

Cours Installation Windows 11

Ecrit par Youenn DUVAL

Mail: youenn@barbed.fr

Linkedin: [Youenn DUVAL](#)

Dernière mise à jour : **21/10/2024**

Table des matières

1. [Prérequis](#)
2. [Création de la VM](#)
3. "Quelques" définitions
 1. [Fichier](#)
 2. [Dossier ou Répertoire:](#)
 3. [Explorateur Windows](#)
 4. [Droits des dossiers et fichier en NTFS](#)
 5. [Les extensions sous Windows](#)
 6. [Les fichiers cachés](#)
 7. [Panneau de configuration](#)
 8. [Centre de réseau et partage](#)
 9. [Programmes et fonctionnalités](#)
 10. [Comptes d'utilisateurs](#)
 1. [Utilisateurs et groupes via la Gestion de l'ordinateur.](#)
 11. [Les services](#)
 12. [Informations Systèmes](#)
 13. "Gestion de l'ordinateur"
 14. [Observateur d'évènement](#)
 15. [Gestionnaire de périphériques](#)
 16. [Gestion des disques](#)
 17. [Table des registres](#)
 18. [Windows Defender](#)
 19. [Firewall](#)
 1. [Zones Public et Privé du Pare-feu](#)
 20. [Gestionnaire des tâches](#)
 21. [Démo Couper Explorer.exe et le relancer](#)
 22. [Applications de démarrage](#)
 23. [Exécuter](#)
 24. [Gestion des Paths](#)
 25. [Quelques raccourcis clavier](#)
 26. [Bitlocker](#)
4. [Les backups](#)
5. [Ajouter un disque dans Win11](#)
6. [Créer un volume de sauvegarde](#)
 1. [D'autres outils de sauvegarde](#)
7. [Le Raid](#)
8. [Créer un RAID 1 logiciel sous W11](#)
 1. [Créer 2 disques dans votre VM](#)
 2. [Les disques dans le gestionnaire de disque de W11](#)
 3. [Détruirez un disque!](#)
 4. [Reconstruire le Raid](#)
9. [Invite de commande](#)
 1. [Une liste non exhaustive de commandes DOS régulièrement utilisées](#)

2. [Scripting Bash](#)
10. [Powershell et le terminal](#)
 1. [Scripting Powershell](#)
 2. [Des commandes utile](#)
 3. [Le piping](#)
 4. [Manipulation d'une commande et d'objet Powershell](#)
 1. [Utilisons la commande `get-process`](#)
 2. [Comprendre get-process `get-help get-process`](#)
 3. [Rajoutons des paramètres `get-process explorer`](#)
 4. [format-list -Property *`|Piping et changement de format `get-process explorer | format-list -Property *](#)
 5. [Sort-Object -Property CPU -Descending`|Piping et Tri d'objets `Get-Process | Sort-Object -Property CPU -Descending`](#)
 6. [Sort-Object -Property CPU -Descending.| Select-Object -First 5 -Property ID, ProcessName`|On rajoute un filtre pour ne voir que les 5 premiers objets `Get-Process | Sort-Object -Property CPU -Descending.| Select-Object -First 5 -Property ID, ProcessName`](#)
 7. [On transforme cette commande en script](#)
 8. [Tester le script `.\test.ps1`](#)
 9. [Autoriser l'exécution de script non signé](#)
 5. [Exemple de Script plus complet](#)
11. [Spécifier le chemin du dossier à analyser](#)
12. [Lister tous les fichiers et dossiers dans le chemin spécifié](#)
13. [Afficher les noms et la taille de chaque élément](#)
 1. [Exercice Script Powershell](#)
14. [Windows en milieu Professionnel](#)
 1. [Les problématique d'une entreprise](#)
 2. [Active Directory](#)
 3. [Les avantages](#)

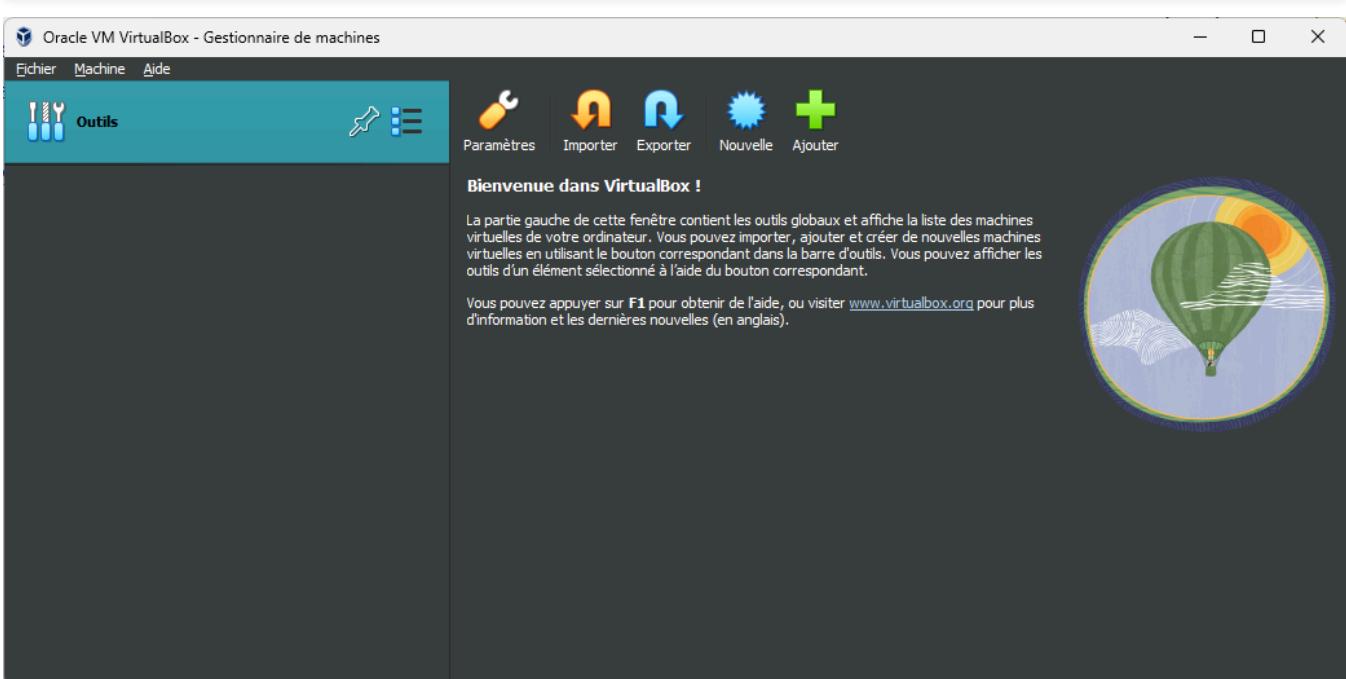
Prérequis

- Installer VirtualBox (à télécharger sur leur site, la dernière version)
- Télécharger ISO Windows 11 (Version Entreprise ou pro, Microsoft les fournit gratuitement pour des tests de 90 jours)

Création de la VM

Todo

Dans VirtualBox, sélectionnez Outils puis "Nouvelle"



Todo

Décochez Skip Unattended Installation

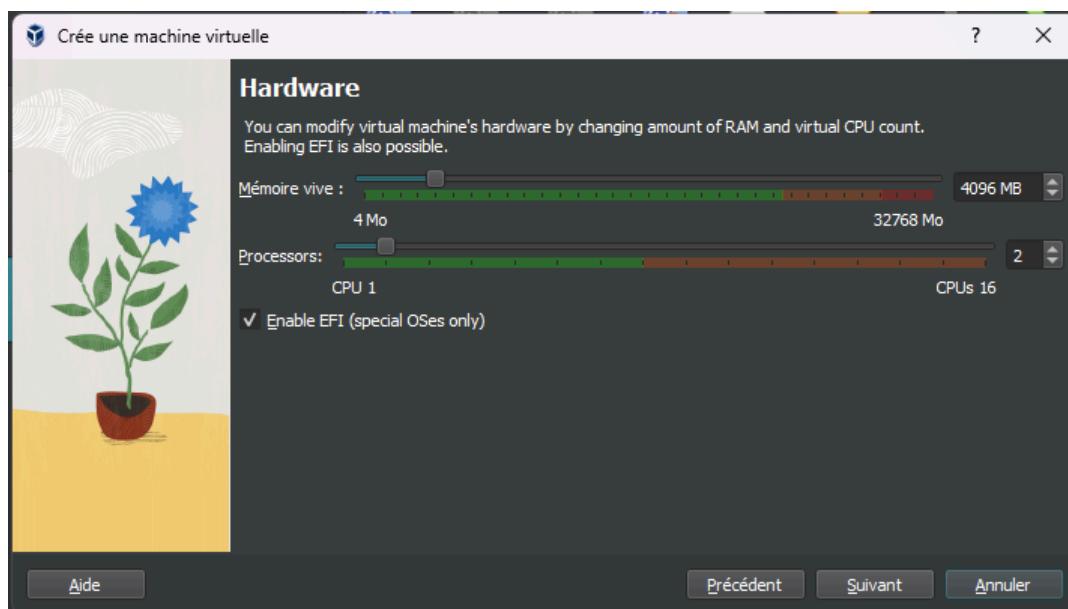
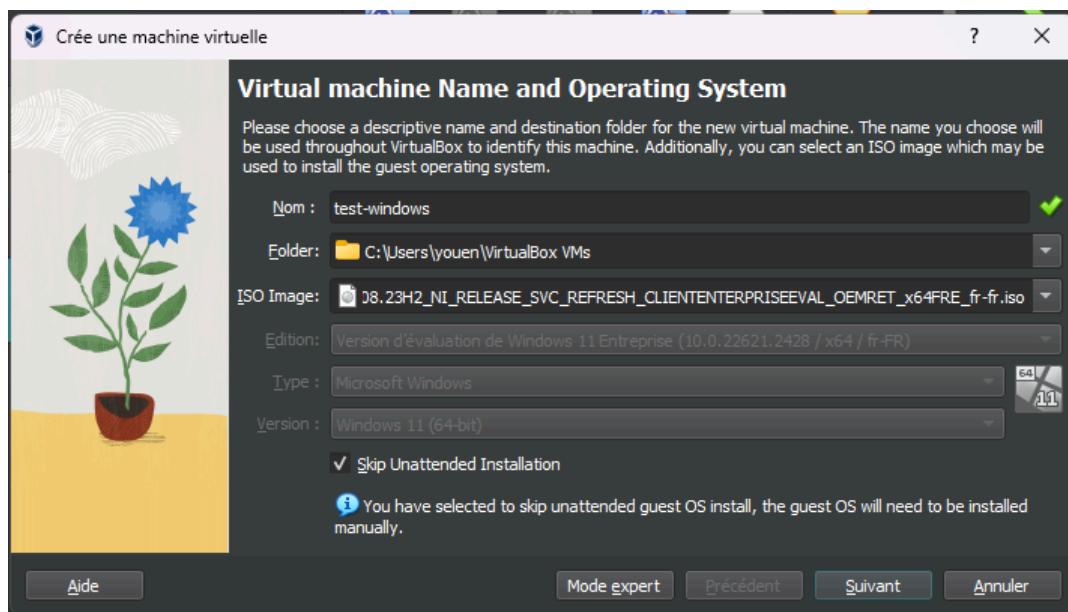
💡 Unattended Installation

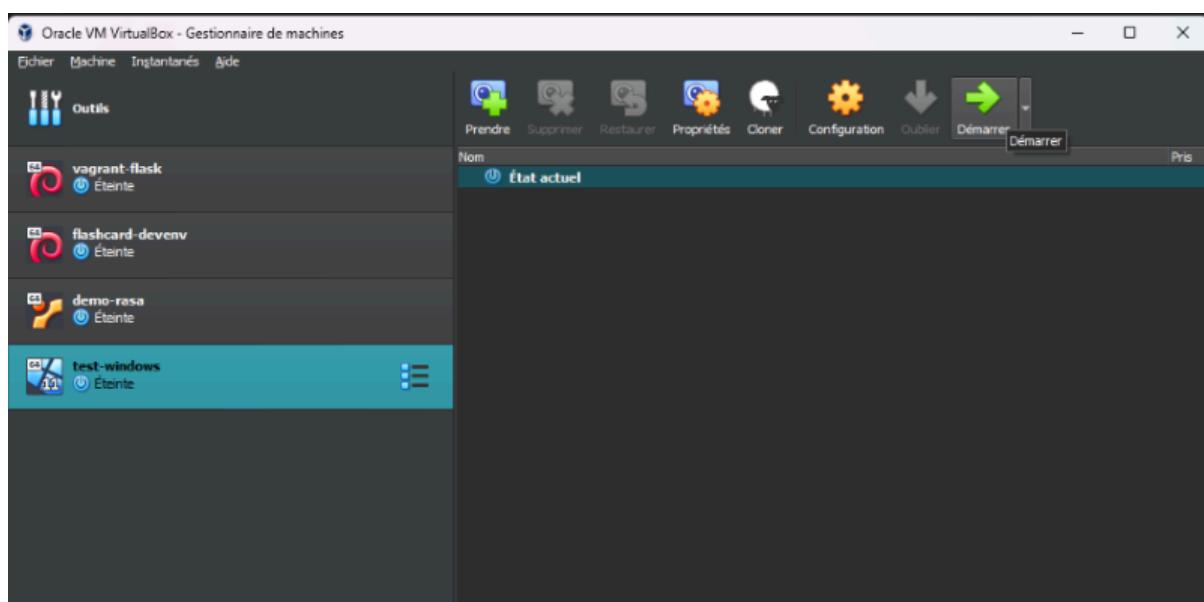
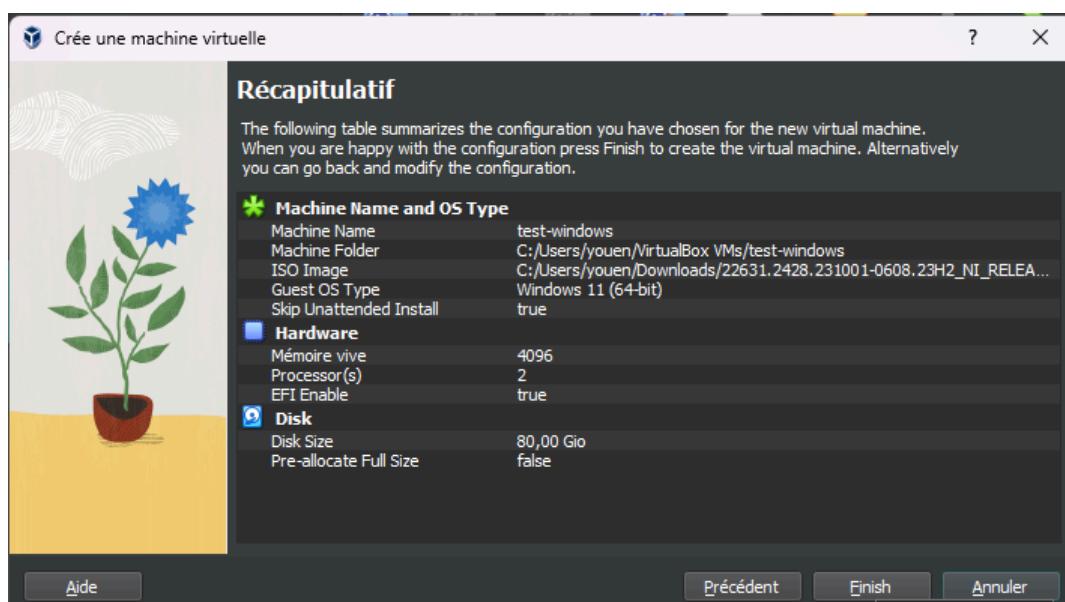
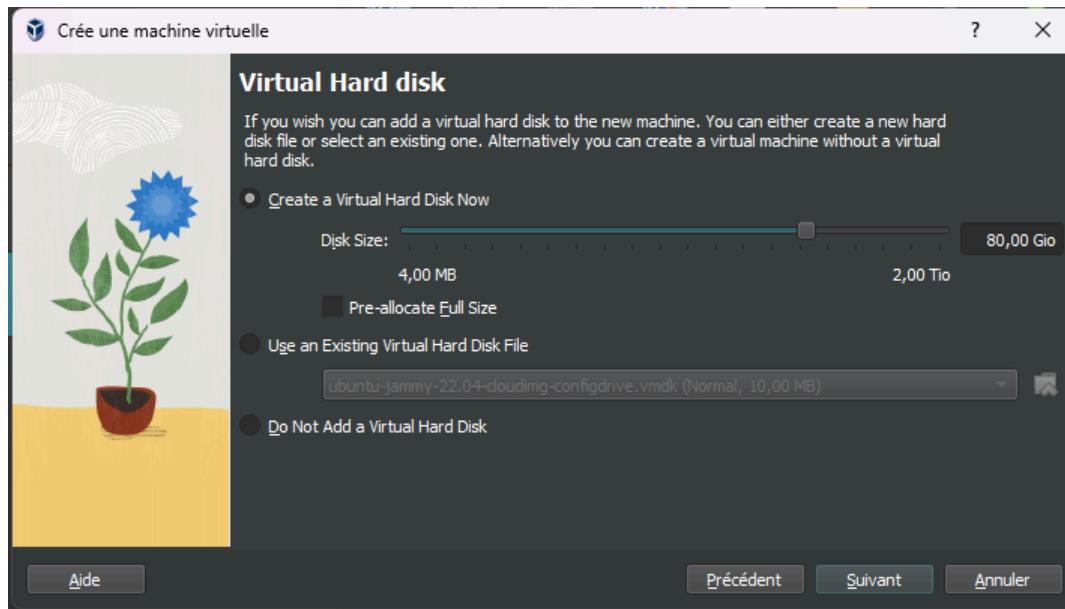
Cela permet d'installer des OS avec des fichiers XML prérempli qui permettra d'éviter d'avoir des menu à remplir à la main.

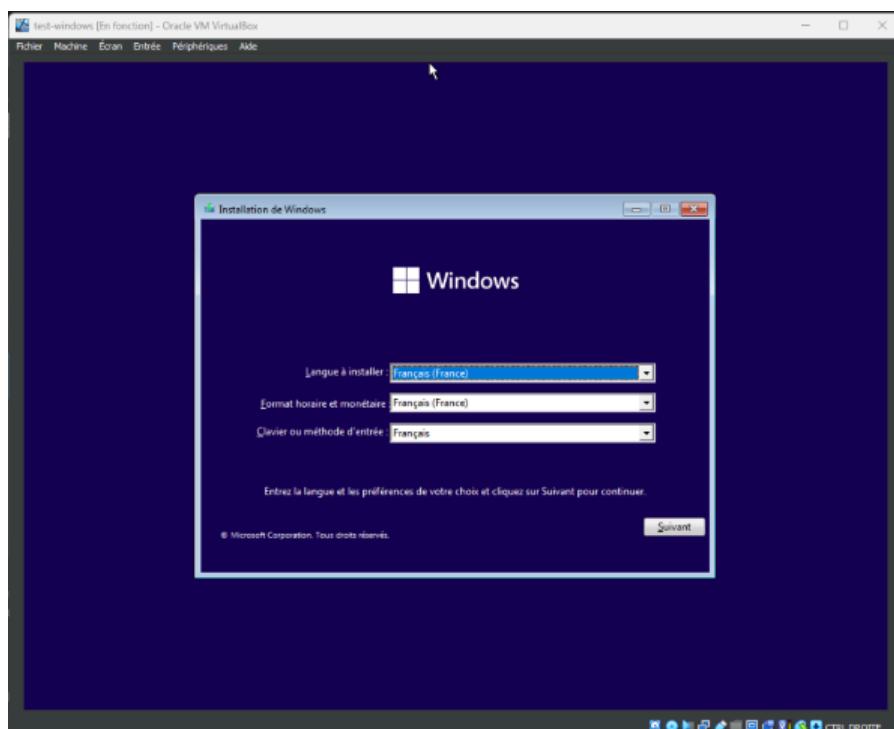
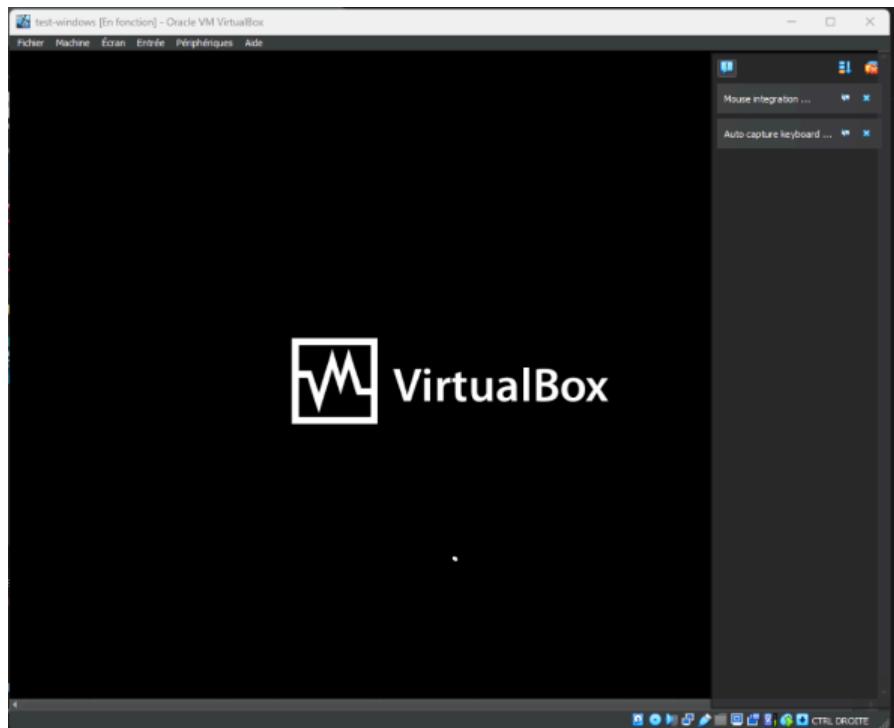
On retrouve cela souvent en entreprise

