : `sudo fsck /dev/sdX`.
  - Test des performances disque : `sudo hdparm -Tt /dev/sdX`.
- **Ressources supplémentaires** :
  - Documentation officielle Rescuezilla : https://rescuezilla.com/.

Temps de realisation

Linux

---

0. Installation de Linux Mint sur VMware

- **Temps pris : 2h**
- **Justification :** Inclut l'installation, les paramétrages initiaux, et les tests pour s'assurer que le système est prêt pour les configurations suivantes.

---

1. Mise à jour du système

- **Temps pris : 6h**
- **Justification :** Comprend les mises à jour, la configuration de mises à jour automatisées, les tests et les correctifs pour garantir la sécurité du système.

---

2. Désactivation des Services Non Nécessaires

- **Temps pris : 3h**
- **Justification :** Analyser, identifier et désactiver tous les services inutiles, tout en documentant les changements pour éviter les conflits.

---

3. Activation de l'Audit Système

- **Temps pris : 6h**
- **Justification :** Configurer l'audit système pour une surveillance détaillée, avec tests et vérifications des politiques d'audit.

---

4. Sécurisation de SSH

- **Temps pris : 2h**
- **Justification :** Mise en place de clés SSH, désactivation de l'accès root, modification des ports et tests de connexion sécurisés.

---

5. Configuration du Pare-feu UFW

- **Temps pris : 4h**
- **Justification :** Inclut des règles avancées, des tests approfondis pour le trafic entrant et sortant, et des ajustements basés sur des scénarios simulés.

---

6. Configuration des Règles iptables

- **Temps pris : 5h**
- **Justification :** Configurer et tester des règles complexes pour un contrôle strict du trafic réseau.

---

7. Installation de ClamAV et Lynis

- **Temps pris : 4h**
- **Justification :** Installation, configuration avancée, tests de scans et configuration des rapports automatisés.

---

8. Installation de fail2ban

- **Temps pris : 3h**
- **Justification :** Configurer fail2ban pour protéger contre les attaques par force brute et tester les scénarios d'attaque.

---

9. Désactivation de l'Exécution de Scripts dans /tmp

- **Temps pris : 2h**
- **Justification :** Modification des permissions pour renforcer la sécurité et tests d'impact sur les services système.

---

10. Stratégie de Sécurité Locale

- **Temps pris : 3h**
- **Justification :** Mise en place d'une stratégie de mots de passe, verrouillage de compte et audit des paramètres locaux.

---

11. Restriction d'Accès aux Journaux Système

- **Temps pris : 5h**
- **Justification :** Révision des permissions, documentation et tests d'accès aux journaux pour garantir leur intégrité.

---

12. Restriction des Droits sur les Fichiers Sensibles

- **Temps pris : 3h**
- **Justification :** Configuration des permissions sur des fichiers critiques et tests pour s'assurer qu'ils ne sont accessibles qu'aux utilisateurs autorisés.

---

13. Déploiement de Logiciel

- **Temps pris : 6h**
- **Justification :** Mise en place de scripts pour déployer des logiciels de manière automatisée, avec tests sur différents environnements.

---

14. Masterisation du Poste Linux

- **Temps pris : 5h**
- **Justification :** Création d'une image système prête à l'emploi, tests de restauration et documentation pour la réplication sur d'autres machines.

Résumé des temps révisés

Tâche	Temps (h)
Installation de Linux Mint sur VMware	2h
Mise à jour du système	6h
Désactivation des Services Non Nécessaires	3h
Activation de l'Audit Système	6h
Sécurisation de SSH	2h
Configuration du Pare-feu UFW	4h
Configuration des Règles iptables	5h
Installation de ClamAV et Lynis	4h
Installation de fail2ban	3h
Désactivation de l'Exécution de Scripts dans /tmp	2h
Stratégie de Sécurité Locale	3h
Restriction d'Accès aux Journaux Système	5h
Restriction des Droits sur les Fichiers Sensibles	3h
Déploiement de Logiciel	6h
Masterisation du Poste Linux	5h
Total	**75h**

Windows

---

0 : Création d'une machine virtuelle (VM) dans VMware

- **Temps pris : 2h**

- **Justification :** Inclut la création de la VM, la configuration initiale et les tests pour garantir que l'environnement est prêt pour les prochaines étapes.