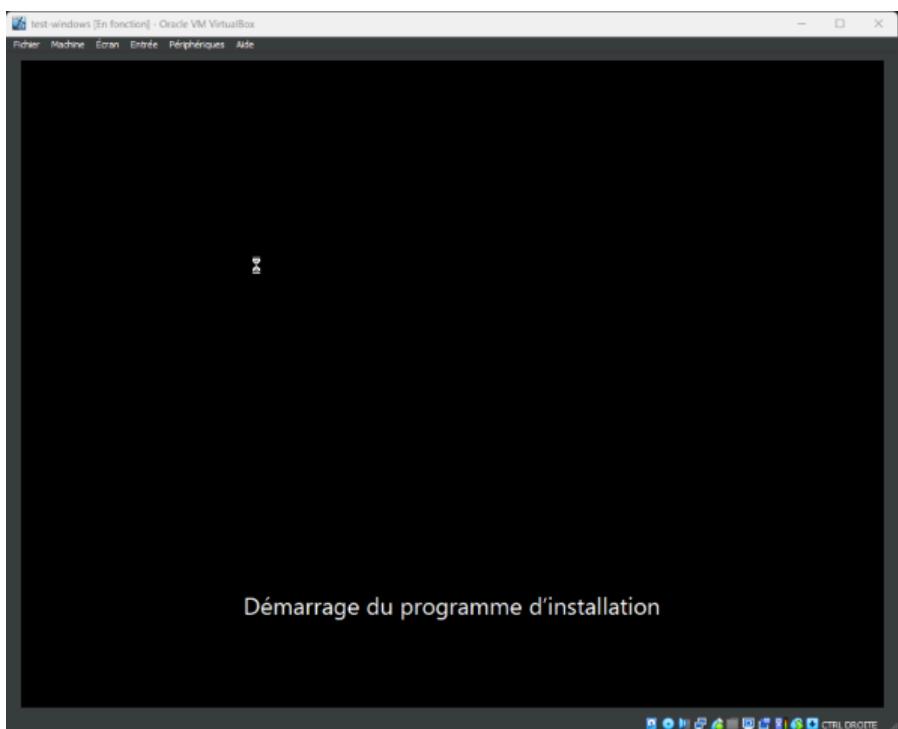
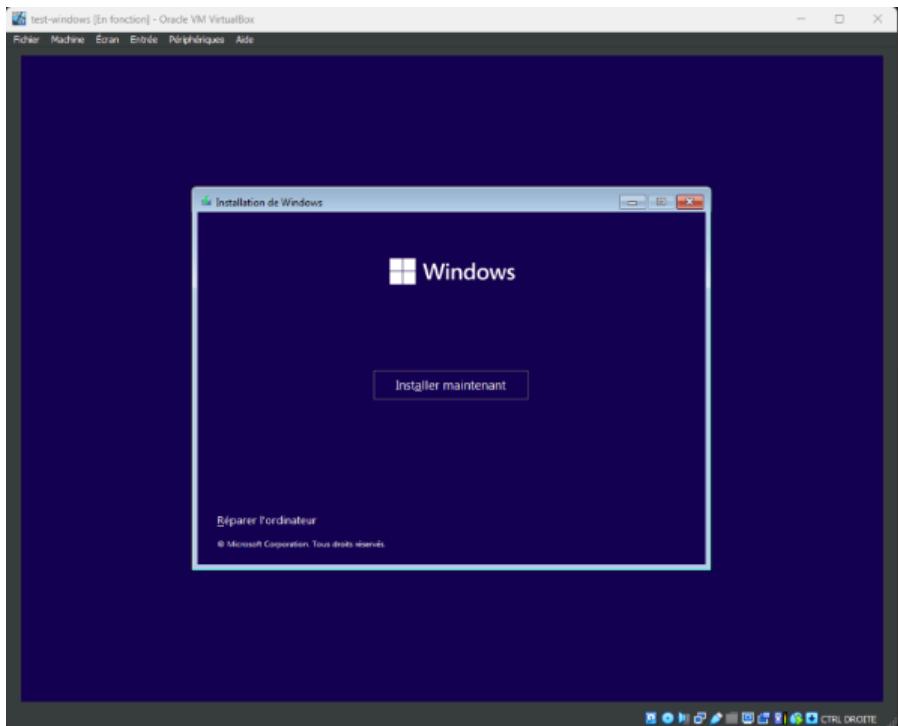
S

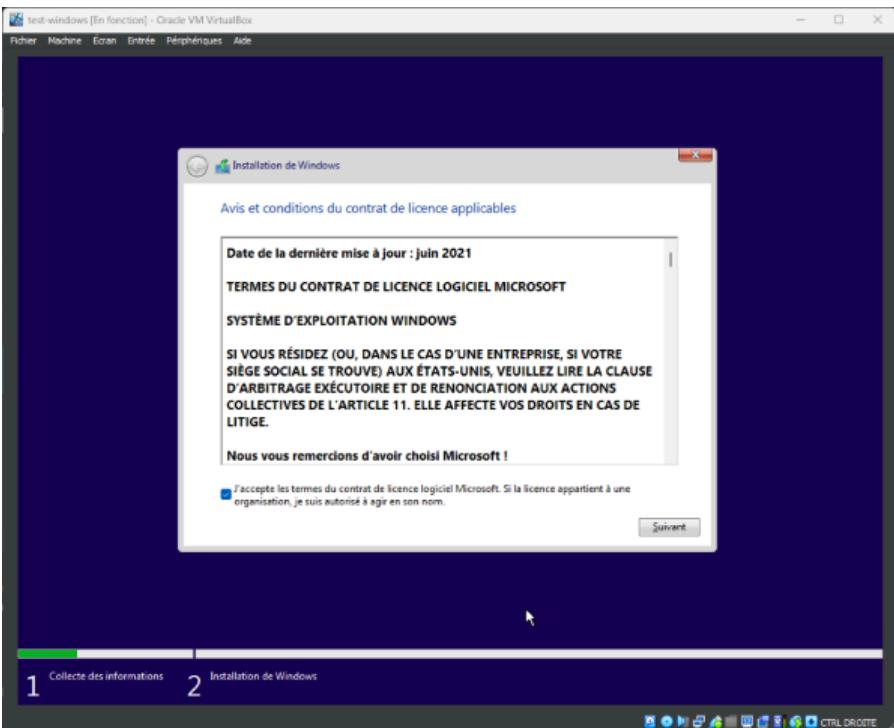
Si vous souhaitez par exemple générer une clef USB d'installation avec des données d'installation préremplie, vous pouvez utiliser l'outil [Rufus](#). Il générera alors les fichiers pour une clef USB.



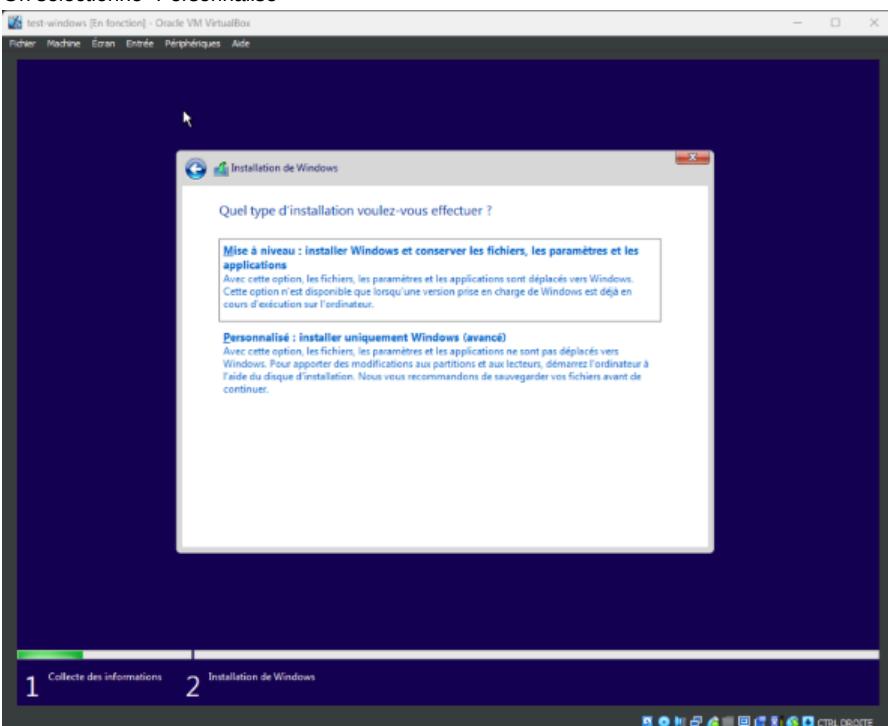


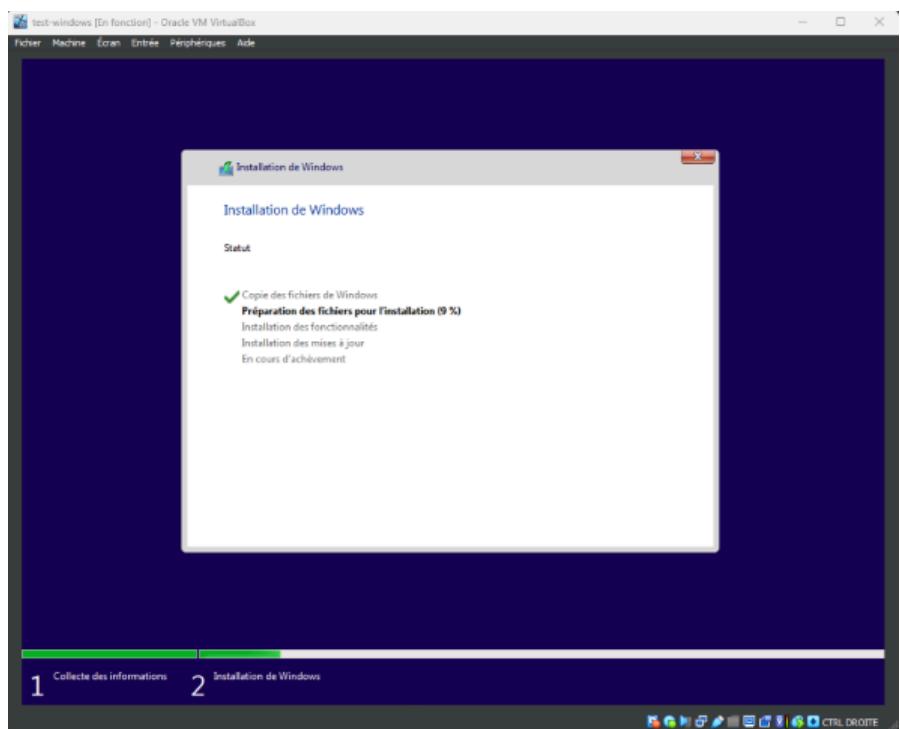
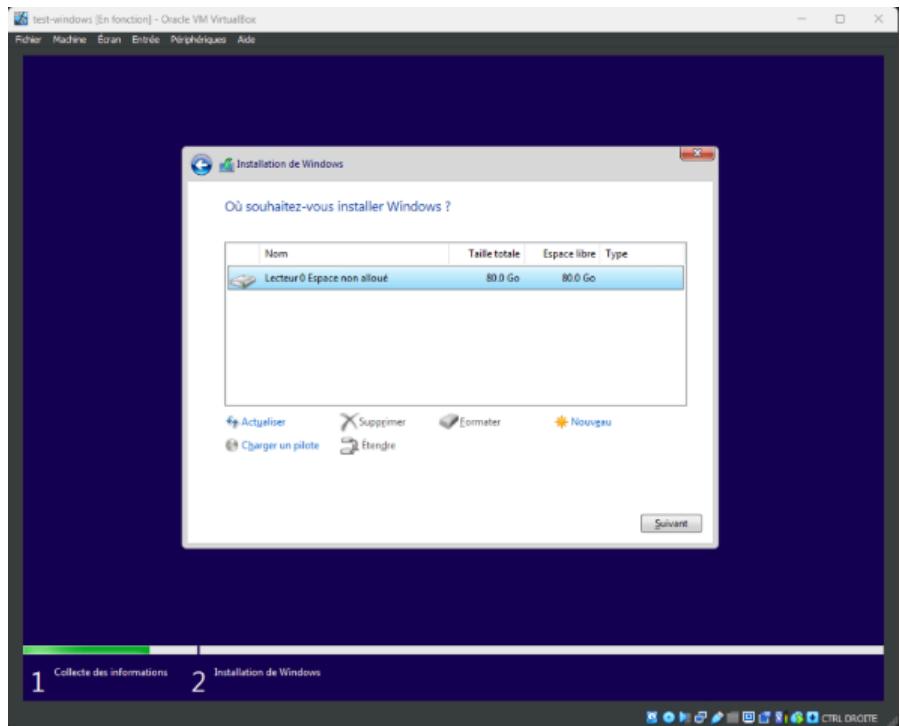


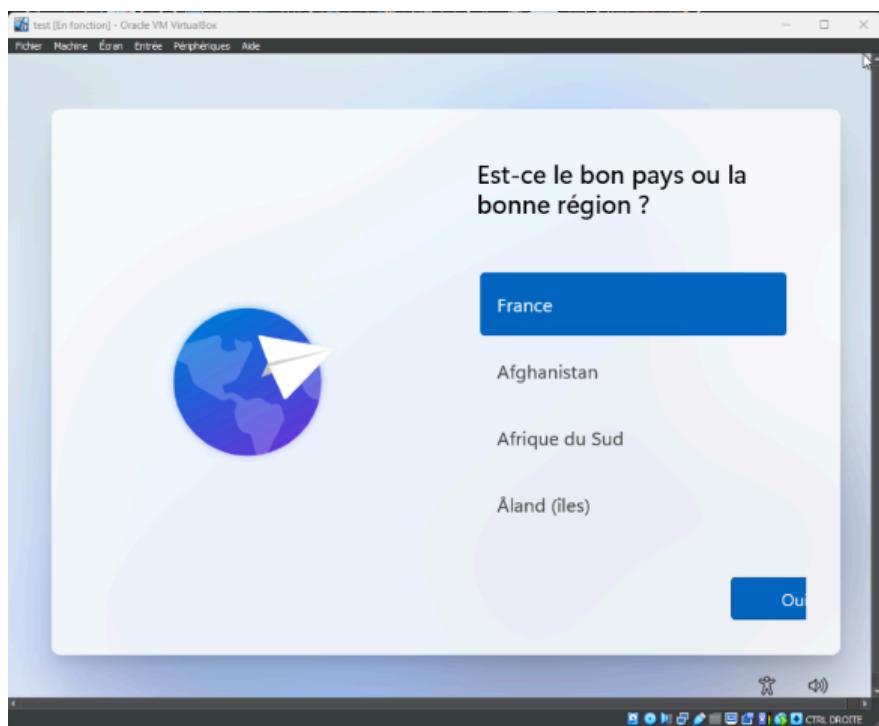
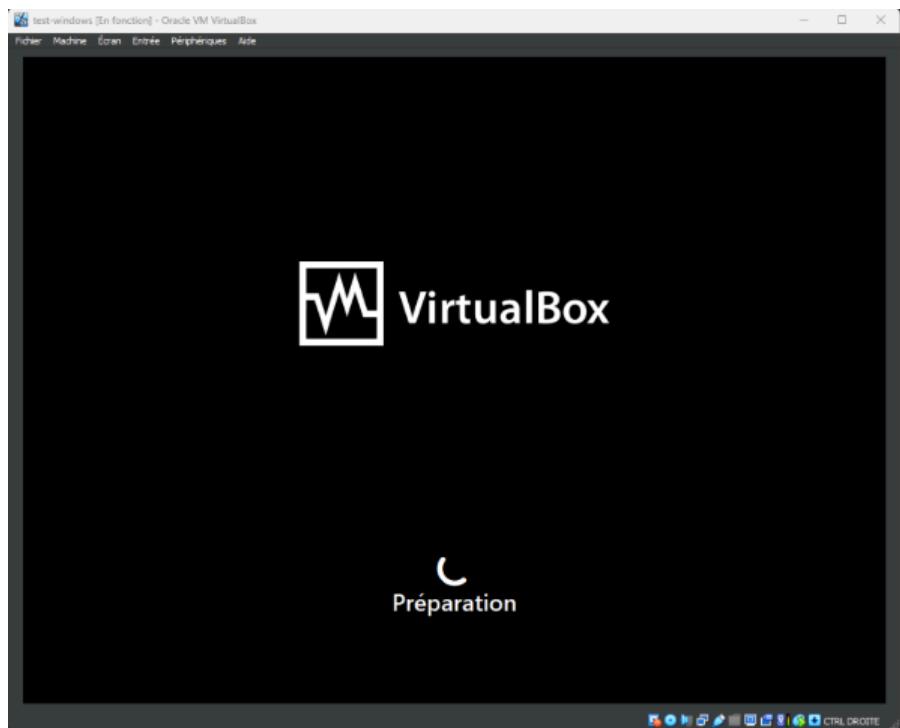


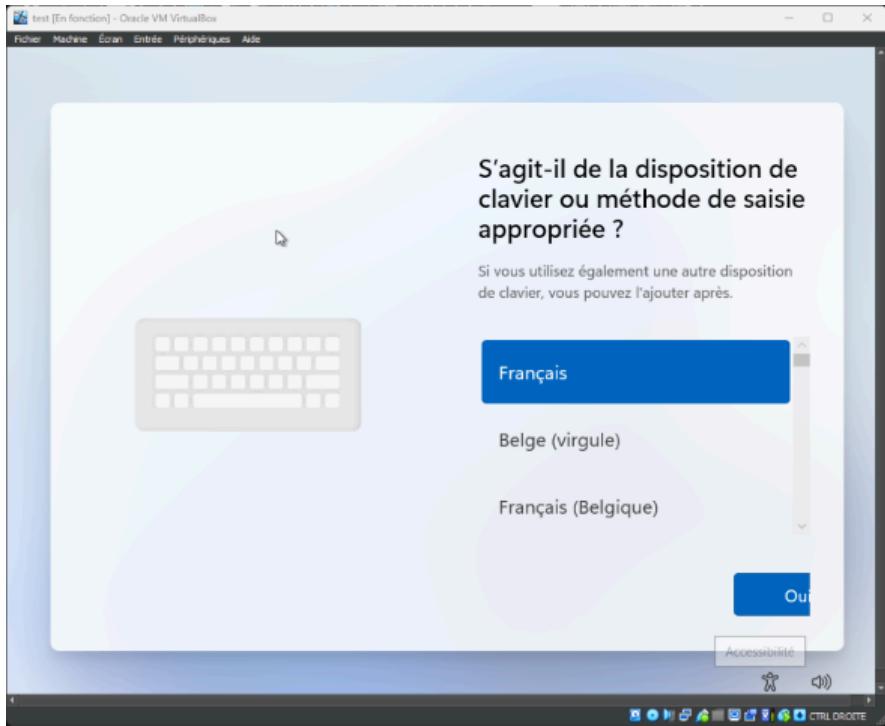


On sélectionne "Personnalisé"



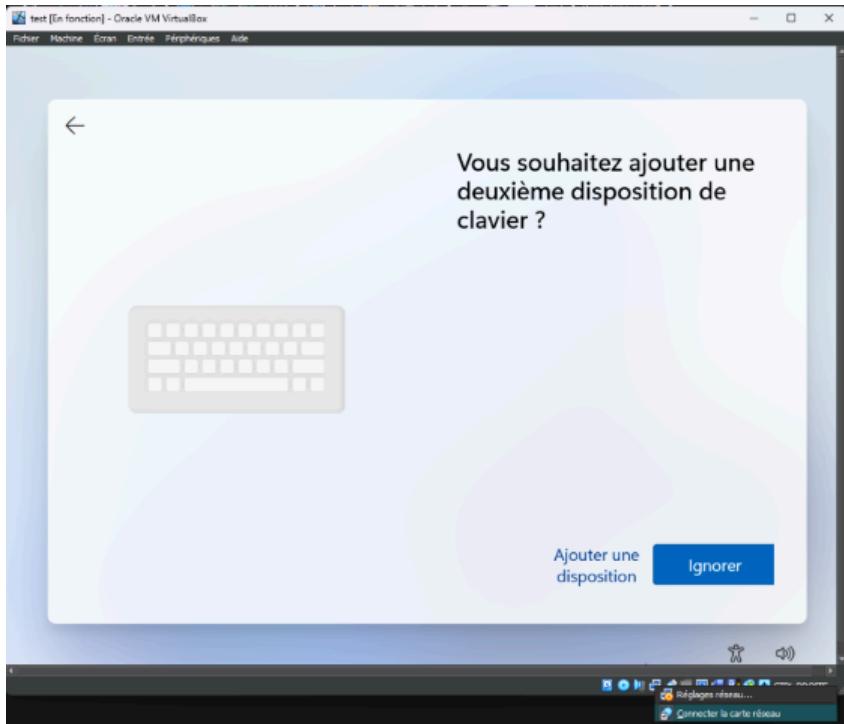


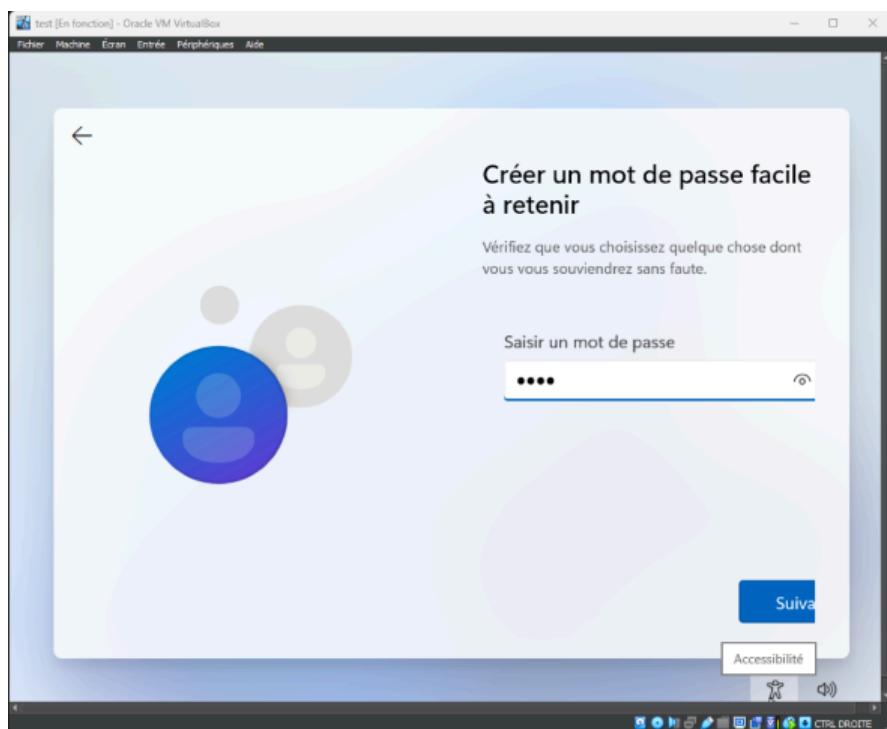
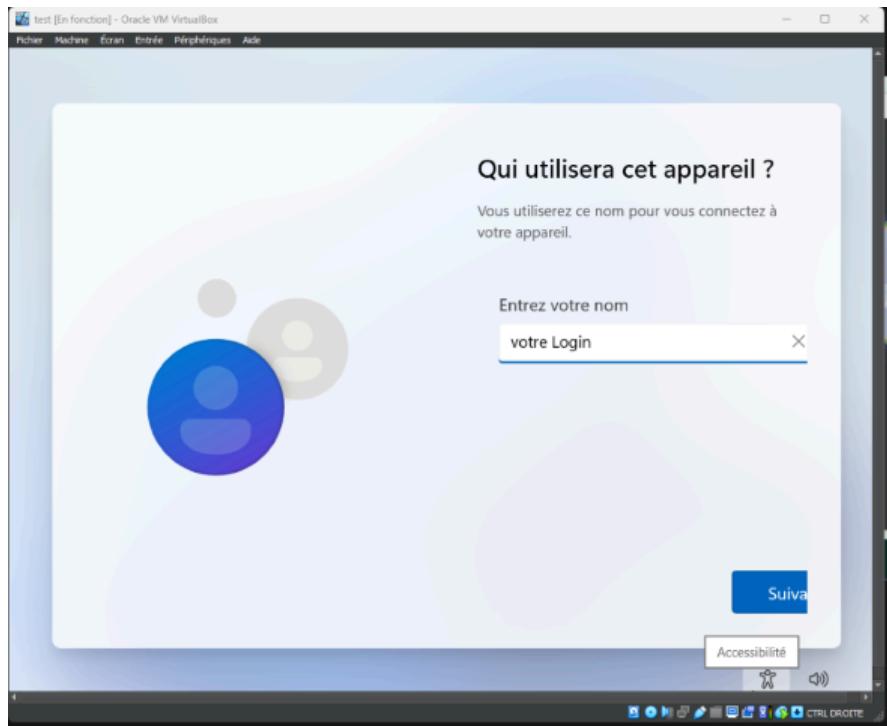


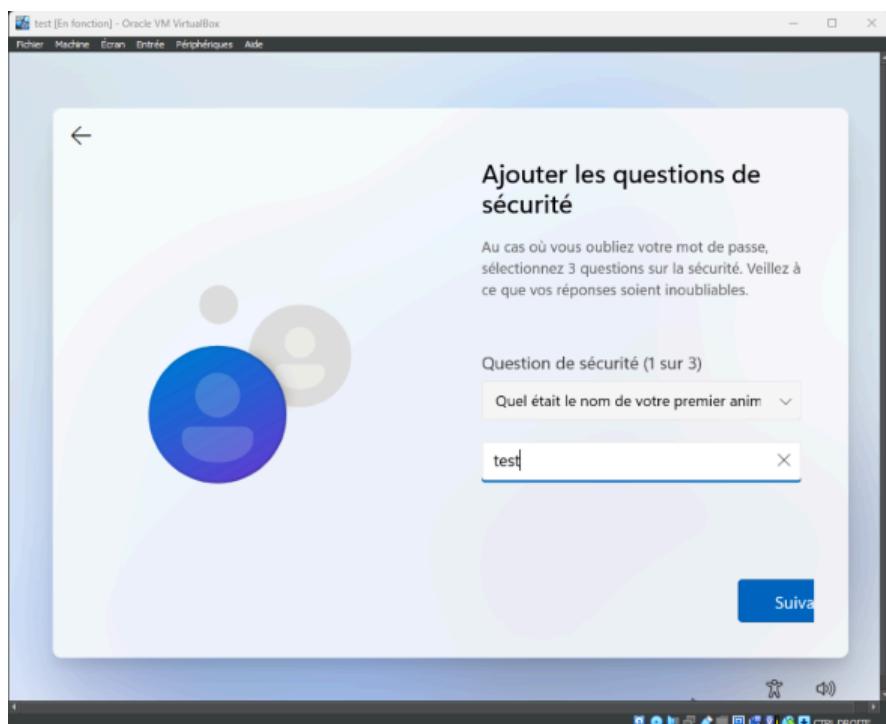
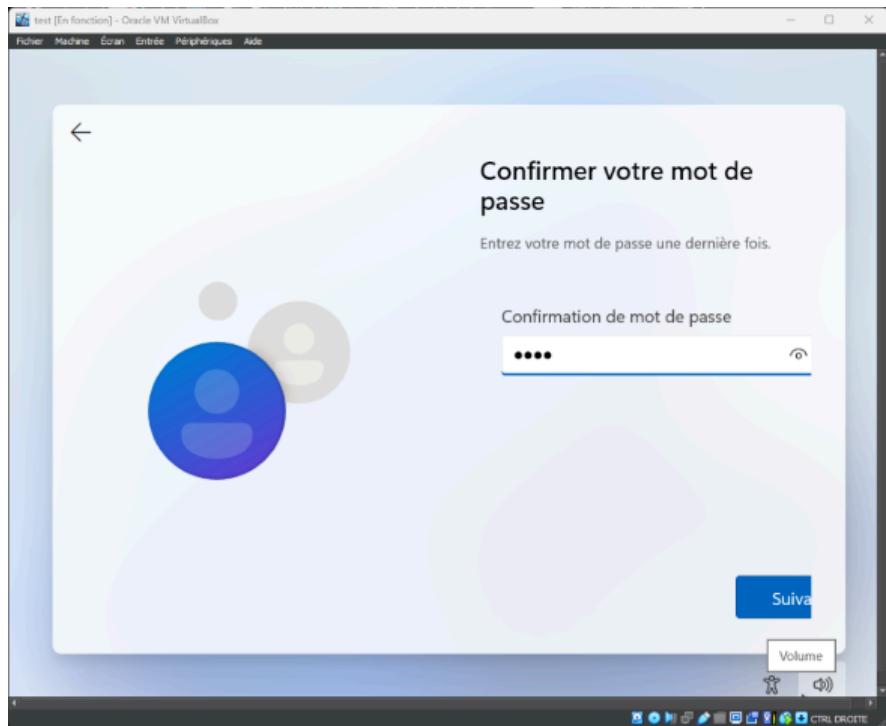


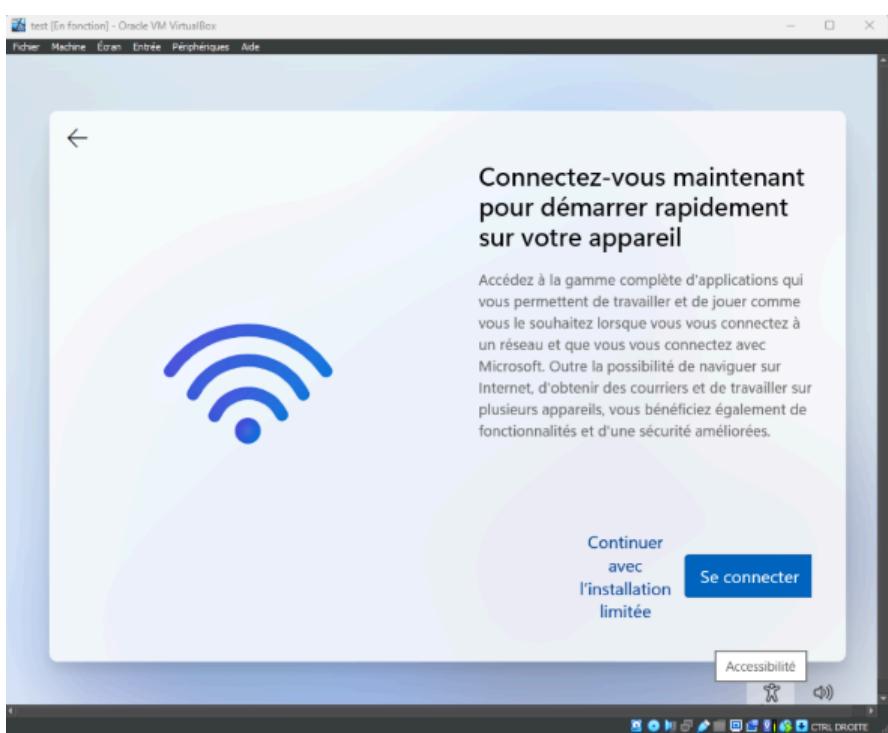
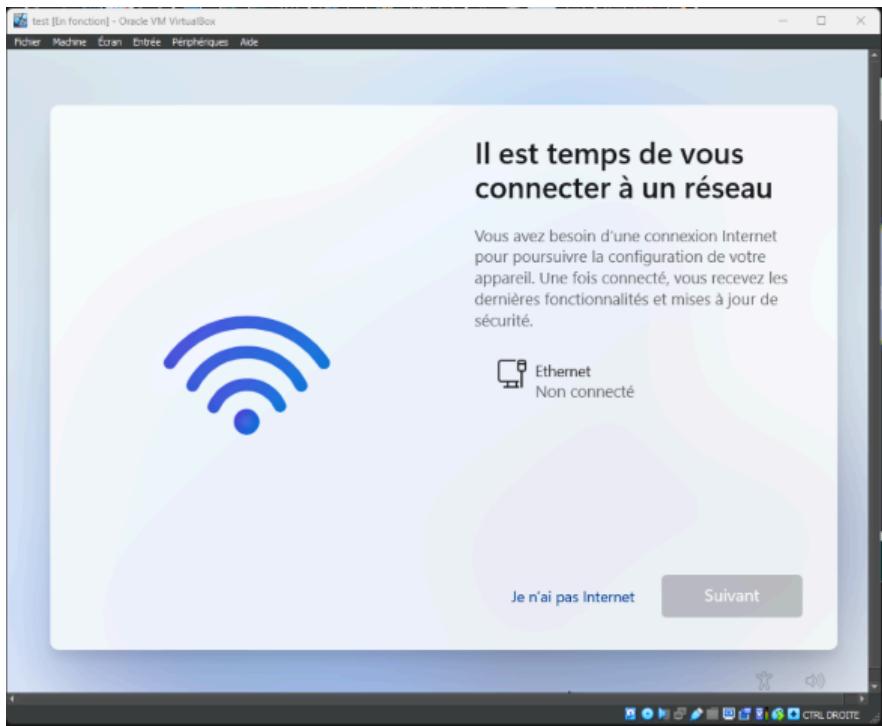
➊ Todo

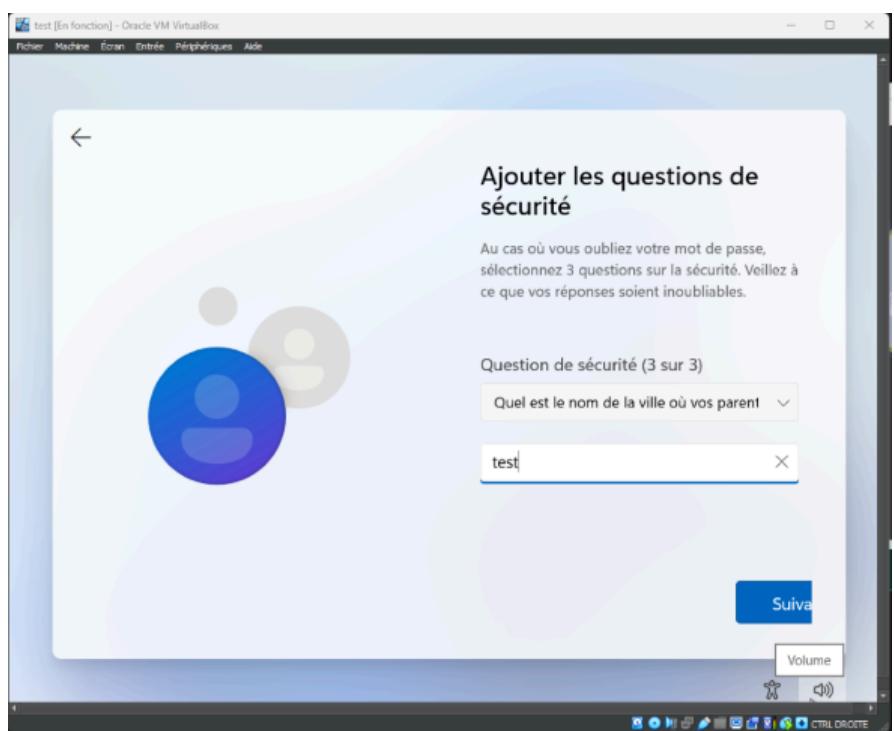
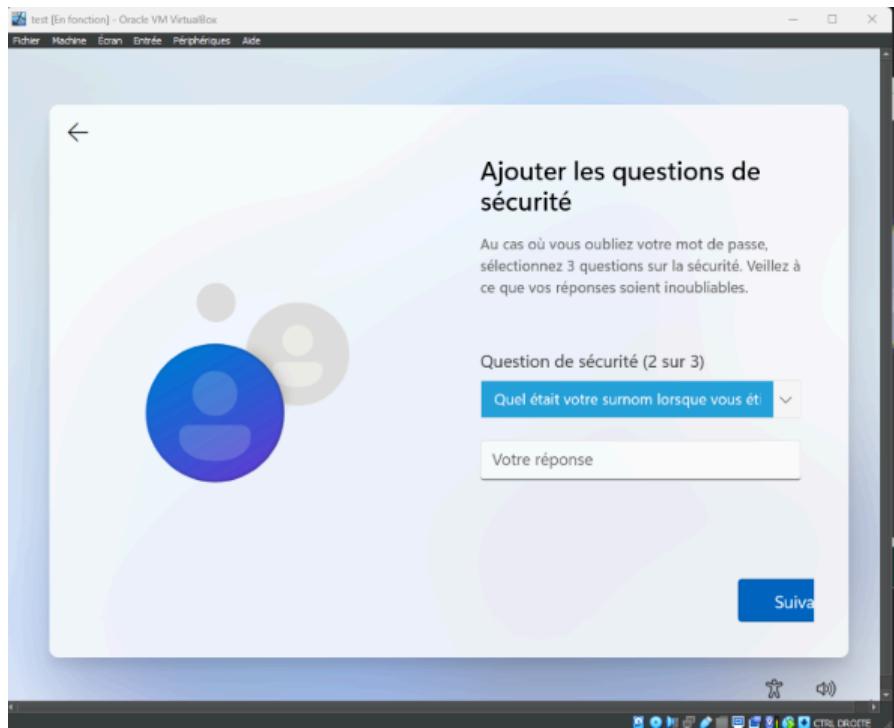
Regardez en bas à droite et cliquez sur **Connecter la carte réseau** (click droit pour ouvrir le menu). Cela va couper le réseau à la VM et empêcher l'installation de Windows de chercher internet et de vous forcer à créer un compte en ligne dans l'écran suivant.

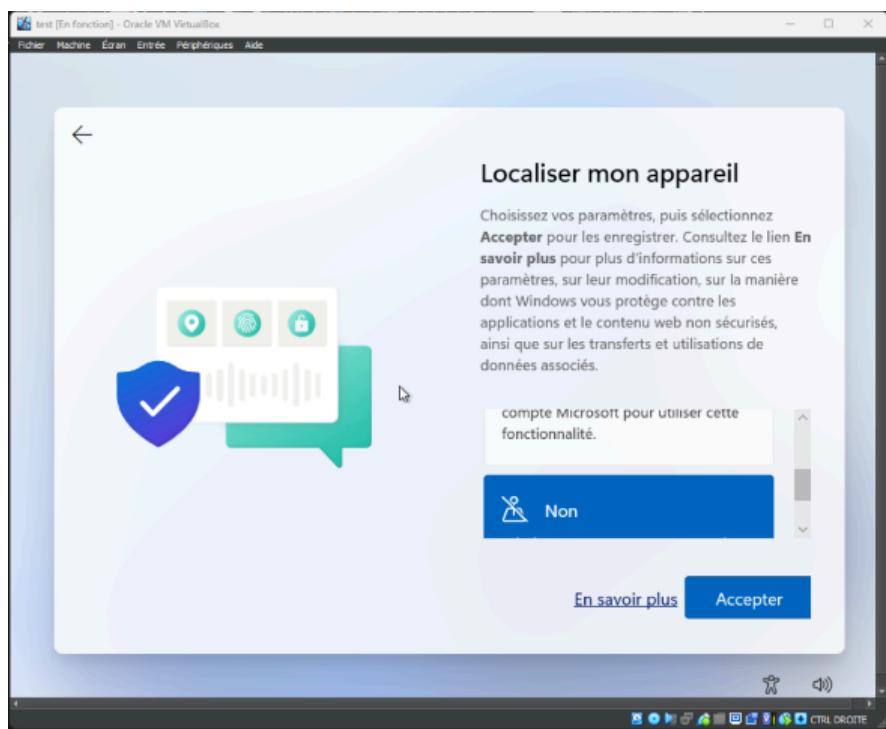
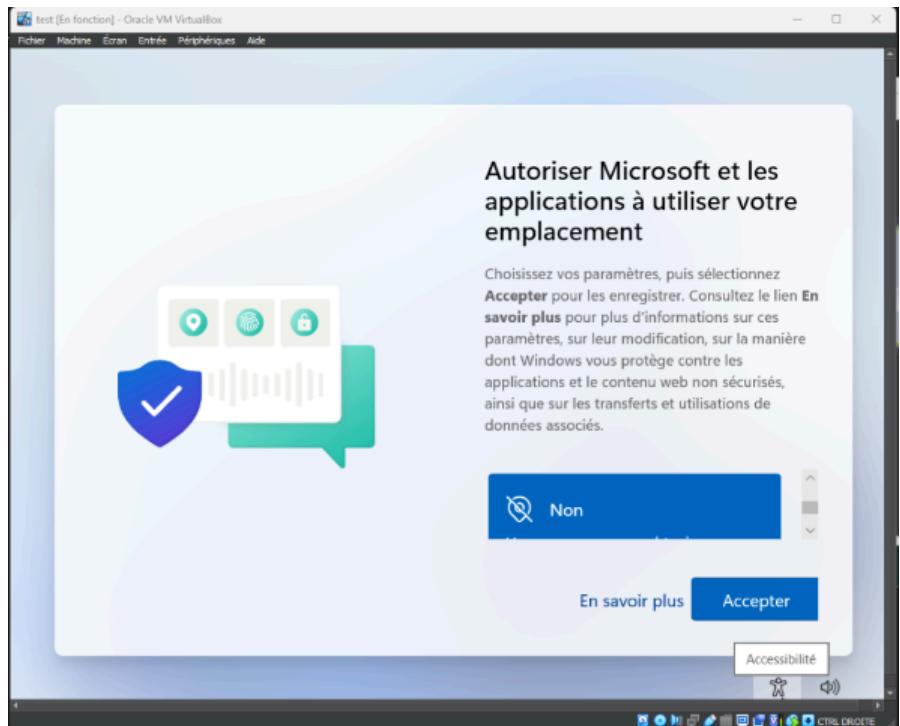