---

0 bis : Installation du VMware Tools

- **Temps pris : 1h**
- **Justification :** Installer et configurer VMware Tools pour améliorer les performances et la compatibilité avec le système hôte.

---

1 : Paramètres biométriques et d'écran de verrouillage

- **Temps pris : 4h**
- **Justification :** Configurer des paramètres avancés pour la reconnaissance faciale, le verrouillage de l'écran, et effectuer des tests approfondis.

---

2 : DNS et Sécurité Réseau

- **Temps pris : 6h**
- **Justification :** Configurer les paramètres DNS, désactiver les protocoles non sécurisés, tester la connectivité et documenter les configurations.

---

3 : Sécurité des mots de passe et de l'authentification

- **Temps pris : 6h**
- **Justification :** Configurer les politiques de mots de passe et d'authentification, y compris Kerberos, avec tests sur plusieurs comptes.

---

4 : Protection réseau

- **Temps pris : 5h**
- **Justification :** Configurer les protections de réseau, notamment les signatures SMB/LDAP et les restrictions réseau spécifiques.

---

5 : Configuration de Windows Defender

- **Temps pris : 5h**
- **Justification :** Configurer Windows Defender, activer les protections avancées et effectuer des scans pour tester l'efficacité.

---

6 : Sécurisation de MS Office

- **Temps pris : 4h**
- **Justification :** Configurer les paramètres de sécurité avancés pour protéger contre le phishing et les malwares dans les applications Office.

---

7 : Journalisation des événements Windows

- **Temps pris : 5h**
- **Justification :** Configurer les journaux, augmenter leur taille, activer la journalisation des commandes et vérifier leur fonctionnement.

---

8 : Mesures de sécurité avancées

- **Temps pris : 5h**
- **Justification :** Inclut la configuration de PowerShell sécurisé, des blocs de scripts et des politiques d'audit.

---

9 : Sécurisation de lsass

- **Temps pris : 3h**
- **Justification :** Renforcer lsass contre les vols d'informations d'identification, avec tests pour garantir la stabilité.

---

10 : Gestion des applications

- **Temps pris : 3h**
- **Justification :** Désinstaller les applications inutiles et configurer les restrictions pour limiter l'installation de nouvelles applications.

---

11 : Pare-feu et Blocage des Connexions

- **Temps pris : 5h**
- **Justification :** Configurer les règles avancées du pare-feu et bloquer les binaires spécifiques (LOLBins), avec des tests.

---

12 : Gestion des mises à jour Windows et AutoRun

- **Temps pris : 4h**

- **Justification :** Configurer les mises à jour automatiques, désactiver AutoRun, et tester le comportement des périphériques.

---

13 : Création d'un utilisateur standard pour la mise en production

- **Temps pris : 3h**
- **Justification :** Créer des utilisateurs standard, configurer leurs permissions et tester leur accès.

---

14 : Installation des logiciels pour Windows 10

- **Temps pris : 5h**
- **Justification :** Installer et configurer les logiciels nécessaires avec des scripts automatisés pour accélérer les déploiements.

---

15 : Masterisation du poste Windows 10

- **Temps pris : 6h**
- **Justification :** Créer une image système, tester la restauration et documenter les étapes pour une réplication facile.

---

16 : Chiffrement de disque avec BitLocker

- **Temps pris : 4h**
- **Justification :** Activer et configurer BitLocker, tester le déverrouillage avec TPM et les clés de récupération.

---

17 : Activation de la clé Windows 10

- **Temps pris : 1h**
- **Justification :** Activer Windows avec une clé valide, vérifier l'activation et documenter le processus.

Résumé des temps ajustés

Tâche	Temps (h)
Création d'une machine virtuelle	2h
Installation du VMware Tools	1h
Paramètres biométriques et écran	4h
DNS et Sécurité Réseau	6h
Sécurité des mots de passe	6h
Protection réseau	5h
Configuration de Windows Defender	5h
Sécurisation de MS Office	4h
Journalisation des événements	5h
Mesures de sécurité avancées	5h
Sécurisation de lsass	3h
Gestion des applications	3h
Pare-feu et Blocage des Connexions	5h
Gestion des mises à jour et AutoRun	4h
Création d'un utilisateur standard	3h
Installation des logiciels	5h
Masterisation du poste Windows	6h
Chiffrement de disque avec BitLocker	4h
Activation de la clé Windows	1h
Total	**75h**