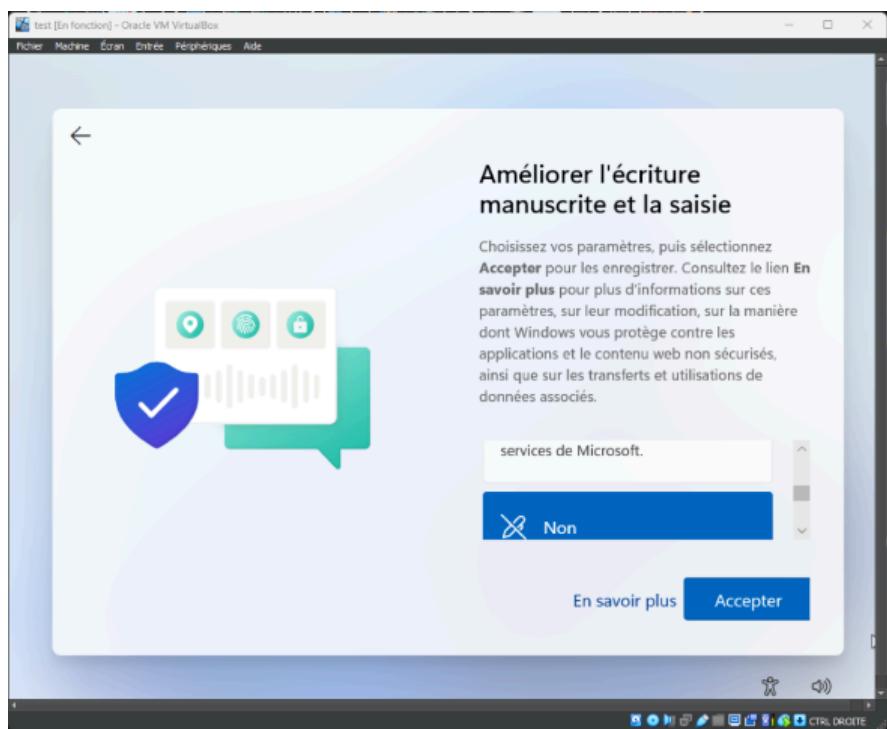
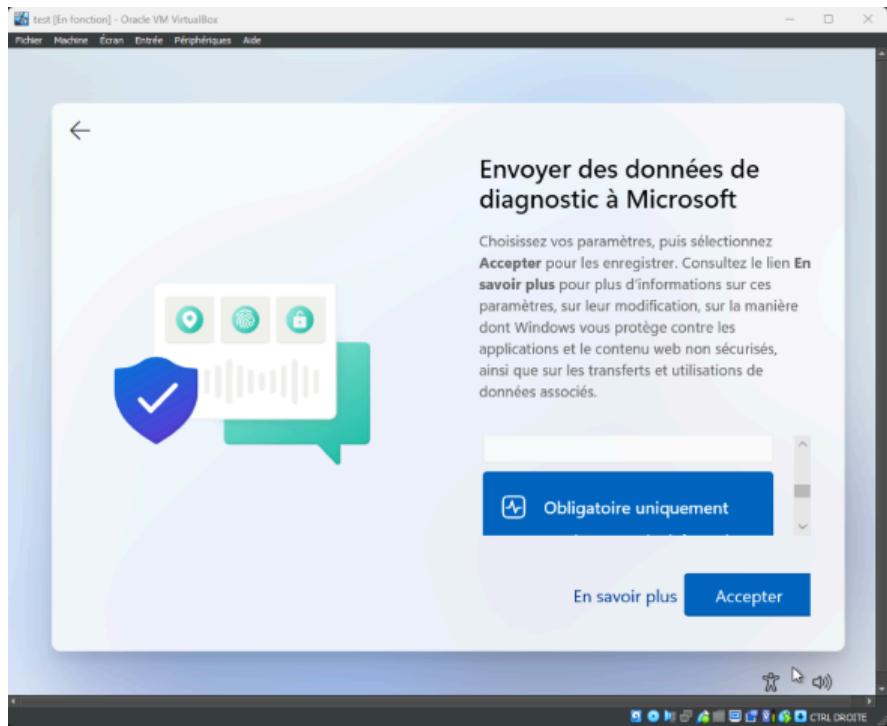


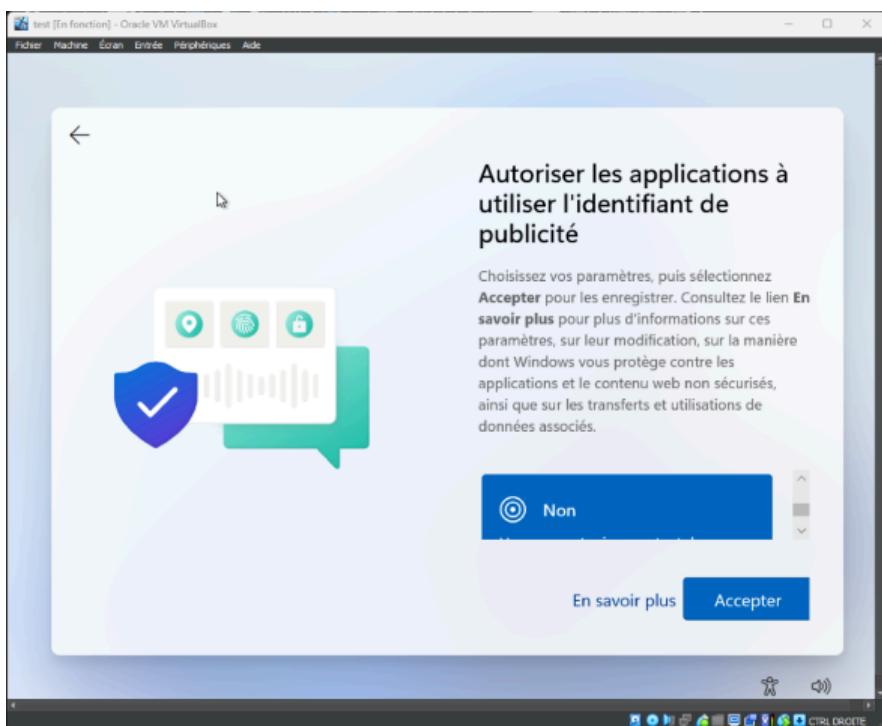
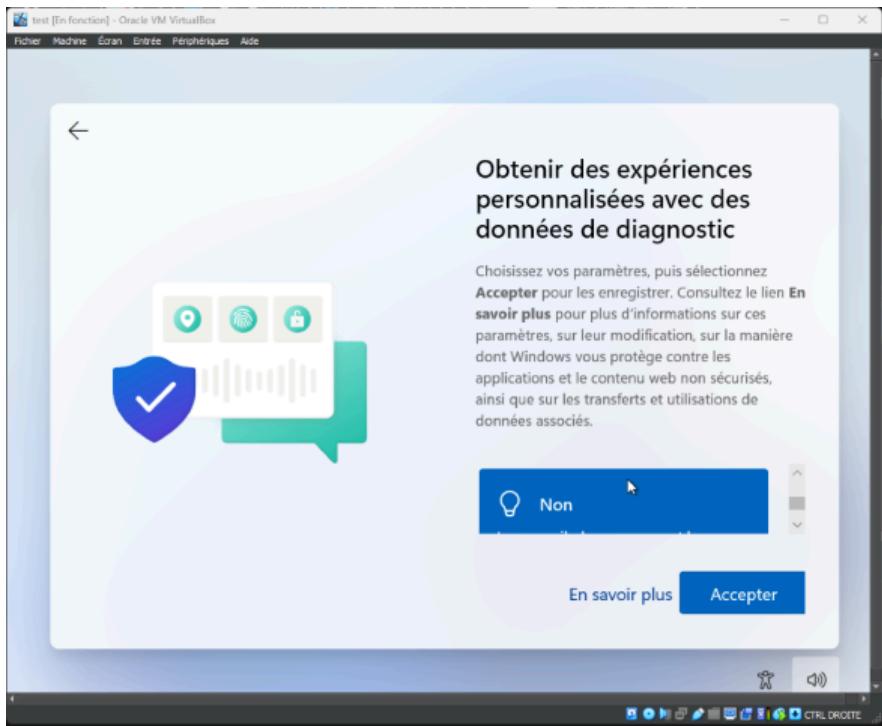






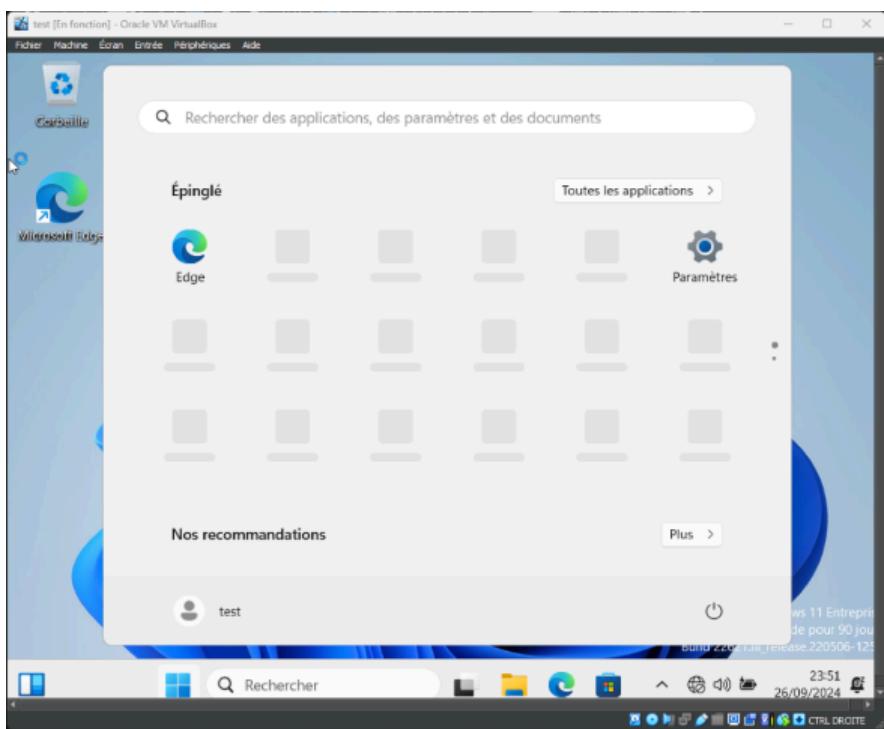
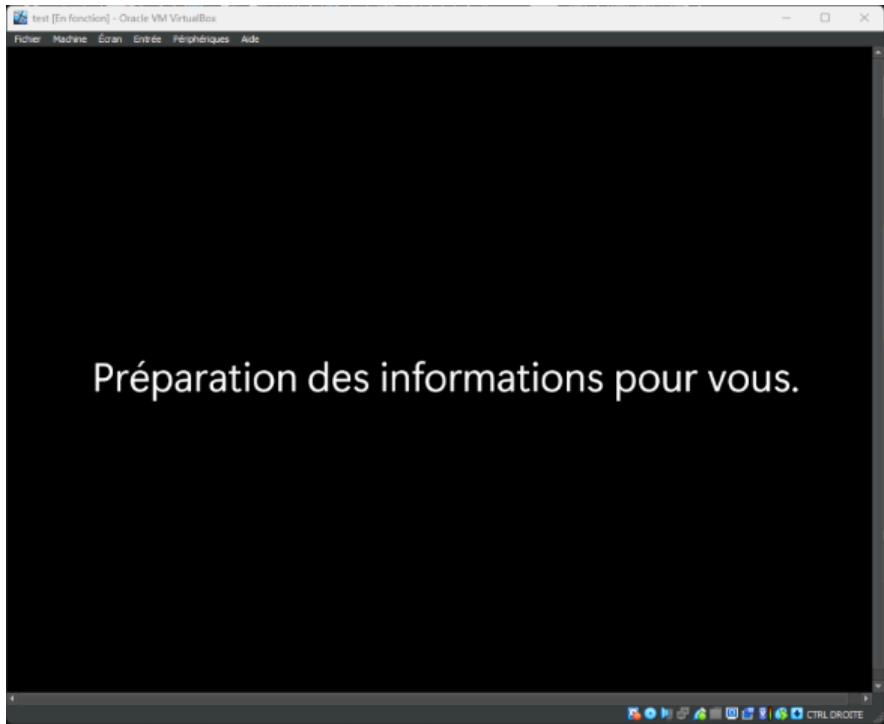






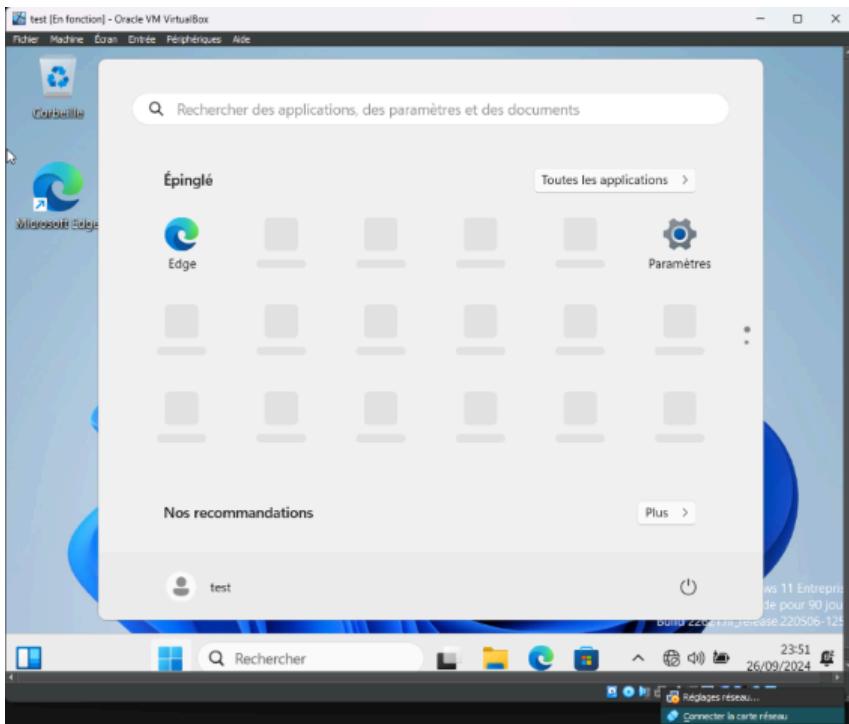
⌚ Todo

L'ordinateur va redémarrer.



⌚ Todo

Regardez en bas à droite et cliquez à nouveau sur [Connecter la carte réseau](#) (click droit pour ouvrir le menu). Cela va remettre le réseau et permettre à Windows d'accéder à internet



"Quelques" définitions

Fichier

- Unité de stockage de données.
- Contient des informations (texte, images, programmes, etc.).
- A une extension qui indique son type (ex : .txt, .jpg, .exe).

Dossier ou Répertoire:

- Conteneur pour organiser des fichiers et d'autres dossiers.
- Permet de structurer les données en catégories.
- N'a pas d'extension propre ; identifié par son nom.

Explorateur Windows

- Interface graphique pour accéder et gérer les fichiers et dossiers.
- Permet de naviguer, copier, déplacer, supprimer, et rechercher des fichiers/dossiers.
- Offre une vue hiérarchique des lecteurs, dossiers, et fichiers.
- C'est un programme (et il peut donc planter et être redémarré)
- Supporte les onglets dans Windows 11 pour faciliter la navigation multipage.

Info

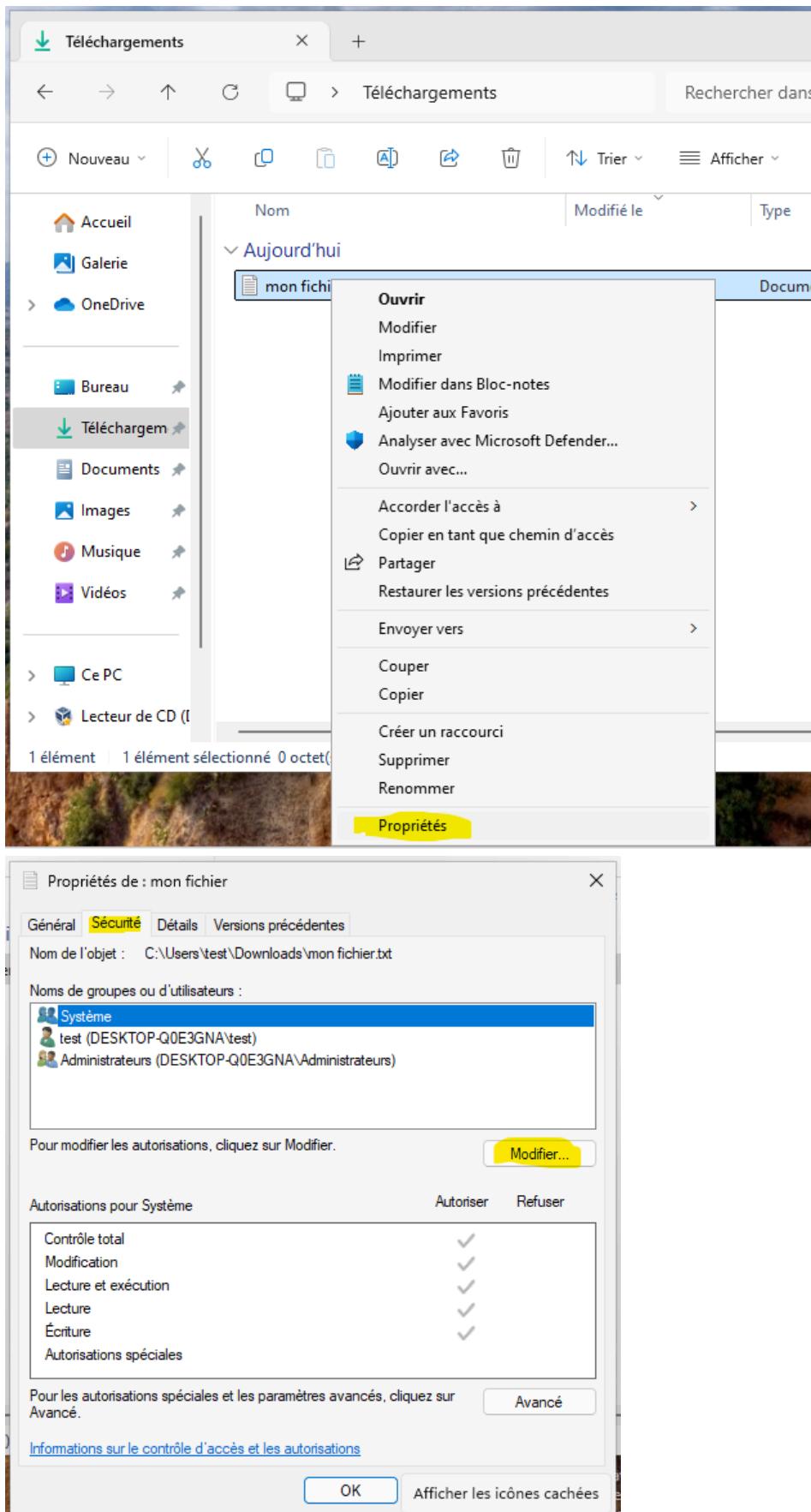
Il est possible de le couper et/ou de le relancer.

Le couper en utilisant le gestionnaire de tâche et le relancer en utilisant l'utilitaire de commande

Droits des dossiers et fichier en NTFS

Sous Windows, les droits des fichiers et dossiers (ou **autorisations**) déterminent qui peut accéder à un fichier ou dossier et quelles actions ils peuvent effectuer. Voici les principales permissions :

- **Lecture** : permet de voir le contenu du fichier ou du dossier.
- **Écriture** : permet de modifier ou supprimer le fichier/dossier.
- **Exécution** : permet de lancer un fichier (ex. un programme).
- **Modification** : permet de lire, écrire et supprimer un fichier.
- **Contrôle total** : permet toutes les actions, y compris la modification des autorisations.



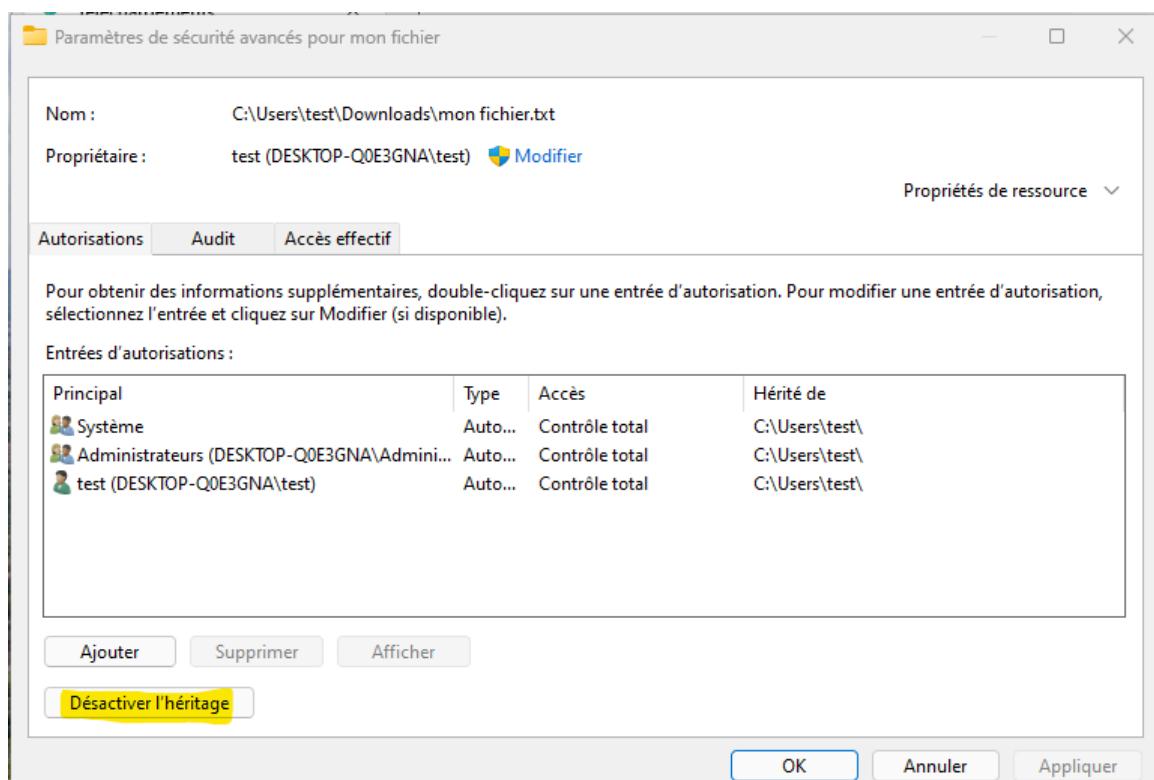
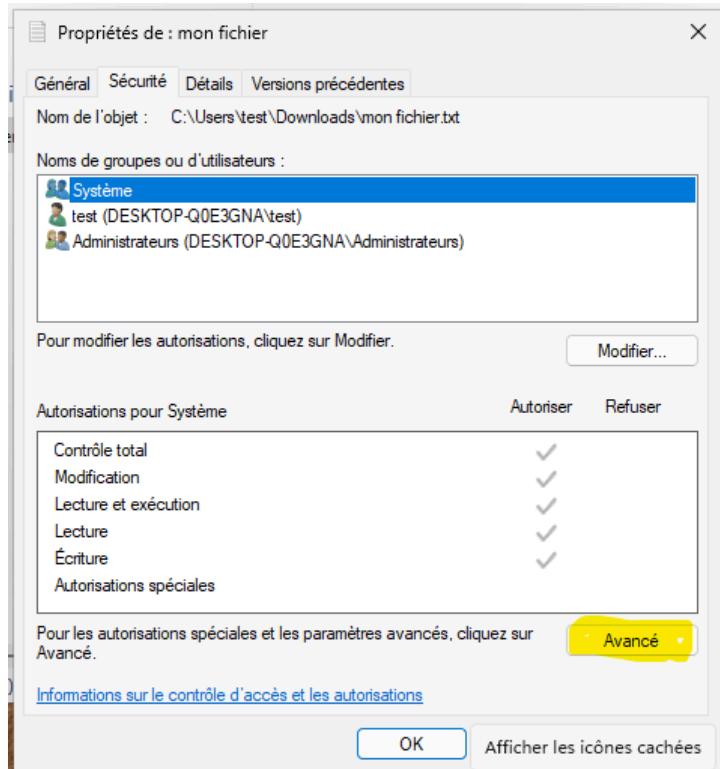
Il y a une notion d'héritage pour les droits dans Windows.

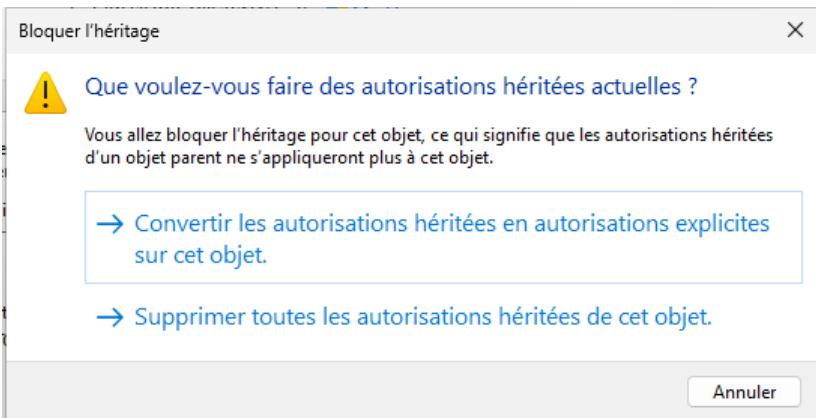
Les **droits hérités** sous Windows désignent donc les permissions d'un dossier parent qui sont automatiquement appliquées à ses sous-dossiers (dossiers enfants) et fichiers. Cela permet de gérer plus facilement les autorisations sur un ensemble de dossiers en les définissant une seule fois au niveau du parent.

- **Principe** : les dossiers enfants héritent des permissions du dossier parent, à moins que cet héritage ne soit explicitement désactivé.
- **Avantage** : cela assure une cohérence et simplifie la gestion des droits, car tout changement au niveau du dossier parent se répercute automatiquement.

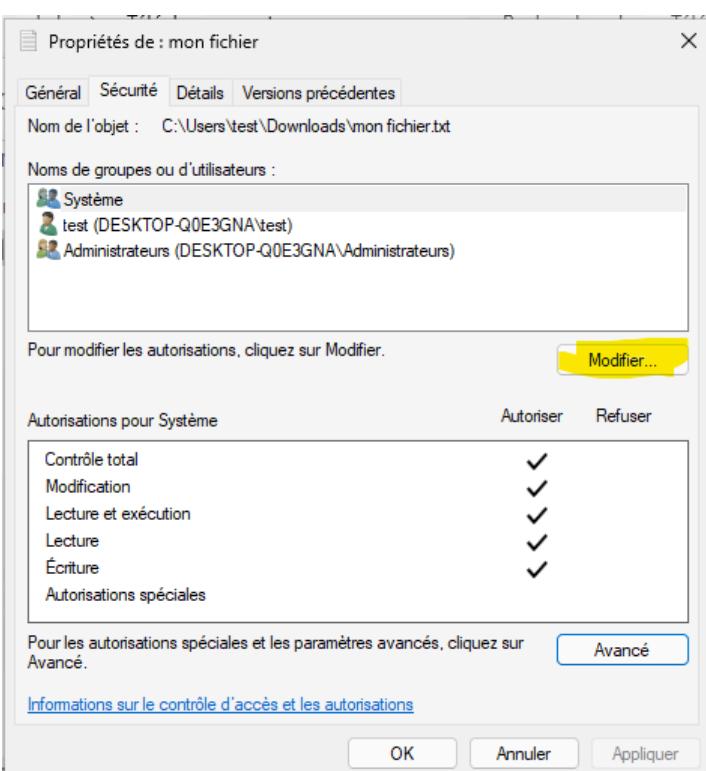
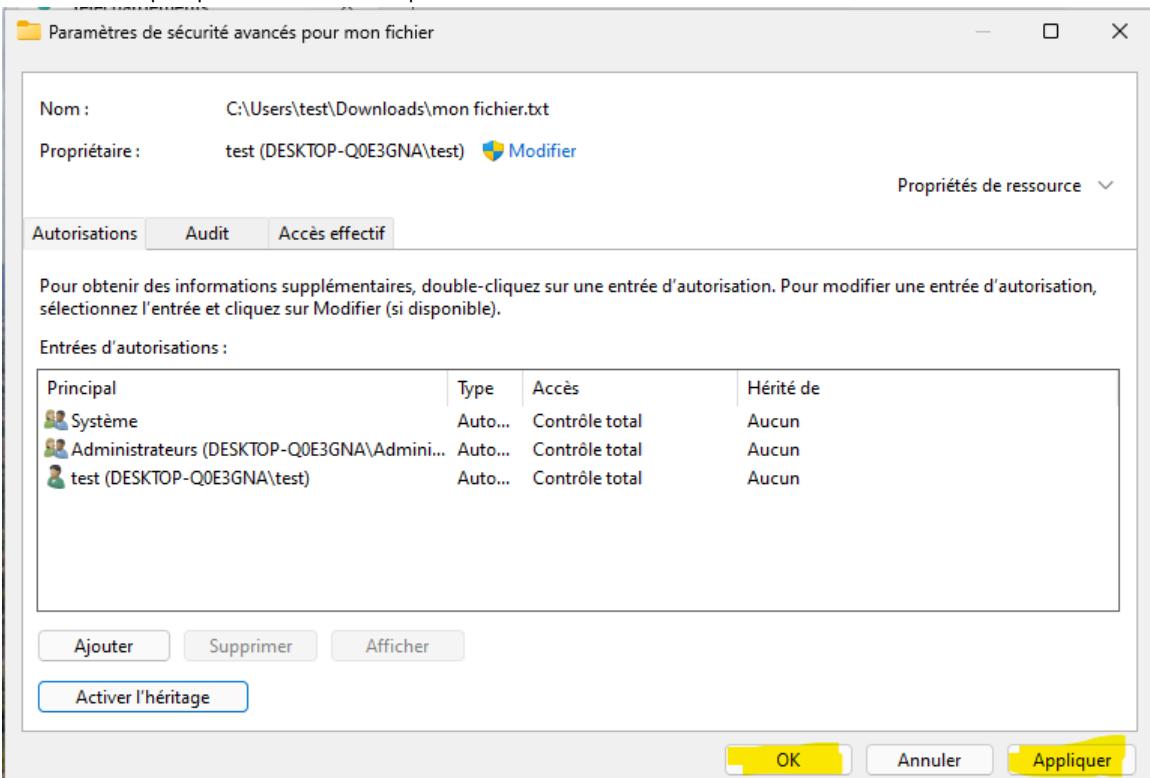
- **Désactivation de l'héritage** : on peut empêcher un dossier enfant d'hériter en décochant l'option d'héritage, puis en personnalisant les permissions.

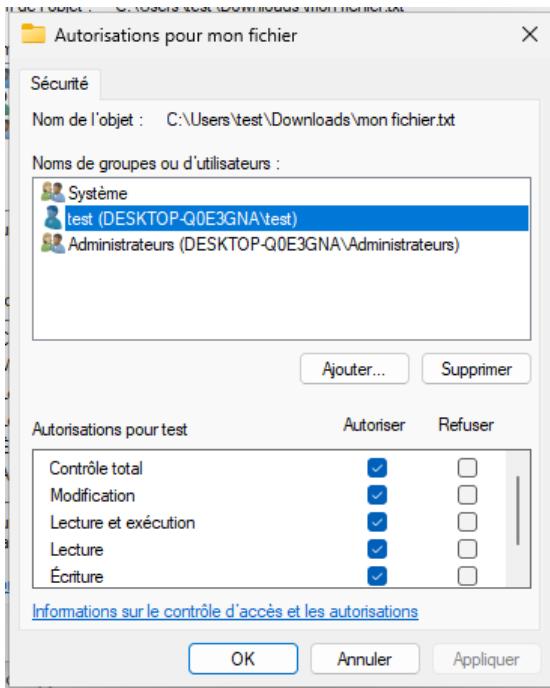
Il est possible de casser cet héritage si par exemple un dossier parents accorde des droits à plusieurs utilisateurs mais qu'on souhaite que les dossiers/fichiers enfants soient accessible à moins d'utilisateurs. Exemple avec un répertoire d'une entreprise qui contient un dossier compta, un dossier RH et d'autres dossier par service mais également des dossier interservices.





On converti! L'objectif ici c'est d'attribué des droits à l'objet lui même plutôt qu'il ne les hérite. On lui applique donc les droits existant à lui même. On ne souhaite pas qu'il n'ai soudainement plus aucun droit.





Il sera possible de modifier le droits pour l'utilisateur sélectionné.

On peut d'ailleurs voir qu'il est aussi par défaut utilisable pour les comptes dans les groupes systèmes ou administrateurs.

En cliquant sur ajouter il sera possible de rajouter un utilisateur créé précédemment puis lui donner ou non des droits.

Les extensions sous Windows

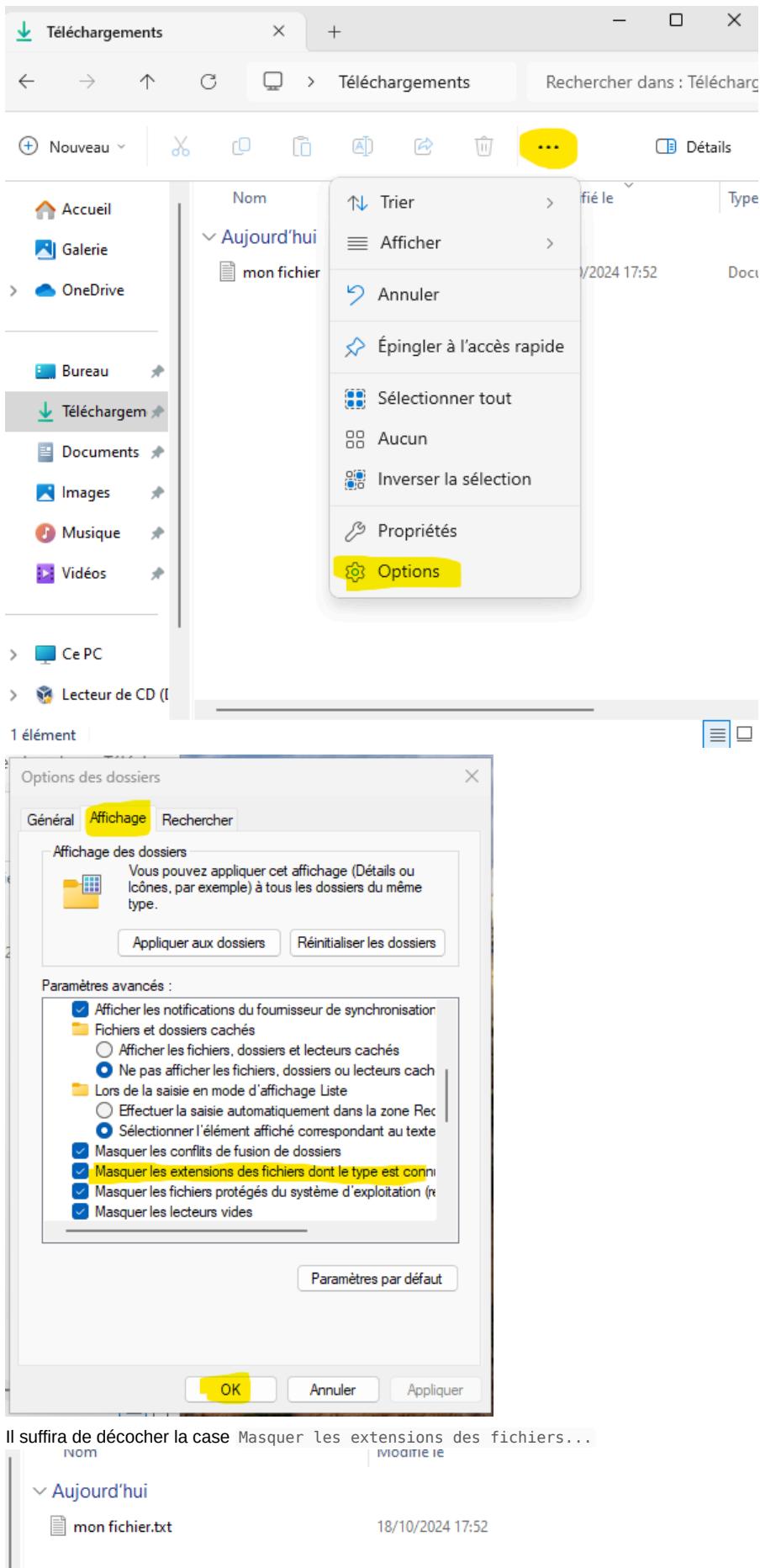
Les **extensions de fichiers** dans Windows sont des suffixes (généralement 3 ou 4 lettres) à la fin du nom d'un fichier, séparées par un point (ex. .docx, .jpg). Elles sont cruciales car elles indiquent à Windows quel programme utiliser pour ouvrir ou exécuter le fichier.

- **Identification du type de fichier** : l'extension permet de savoir si le fichier est un document, une image, une vidéo, etc. (ex. .txt pour du texte, .exe pour un programme).
- **Association avec des logiciels** : Windows utilise les extensions pour associer les fichiers aux programmes (ex. .pdf s'ouvre avec un lecteur PDF).
- **Sécurité** : les extensions aident à identifier des fichiers potentiellement dangereux (ex. .exe ou .bat qui peuvent exécuter du code).
- **Personnalisation des fichiers** : les utilisateurs peuvent renommer les extensions pour changer le comportement d'un fichier, mais cela peut rendre certains fichiers inaccessibles ou les ouvrir avec un mauvais programme.

Par défaut, windows masque les extensions.

▼ Aujourd'hui
📄 mon fichier 18/10/2024 17:52

Il est possible cependant de les afficher.



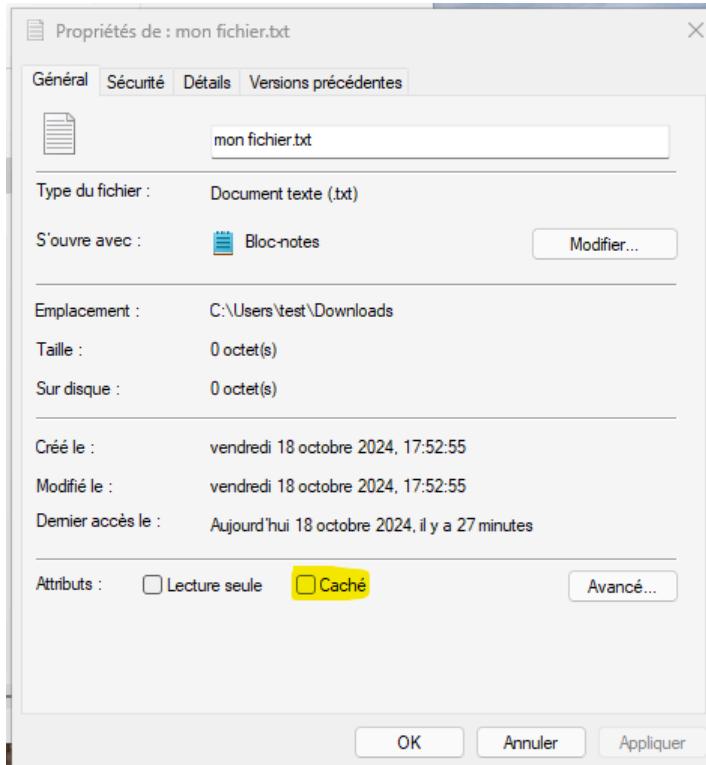
Attention. Changer l'extension change la manière dont Windows interprétera ce fichier.

Les fichiers cachés

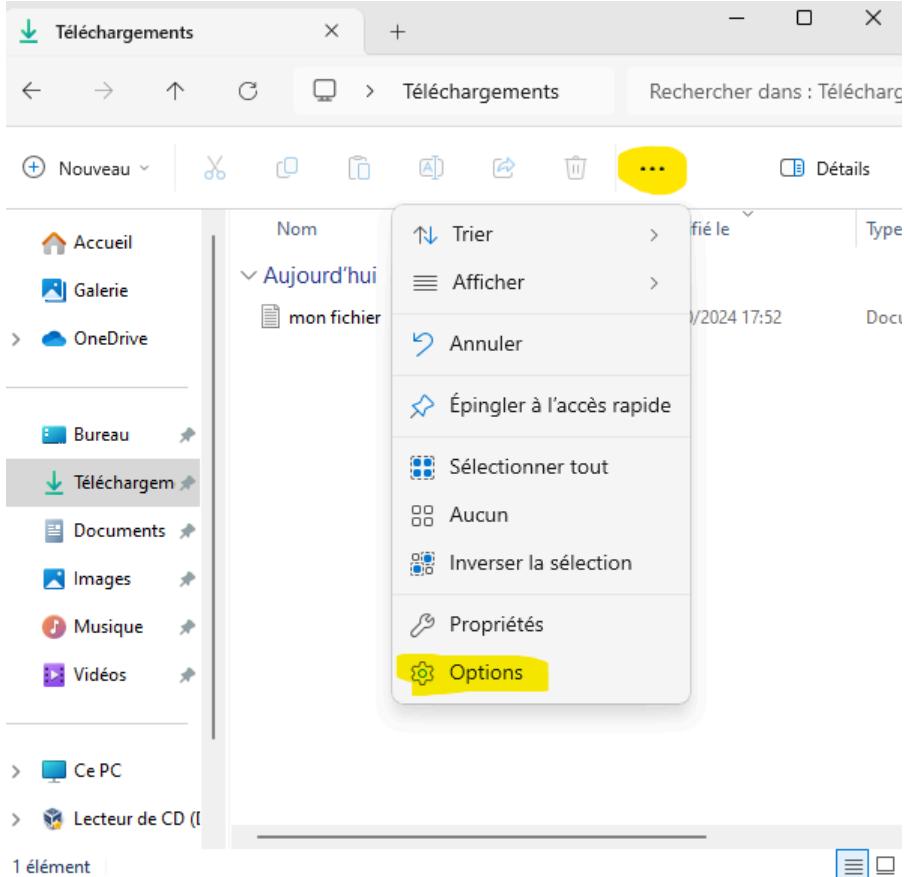
Les **fichiers cachés** sous Windows sont des fichiers ou dossiers qui ne sont pas visibles par défaut dans l'explorateur de fichiers. Ils sont souvent utilisés pour stocker des données critiques du système ou des configurations que l'utilisateur moyen n'a pas besoin de modifier.

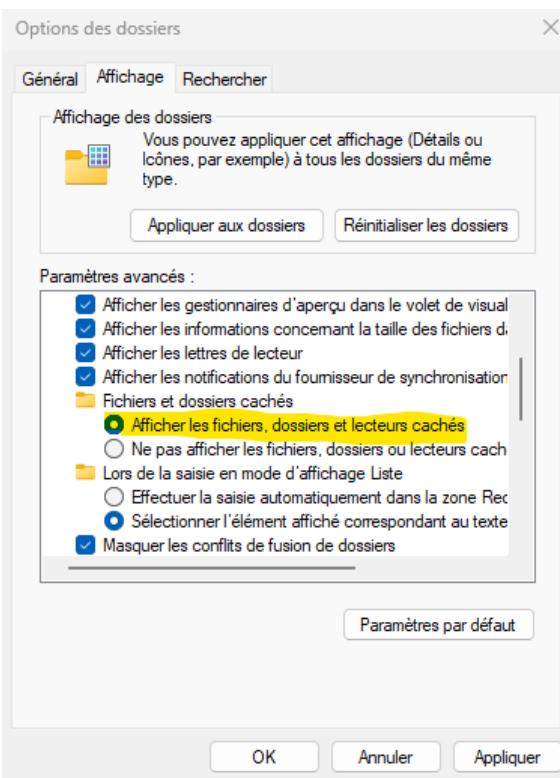
- **Invisible par défaut** : Windows les masque pour éviter les suppressions ou modifications accidentelles.
- **Utilisation principale** : ils contiennent souvent des fichiers système, des configurations d'applications ou des fichiers temporaires.
- **Affichage manuel** : pour voir les fichiers cachés, l'utilisateur doit activer l'option "Afficher les fichiers cachés" dans les paramètres de l'explorateur de fichiers.
- **Protection du système** : cela évite des erreurs ou dysfonctionnements, car ces fichiers sont essentiels pour la stabilité et la sécurité de Windows.

"Cacher" est un attribut de fichier ou de dossier. Il est possible de l'activer ou le désactiver dans les propriétés du fichier ou dossier.



Il est également possible d'afficher ou de masquer les fichiers cachés.

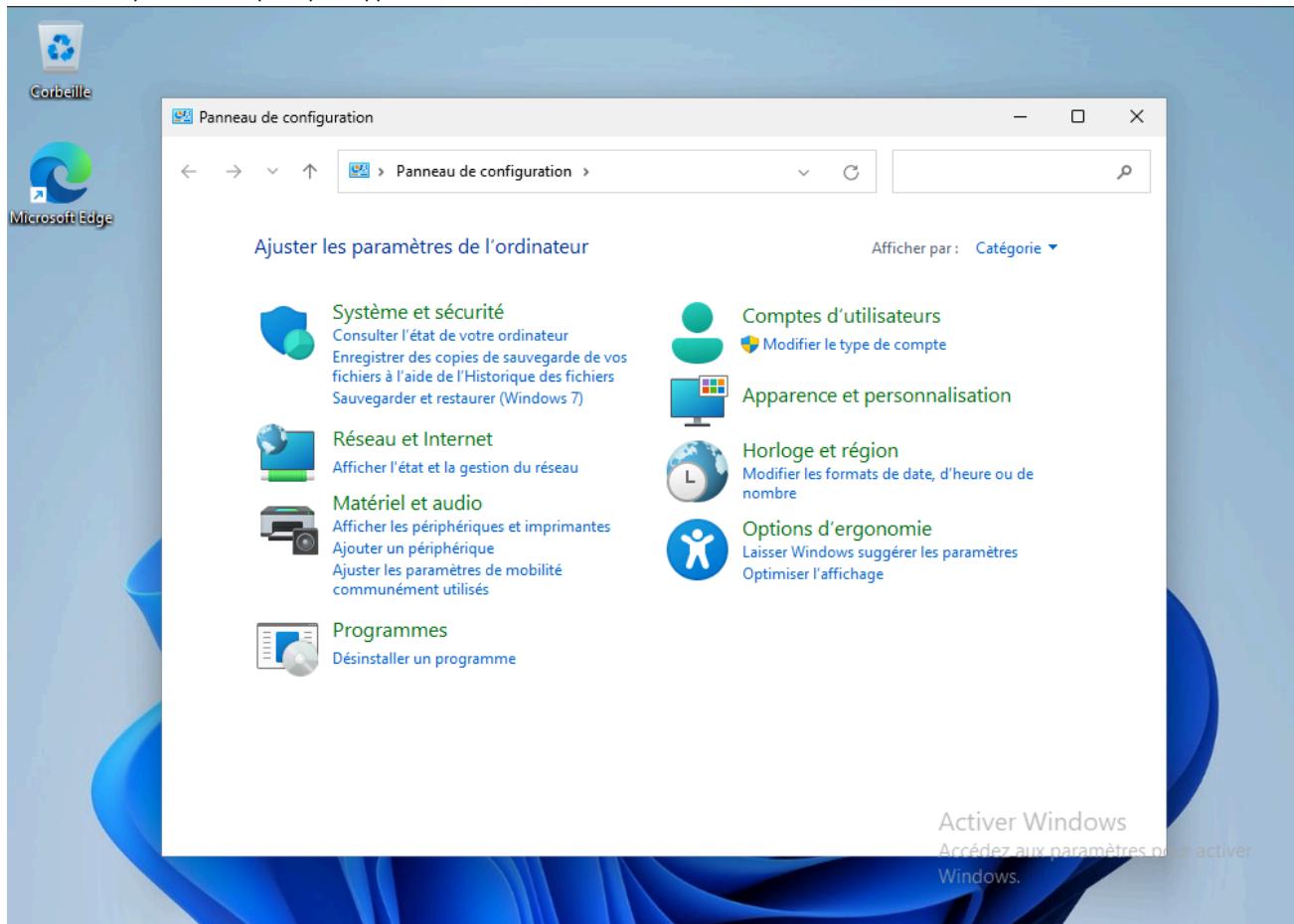


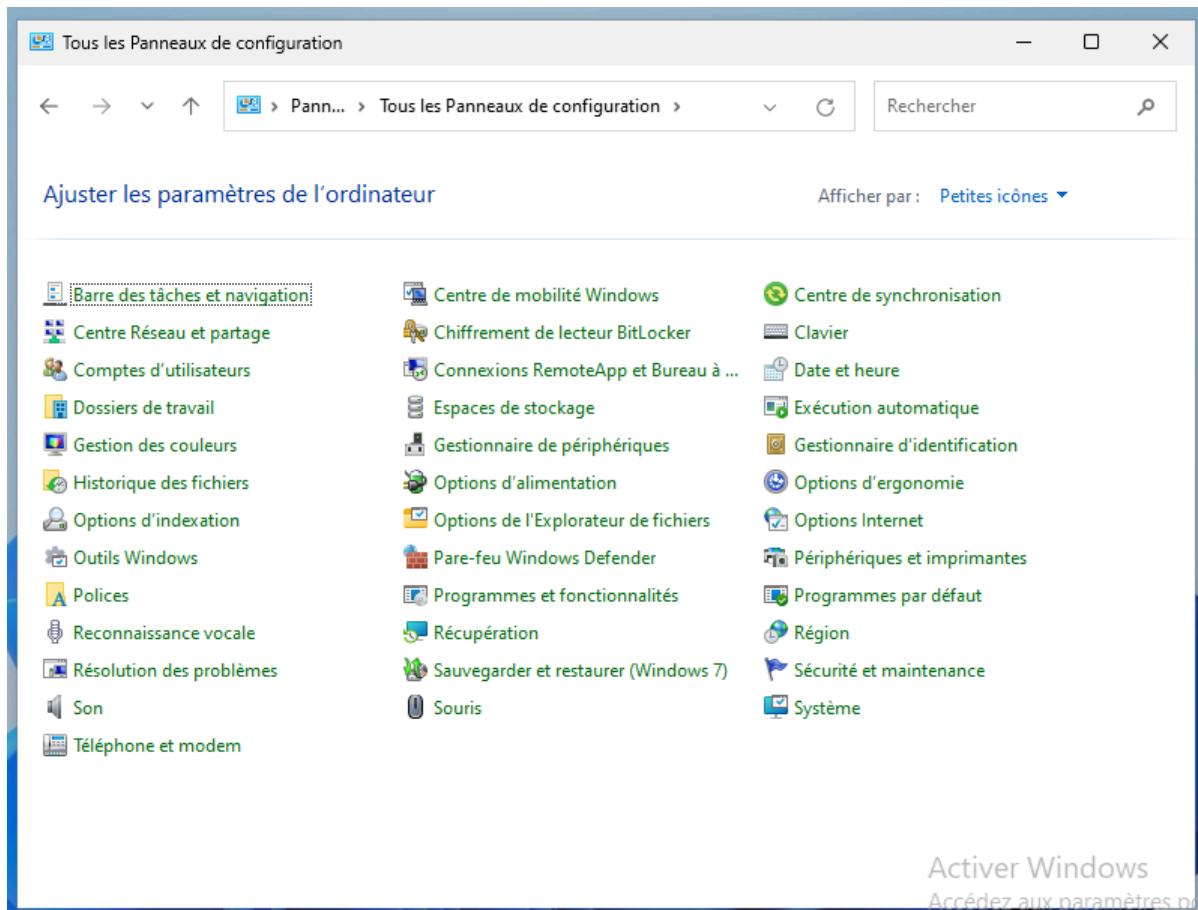


Les fichiers et dossiers cachés apparaîtront dans l'explorateur avec un icône légèrement transparente.

Panneau de configuration

- Outil système pour modifier les paramètres de configuration de Windows.
- Permet de gérer des aspects tels que le matériel, les programmes, la sécurité, et les comptes utilisateurs.
- Offre accès à des outils de personnalisation, de réseau et d'Internet, de matériel et de son, d'applications par défaut, et plus.
- Structuré en catégories pour une navigation facilitée (ou pas).
- Peut être remplacé ou complété par l'application Paramètres dans les versions récentes de Windows.





Centre de réseau et partage

- Panneau de configuration dédié à la gestion des connexions réseau.
- Permet de visualiser l'état actuel des réseaux auxquels l'ordinateur est connecté.
- Offre des options pour configurer, gérer les réseaux Wi-Fi, Ethernet, VPN, etc.
- Facilite la création et la gestion de réseaux domestiques et professionnels.
- Donne accès aux paramètres de partage, permettant de choisir ce qui peut être partagé avec le réseau.
- Inclut des outils pour diagnostiquer et résoudre les problèmes de connexion.

Centre Réseau et partage

Page d'accueil du panneau de configuration

Modifier les paramètres de la carte

Modifier les paramètres de partage avancés

Options de diffusion multimédia en continu

Afficher les informations de base de votre réseau et configurer des connexions

Afficher vos réseaux actifs

Réseau

Réseau public

Type d'accès : Internet

Connexions : Ethernet

Modifier vos paramètres réseau

Configurer une nouvelle connexion ou un nouveau réseau

Configurez une connexion haut débit, d'accès à distance ou VPN, ou configurez un routeur ou un point d'accès.

Résoudre les problèmes

Diagnostiquez et réparez les problèmes de réseau ou accédez à des informations de dépannage.

Voir aussi

Options Internet

Pare-feu Windows Defender

Activer Windows

Accédez aux paramètres pour activer Windows.

Centre Réseau et partage

Connexions réseau

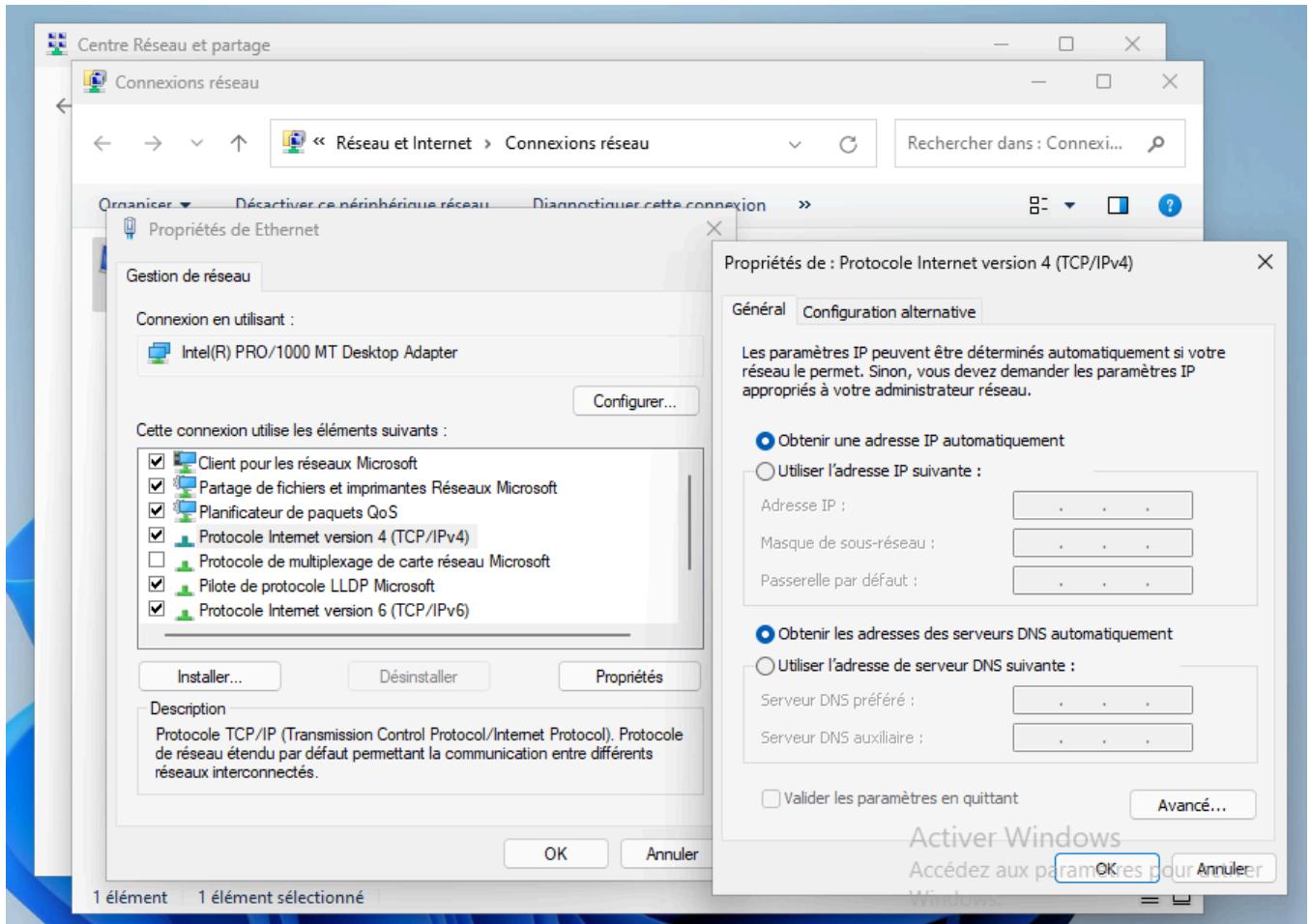
Organiser ▾ Désactiver ce périphérique réseau Diagnostiquer cette connexion >

Ethernet Réseau Intel(R) PRO/1000 MT Desktop Ad...

1 élément | 1 élément sélectionné |

Activer Windows

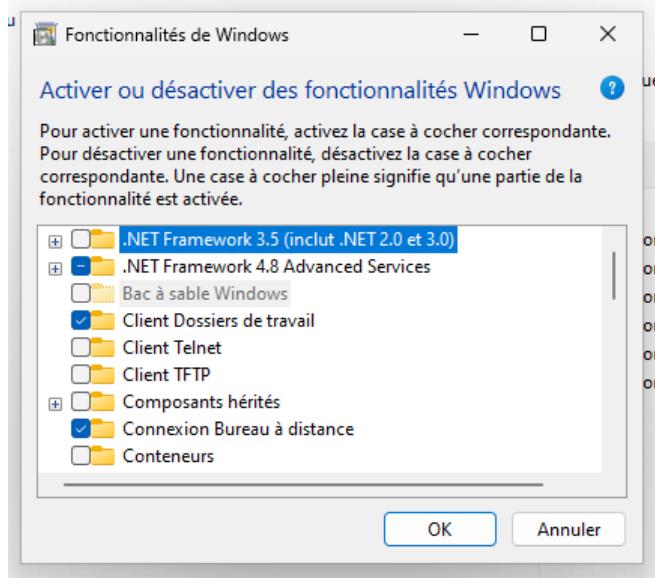
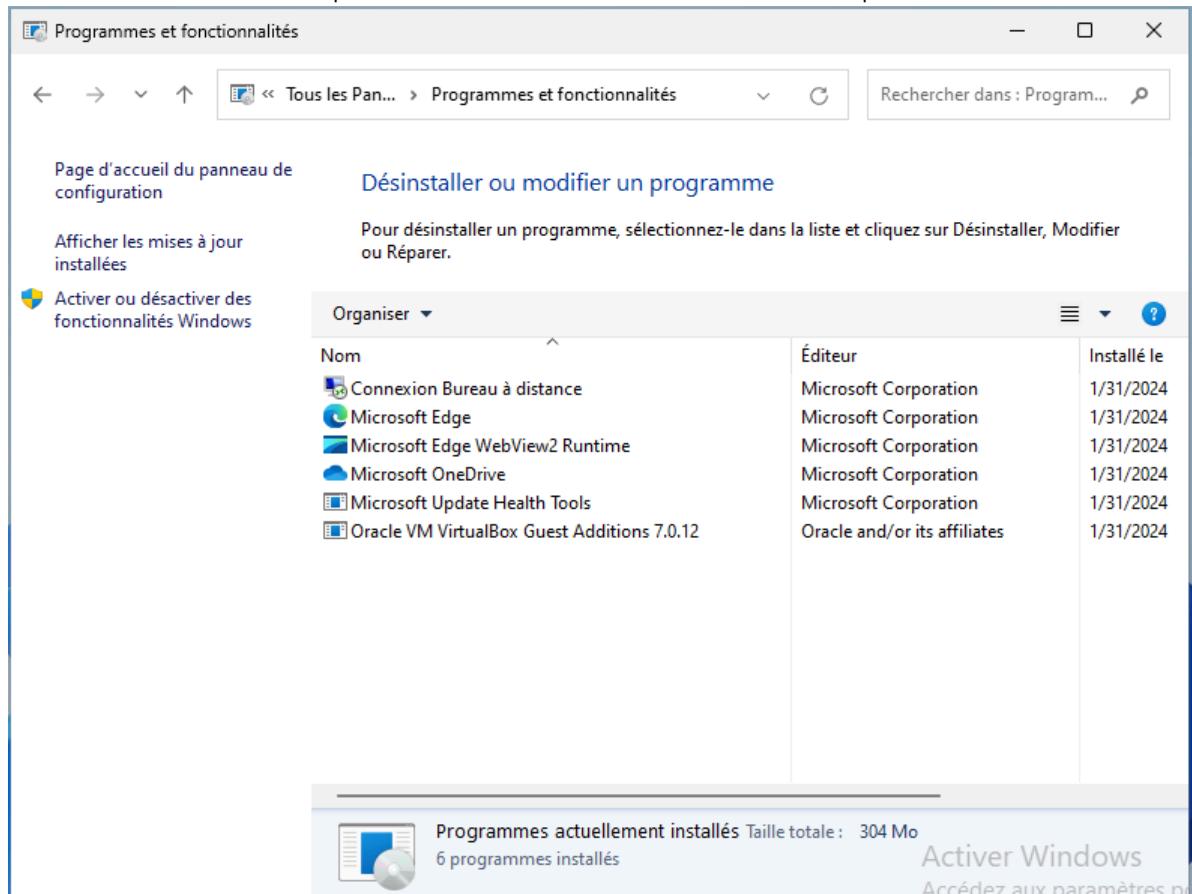
Accédez aux paramètres pour activer Windows.



Programmes et fonctionnalités

- Section du Panneau de Configuration pour gérer les logiciels installés.
- Permet de désinstaller, modifier ou réparer des programmes.
- Affiche la liste des applications installées avec des détails tels que la taille, la version et la date d'installation.
- Offre la possibilité de trier, filtrer, et rechercher des applications spécifiques.

- Donne accès à Windows Features pour activer ou désactiver des fonctionnalités Windows optionnelles.

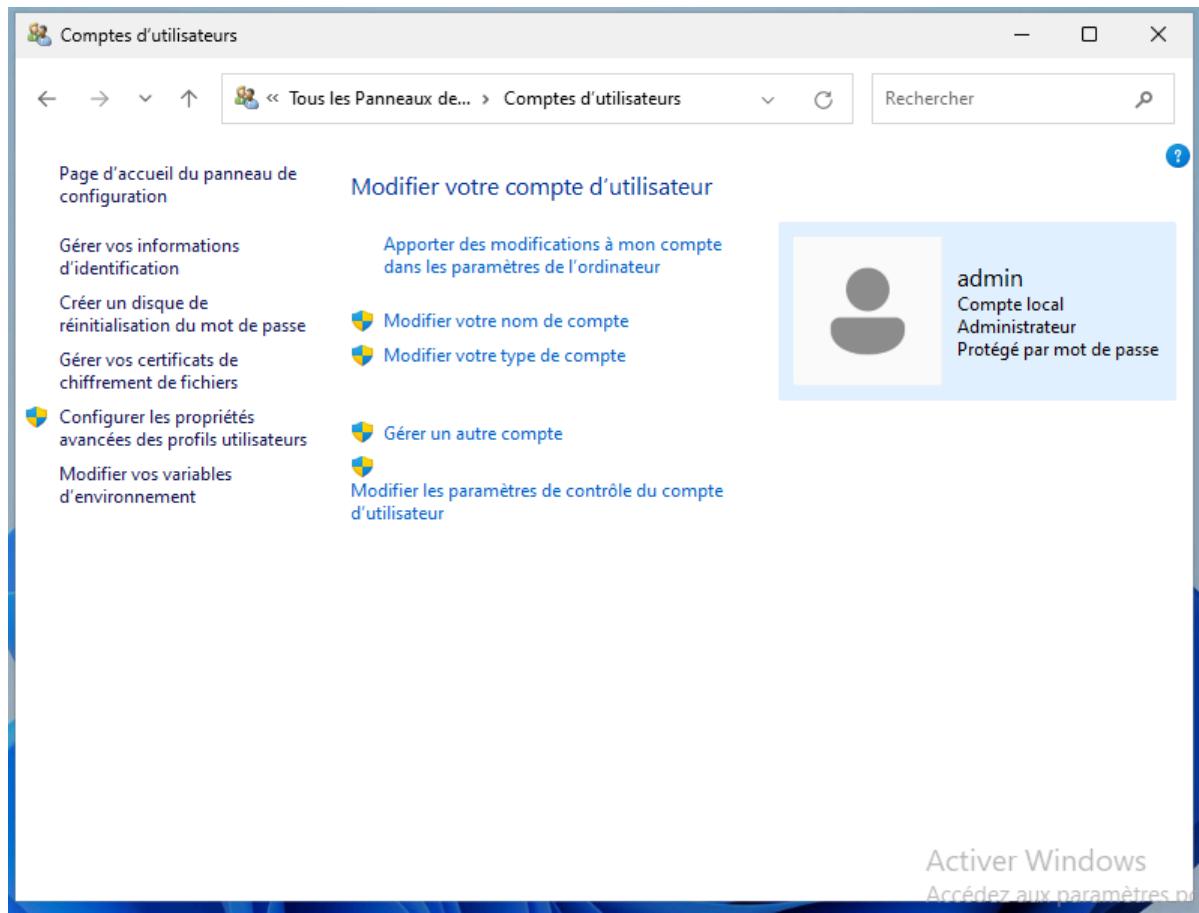


Todo

Installez la fonctionnalité Client Telnet

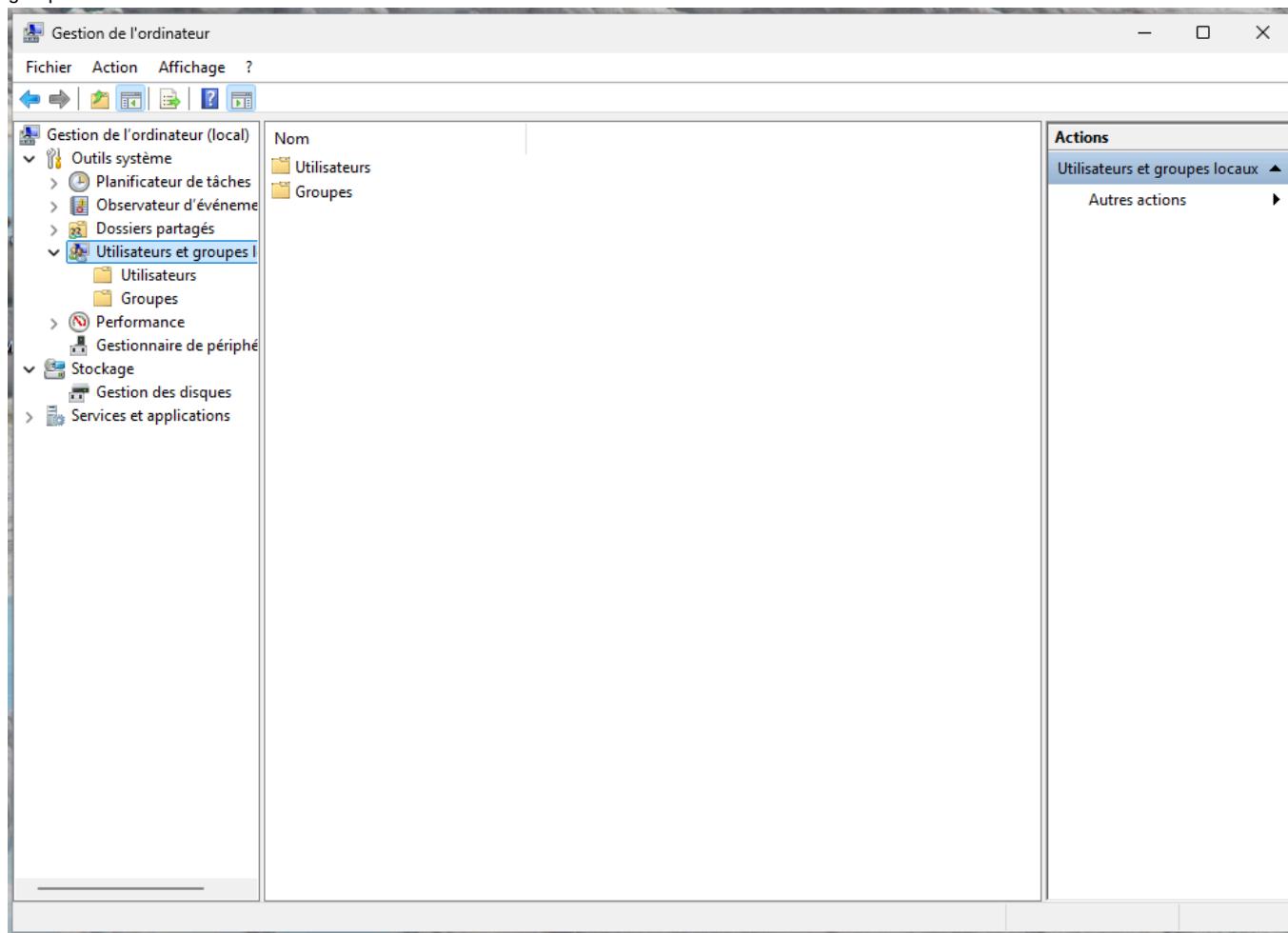
Comptes d'utilisateurs

- Permet de gérer les profils d'accès au système Windows.
- Offre la possibilité de créer, modifier, ou supprimer des comptes.
- Différents types de comptes disponibles : Administrateur, Standard, Invité.
 - Administrateur : Accès complet, peut modifier les paramètres système et gérer d'autres comptes.
 - Standard : Accès limité, peut utiliser des applications et modifier certains paramètres.
 - Invité : Accès très limité, destiné à une utilisation temporaire sans accès aux fichiers personnels.
- Intègre des options de sécurité comme le contrôle parental et la gestion des mots de passe.



Utilisateurs et groupes via la Gestion de l'ordinateur.

Plus loin vous allez explorer une fenêtre nommée "gestion de l'ordinateur". Ce panneau contient une autre approche de la gestion des comptes et groupes de l'ordinateur.



Vous pouvez voir ici qu'il y a plusieurs comptes, pas seulement celui de mon utilisateur principal. Windows embarque d'autres comptes pour fonctionner. Généralement ces comptes sont en revanche innaccessible par défaut tel que le compte Administrateur.

Gestion de l'ordinateur

Fichier Action Affichage ?

Gestion de l'ordinateur (local)

Outils système

Planificateur de tâches

Observateur d'événements

Dossiers partagés

Utilisateurs et groupes

Utilisateurs

Groupes

Performance

Gestionnaire de périphérique

Stockage

Gestion des disques

Services et applications

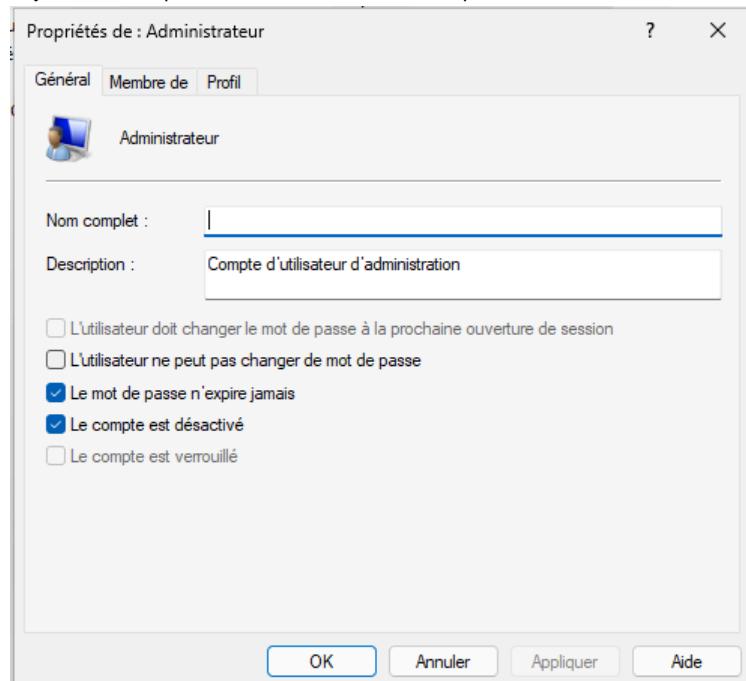
Nom	Nom complet	Description
Administrat...	Administrateur	Compte d'utilisateur d'administra...
DefaultAcco...	DefaultAccount	Compte utilisateur géré par le syst...
Invité	Invité	Compte d'utilisateur invité
test	test	Compte d'utilisateur géré et utilis...
WDAGUtility...	WDAGUtility	

Actions

Utilisateurs

Autres actions

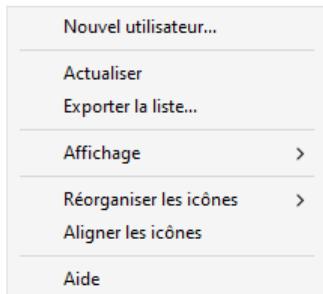
Si j'ouvre le compte administrateur en double cliquant dessus :



Je peux constater le compte est désactivé. Il n'est donc pas fonctionnel. Il lui est également interdit de changer son mot de passe.

Il nous est possible de créer un autre utilisateur via cette fenêtre. Click droit au milieu de la fenêtre, Nouvel utilisateur....

Nom	Nom complet	Description
Administrat...		Compte d'utilisateur d'administra...
DefaultAcco...		Compte utilisateur géré par le syst...
Invité		Compte d'utilisateur invité
test		Compte d'utilisateur géré et utilis...
WDAGUtility...		



Nouvel utilisateur

Nom d'utilisateur :	albert
Nom complet :	Albert Dupond
Description :	Comptable
Mot de passe :	****
Confirmer le mot de passe :	****
<input checked="" type="checkbox"/> L'utilisateur doit changer le mot de passe à la prochaine ouverture de session	
<input type="checkbox"/> L'utilisateur ne peut pas changer de mot de passe	
<input type="checkbox"/> Le mot de passe n'expire jamais	
<input type="checkbox"/> Le compte est désactivé	

Aide Crée... Fermer

Il est possible de lui imposer le changement de mot de passe lors de sa première connexion, ce qui est généralement conseillé car une bonne pratique. Cela force l'utilisateur à choisir un nouveau mot de passe et donc à vous de ne plus le connaître.

Nom	Nom complet	Description
Administrat...		Compte d'utilisateur d'administra...
albert	Albert Dupond	Comptable
DefaultAcco...		Compte utilisateur géré par le syst...
Invité		Compte d'utilisateur invité
test		Compte d'utilisateur géré et utilis...
WDAGUtility...		

Les groupes servent à organiser les utilisateurs et par gérer leur différents droits et accès.

The screenshot shows the Windows Computer Management console window titled "Gestion de l'ordinateur". The left navigation pane is expanded to show "Utilisateurs et groupes l.", with "Groupes" selected under it. The main pane displays a table of groups with columns "Nom" (Name) and "Description". The "Actions" pane on the right is set to "Groupes".

Nom	Description
Administrateurs	Les membres du groupe Administrateurs
Administrateurs Hypervisor	Les membres de ce groupe disposent d'autorisations supplémentaires pour les fonctionnalités de hyperviseur.
Duplicateurs	Prend en charge la réPLICATION des utilisateurs.
IIS_IUSRS	Groupe intégré utilisé par les services IIS.
Invités	Les membres du groupe Invités peuvent accéder aux ressources partagées.
Lecteurs des journaux	Des membres de ce groupe peuvent lire les journaux.
Opérateurs d'assistan...	Les membres de ce groupe peuvent effectuer des opérations administratives.
Opérateurs de chiffre...	Les membres sont autorisés à effacer les données.
Opérateurs de config...	Les membres de ce groupe peuvent modifier les paramètres système.
Opérateurs de sauveg...	Les membres du groupe Opérateurs de sauvegarde ont des droits de sauvegarde et de restauration.
Propriétaires d'appareils	Les membres de ce groupe peuvent être propriétaires d'appareils.
System Managed Acc...	Les membres de ce groupe sont gérés par le système.
Utilisateurs	Les utilisateurs ne peuvent pas établir de sessions.
Utilisateurs avec pouvo...	Les utilisateurs avec pouvoir sont autorisés à effectuer des opérations administratives.
Utilisateurs de gestion...	Les membres de ce groupe ont accès à des fonctionnalités de gestion.
Utilisateurs de l'Analy...	Les membres de ce groupe peuvent accéder aux fonctionnalités d'analyse.
Utilisateurs du Bureau...	Les membres de ce groupe disposent d'autorisations supplémentaires pour les fonctionnalités de bureau.
Utilisateurs du journal...	Les membres de ce groupe peuvent accéder au journal des événements.
Utilisateurs du modèl...	Les membres sont autorisés à lancer des applications.

Note

Je ne fais pas le détail de l'ensemble des droits liés aux groupes ci-dessus. Vous pouvez consulter la documentation en ligne de Windows à ce sujet. Notez cependant qu'a appartenir au groupe Administrateur donne l'ensemble des autres droits.

Pour créer un groupe, c'est comme pour les utilisateurs. Click droit au milieu de l'écran et Nouveau groupe....

The screenshot shows the "Nouveau groupe" dialog box. The "Nom du groupe" field is filled with "compta". The "Membres" section is empty, indicated by a red arrow pointing to the "Ajouter..." button. In the background, a "Groupes" search results window is open, showing a list of groups. A red arrow points from the "Vérifier les noms" button in the search results window to the "OK" button in the "Nouveau groupe" dialog box. The "Créer" button is also visible at the bottom of the dialog box.

On commence par choisir un nom puis nous allons y ajouter un utilisateur. Une nouvelle fenêtre s'ouvre où nous allons pouvoir taper le nom de l'utilisateur puis vérifier si il existe bien.



Ici son nom a légèrement changer. On peut comprendre ici que cet utilisateur existe dans un "contexte". C'est l'utilisateur albert de l'ordinateur DESKTOP-Q0E3GNA. Il n'existe pas sur un autre ordinateur ou sur un domaine d'entreprise (ou voit ça plus tard).

On valide tout ça et le nouveau groupe est créé avec l'utilisateur dedans.

L'utilit  d'un groupe ici nous sera utile pour g rer des droits sur des fichiers, dossier ou encore sur des partages r seau.

Les services

- Outil de gestion des services Windows qui s'exécutent en arrière-plan.
 - Permet de démarrer, arrêter, et configurer les paramètres des services.
 - Offre une vue détaillée de chaque service, incluant le statut, le type de démarrage, et le nom de connexion.
 - Les types de démarrage comprennent : Automatique, Manuel, et Désactivé.
 - Utilisé pour optimiser les performances ou résoudre des problèmes en ajustant les services.
 - Accessible via le Panneau de Configuration ou en tapant "services.msc" dans la commande Exécuter.
 - Important pour les administrateurs système pour la maintenance et la sécurisation du système.

Nom	Description	État	Type de démarrage
Accès aux données utilisat...	Fournit l'accès ...	En cours	Manuel
Acquisition d'image Windo...	Fournit des ...		Manuel (Déclenché par un autre service)
Agent Activation Runtime_...	Runtime for...		Manuel
Agent de stratégie IPsec	La sécurité ...		Manuel (Déclenché par un autre service)
Alimentation	Gère la strat...	En cours	Automatique
Appel de procédure distant...	Le service R...	En cours	Automatique
Application système COM+	Gère la conf...		Manuel
Assistance IP	Fournit une ...	En cours	Automatique
Assistance NetBIOS sur TCP...	Prend en ch...	En cours	Manuel (Déclenché par un autre service)
Assistant Connectivité réseau	Fournit la n...		Manuel (Déclenché par un autre service)
Assistant Connexion avec u...	Autorise la co...	En cours	Manuel (Déclenché par un autre service)
Audio Windows	Gère les péri...	En cours	Automatique
Authentification naturelle	Service d'ag...		Manuel (Déclenché par un autre service)
BranchCache	Ce service ...		Manuel
CaptureService_9007f	Active la fo...	En cours	Manuel
Carte à puce	Gère l'accès...		Manuel (Déclenché par un autre service)
Carte de performance WMI	Fournit des ...		Manuel
Centre de sécurité	Le service ...	En cours	Automatique (débutant)
Cliché instantané des volu...	Gère et impl...		Manuel
Client de stratégie de groupe	Le service e...	En cours	Automatique (déclenché par un autre service)
Client de suivi de lien distri...	Conserve le...	En cours	Automatique

Informations Systèmes

- Fournit des détails complets sur la configuration matérielle et logicielle de l'ordinateur.
 - Inclut des informations sur le processeur, la mémoire RAM, le système d'exploitation, les pilotes, l'environnement réseau, et plus.
 - Affiche le type de système (32 ou 64 bits), la version de Windows, et le numéro de build.
 - Permet de voir l'état des composants matériels et les conflits de périphériques.
 - Accessible en tapant "msinfo32" dans la commande Exécuter ou via le Panneau de Configuration.
 - Utile pour le diagnostic de problèmes système et la planification des mises à niveau.

Système > Informations système

testwindows11
VirtualBox

[Renommer ce PC](#)

① Spécifications de l'appareil

Copier ^

Nom de l'appareil	testwindows11
Processeur	AMD Ryzen 7 5800H with Radeon Graphics GHz
Mémoire RAM installée	3.98 Go
ID de périphérique	CC942EC2-7667-408B-8931-AFB8C3EFC296
ID de produit	00330-80000-00000-AA925
Type du système	Système d'exploitation 64 bits, processeur x64
Stylet et fonction tactile	La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran

Liens connexes [Domaine ou groupe de travail](#) [Protection du système](#)

[Paramètres avancés du système](#)

Informations système

Fichier Edition Affichage ?

Résumé système

Élément	Valeur
Nom du système d'exploitation	Microsoft Windows 11 Professionnel
Version	10.0.22631 Build 22631
Autre description du système d... Non disponible	
Fabricant du système d'exploit... Microsoft Corporation	
Ordinateur	TESTWINDOWS11
Fabricant	innotek GmbH
Modèle	VirtualBox
Type	PC à base de x64
Référence (SKU) du système	Non pris en charge
Processeur	AMD Ryzen 7 5800H with Radeon Graphics, 3194 MHz, 2 cœur(s), innotek GmbH VirtualBox, 12/1/2006
Version du BIOS/Date	2.5
Version SMBIOS	UEFI
Mode BIOS	Oracle Corporation
Fabricant de la carte de base	VirtualBox
Produit de la carte de base	
Version de la carte de base	1.2
Rôle de la plateforme	Mobile
État du démarrage sécurisé	Activé
Configuration de PCR 7	Élévation requise à afficher
Répertoire Windows	C:\Windows
Répertoire système	C:\Windows\system32
Déploiement de démarrage	\Device\Harddisk\Volume2

Rechercher :

Uniquement dans la catégorie sélectionnée Rechercher uniquement dans les noms de catégories

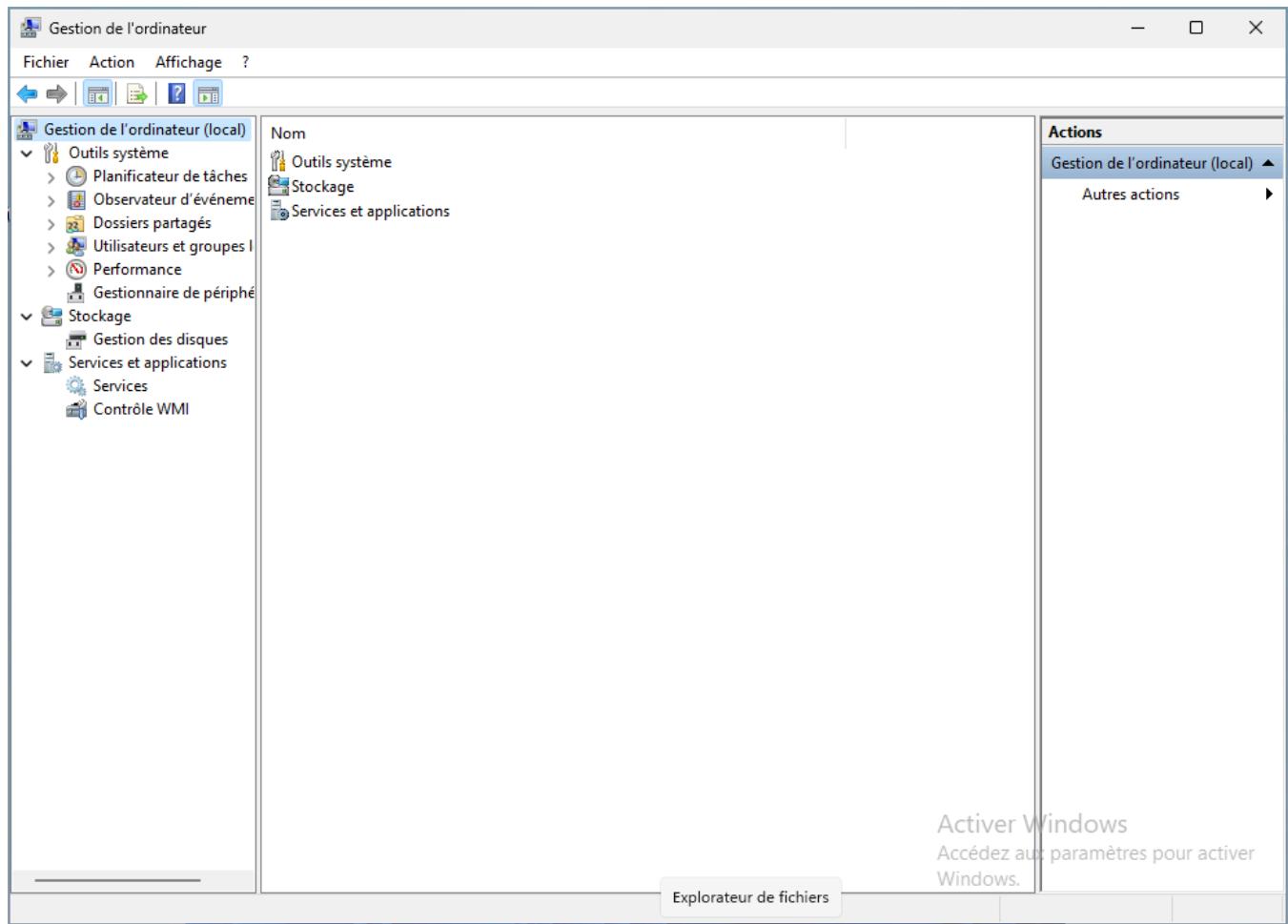
Rechercher [Activer Windows](#) Fermer

Accédez aux paramètres pour activer

"Gestion de l'ordinateur"

- Console unifiée pour l'administration système et la gestion de l'ordinateur.
- Comprend des outils comme le Gestionnaire de disques, l'Observateur d'événements, et les Services.
 - Gestionnaire de disques : permet de partitionner des disques, formater des lecteurs, et gérer les lettres de lecteur.
 - Observateur d'événements : affiche les journaux d'événements système, d'application, et de sécurité.
 - Services : gestion des services Windows qui s'exécutent en arrière-plan.
- Inclut aussi le Gestionnaire de périphériques pour gérer les pilotes et résoudre les problèmes de matériel.
- Accessible en faisant un clic droit sur "Ce PC" ou "Poste de travail" et en sélectionnant "Gérer".

- Essentiel pour les administrateurs et les utilisateurs avancés pour le suivi et la maintenance du système.



Observateur d'évènement

- Outil Windows pour visualiser les journaux d'événements système, d'application, et de sécurité.
- Enregistre des informations sur les opérations du système, comme les démarrages et arrêts de système, les problèmes de pilotes, et les erreurs d'application.
- Classé en plusieurs catégories : Application, Sécurité, Installation, Système, et Journaux Microsoft Windows.
- Permet de diagnostiquer et résoudre des problèmes.
- Offre des fonctionnalités de filtrage et de recherche pour trouver des événements spécifiques.
- Accessible via le Panneau de Gestion de l'Ordinateur ou en tapant "eventvwr.msc" dans Exécuter.

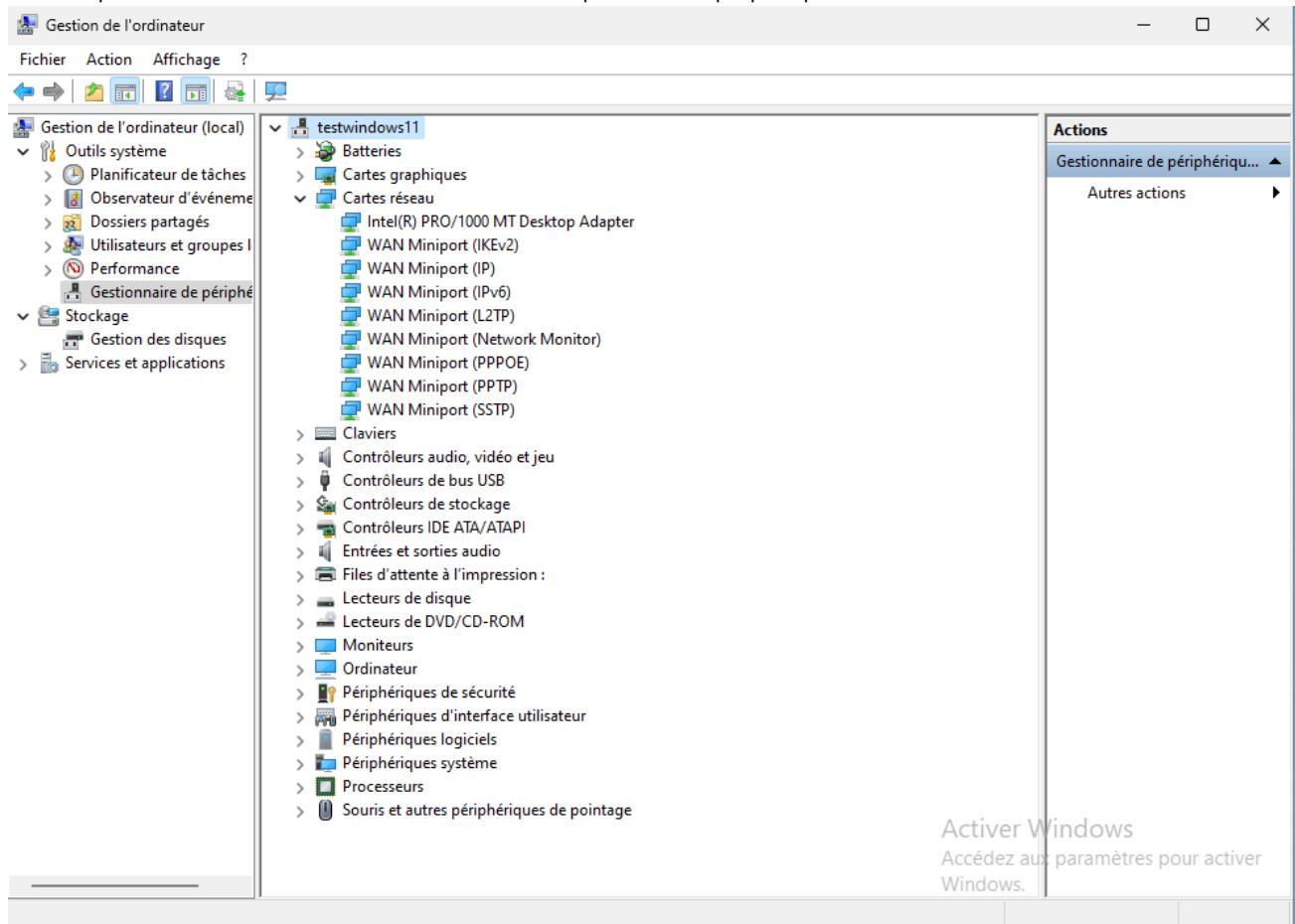
- Peut être utilisé pour surveiller la sécurité et les performances du système.

The screenshot shows the Windows Event Viewer interface. On the left is a navigation pane with categories like Gestion de l'ordinateur (local), Outils système, Observateur d'événement, Journaux Windows, Stockage, Services et applications, and Services. The Journaux Windows section is expanded, showing sub-categories Application, Sécurité, Installation, Système, and Événements trans temporaires. The Système category is selected. The main pane displays a table of events with columns: Niveau, Date et heure, Source, ID de l'événement, and Catégorie de... . The table lists several events, mostly of level Information, from various sources like Service Control Manager, EventLog, and Windows Update. One event, ID 7040, is highlighted. A detailed view of this event is shown in a modal window titled "Événement 7040, Service Control Manager". The details tab is selected, showing the message: "Le type de démarrage du service Pilote ARP IP d'accès à distance est passé de Démarrage à la demande à Démarrage automatique." Below this, event properties are listed: Journal : Système, Source : Service Control Manager, Connecté : 2/1/2024 12:28:03 PM, Événement : 7040, Catégorie : Aucun, Niveau : Information, Mots-clés : Classique, Utilisateur : Système, Ordinateur : testwindows11. To the right of the main window, there is a sidebar titled "Actions" with options like Système, Ouvrir le journal enreg..., Crée une vue perso..., Importer une vue perso..., Effacer le journal..., Filtrer le journal actuel..., Propriétés, Rechercher..., Enregistrer tous les évé..., Joindre une tâche à ce j..., Affichage, Actualiser, and Aide. A tooltip "Activer Windows" is visible at the bottom right.

Gestionnaire de périphériques

- Outil système pour visualiser et gérer le matériel connecté à l'ordinateur.
- Permet d'installer, mettre à jour, désactiver, et désinstaller les pilotes des périphériques.
- Affiche une liste de tous les périphériques classés par catégorie (ex : cartes graphiques, périphériques d'entrée, etc.).
- Identifie les périphériques présentant des problèmes à l'aide d'un point d'exclamation jaune.
- Offre des informations détaillées sur chaque périphérique (fabricant, version du pilote, etc.).
- Accessible via le Panneau de Configuration ou en faisant un clic droit sur "Ce PC" > "Gérer" > "Gestionnaire de périphériques".

- Essentiel pour la maintenance du matériel et la résolution des problèmes de périphériques.



⚠ Warning

Si vous voyez des erreurs ici c'est que votre machine virtuelle (ou votre OS) n'a pas tous les pilotes d'installer. Si votre VM fonctionne sous Virtualbox il vous faudra les installer et pour ça il faudra connecter l'ISO des "Guest Additions" puis d'installer l'outil qui se trouve dessus. Cela vous permettra par exemple de pouvoir changer la résolution de l'écran de votre VM ou d'activer le copier/coller entre l'hôte et la machine virtuelle.

Gestion des disques

- Outil Windows pour configurer les lecteurs de stockage (disques durs, SSD, partitions).
- Permet de créer, supprimer, formater des partitions et changer les lettres de lecteur.
- Offre la possibilité de réduire ou étendre des volumes sans perdre de données.
- Affiche une représentation graphique des disques et de leurs partitions.
- Supporte la gestion des disques dynamiques et des volumes simples, étendus, et en miroir.
- Utilisé pour initialiser de nouveaux disques et créer des volumes RAID.
- Accessible via le Panneau de Gestion de l'Ordinateur ou en tapant "diskmgmt.msc" dans Exécuter.

- Indispensable pour la gestion de l'espace de stockage et l'optimisation des performances du disque.

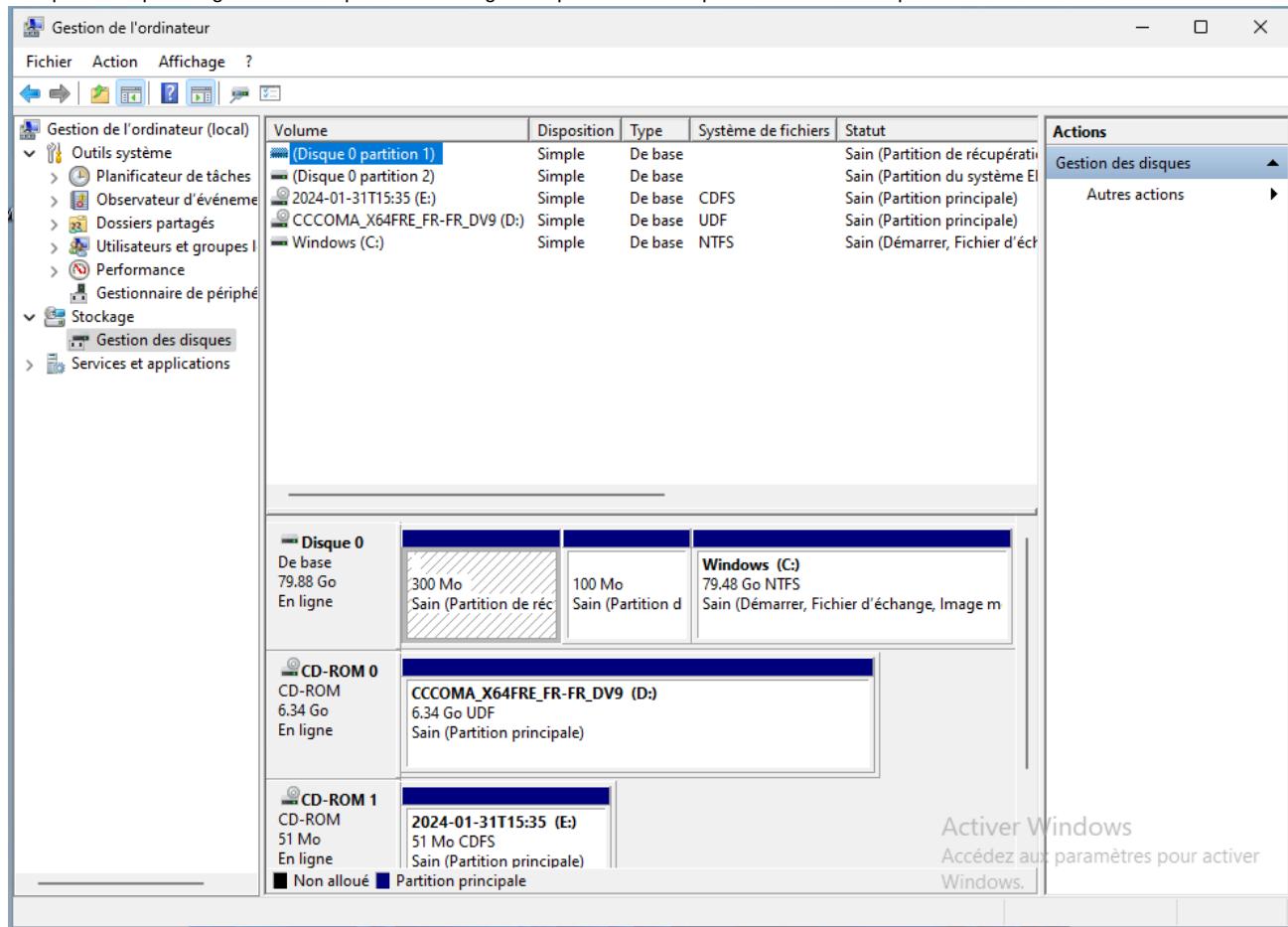
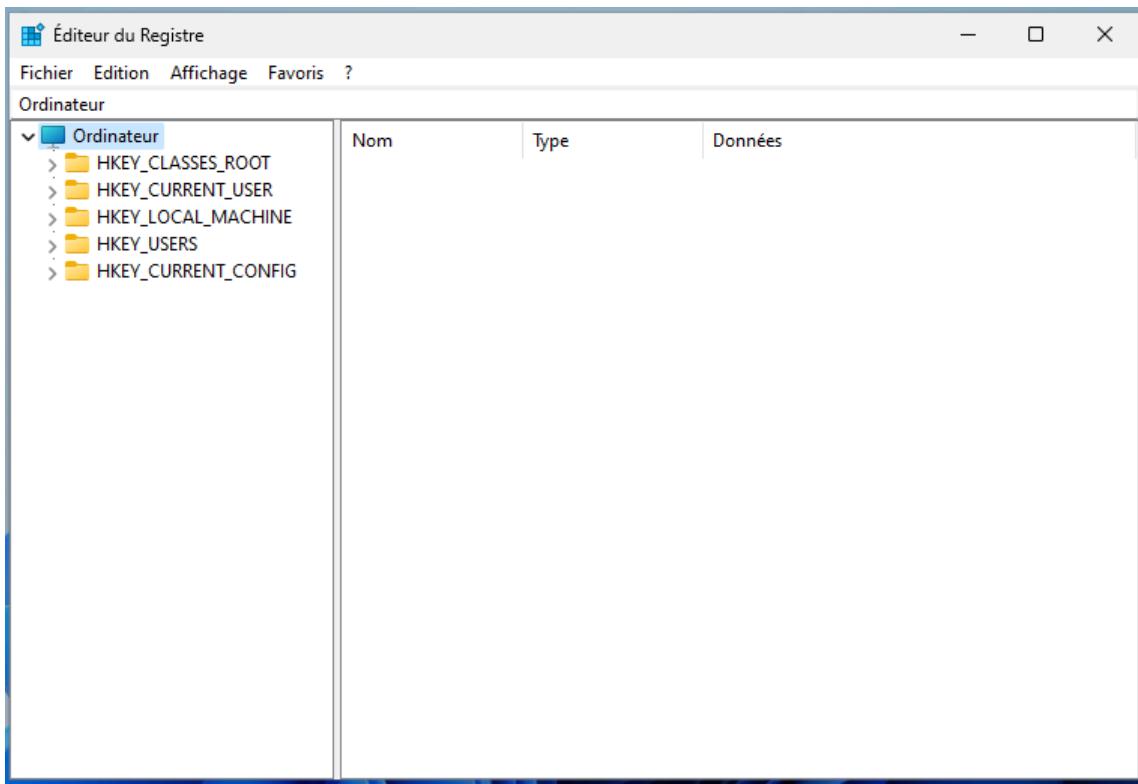


Table des registres

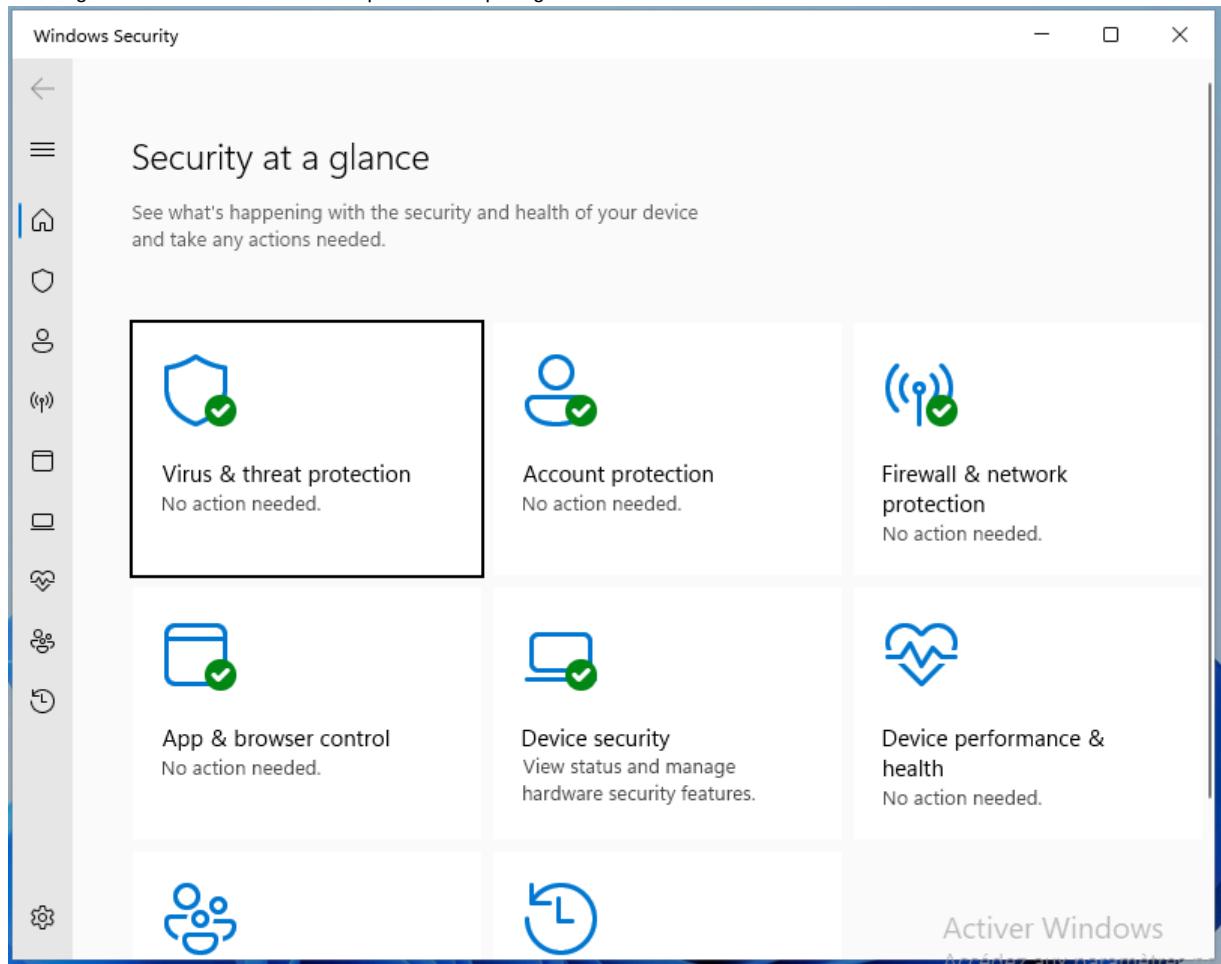
- Base de données de configuration pour le système d'exploitation et les applications.
- Contient des informations, paramètres, et options pour le matériel, les logiciels, les profils utilisateurs, et les préférences du système.
- Organisée en hiérarchie de clés et de valeurs.
- Accès via l'éditeur de registre (regedit) pour visualiser ou modifier les paramètres.
- Modifications effectuées avec précaution car les erreurs peuvent affecter la stabilité du système.
- Utilisé pour des ajustements avancés du système, la résolution de problèmes, et l'optimisation des performances.
- Les clés principales incluent HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, et HKEY_CURRENT_CONFIG.



Windows Defender

- Logiciel antivirus et anti-malware gratuit fourni par Microsoft avec Windows.
- Offre une protection en temps réel contre les logiciels malveillants, les virus, et les menaces de phishing.
- Comprend des fonctionnalités de protection du réseau, de surveillance des performances et de la santé du système.
- Permet l'exécution de scans rapides, complets, ou personnalisés pour détecter les menaces.
- Intègre une protection contre les ransomwares avec l'accès contrôlé aux dossiers.
- Met à jour automatiquement les définitions de virus pour maintenir une protection à jour.
- Peut être configuré via l'application Paramètres sous la section "Mise à jour et sécurité".

- Inclut également le Pare-feu Windows pour aider à protéger l'ordinateur contre les accès non autorisés.



Firewall

- Barrière de sécurité intégrée à Windows pour surveiller et filtrer le trafic réseau entrant et sortant.
- Protège l'ordinateur contre les accès non autorisés et aide à prévenir les cyberattaques.
- Permet de créer des règles personnalisées pour autoriser ou bloquer le trafic réseau pour des applications spécifiques.
- Offre des configurations pour les réseaux privés, publics, et de domaine, adaptant la protection en fonction du niveau de confiance du réseau.
- Inclut des fonctionnalités avancées telles que la protection contre le piratage (IPS) et la surveillance des connexions.
- Accessible via le Panneau de Configuration ou l'application Paramètres sous "Sécurité Windows".
- Fonctionne en arrière-plan et peut être configuré pour envoyer des alertes en cas d'activités suspectes.

Zones Public et Privé du Pare-feu

Zone Privée :

- Réseaux considérés comme sûrs, tels que le réseau domestique ou celui d'un lieu de travail.
- Le pare-feu applique des règles moins restrictives, permettant une plus grande connectivité et partage de fichiers/ressources.
- Idéal pour les environnements où l'utilisateur fait confiance aux autres appareils connectés au réseau.

Zone Publique :

- Réseaux publics tels que ceux des cafés, des aéroports, ou d'autres lieux publics.
- Le pare-feu applique des règles plus strictes pour minimiser les risques d'accès non autorisé et d'attaques.
- Les fonctionnalités de partage et la découverte de réseau sont généralement désactivées pour renforcer la sécurité.

Sélection de la Zone :

- Windows demande généralement à l'utilisateur de spécifier le type de réseau (public ou privé) lors de la première connexion à un nouveau réseau.
- Cette classification influence le comportement du pare-feu et d'autres paramètres de sécurité pour protéger l'ordinateur en fonction du niveau de confiance du réseau.

Gestion et Configuration :

- Les utilisateurs peuvent modifier le type de réseau via les Paramètres de réseau ou le Centre Réseau et Partage.

- Il est recommandé de choisir la zone privée pour les réseaux sûrs et la zone publique pour les réseaux inconnus ou non sécurisés

Windows Security

(i) Firewall & network protection

Who and what can access your networks.

Domain network
Firewall is on.

Private network
Firewall is on.

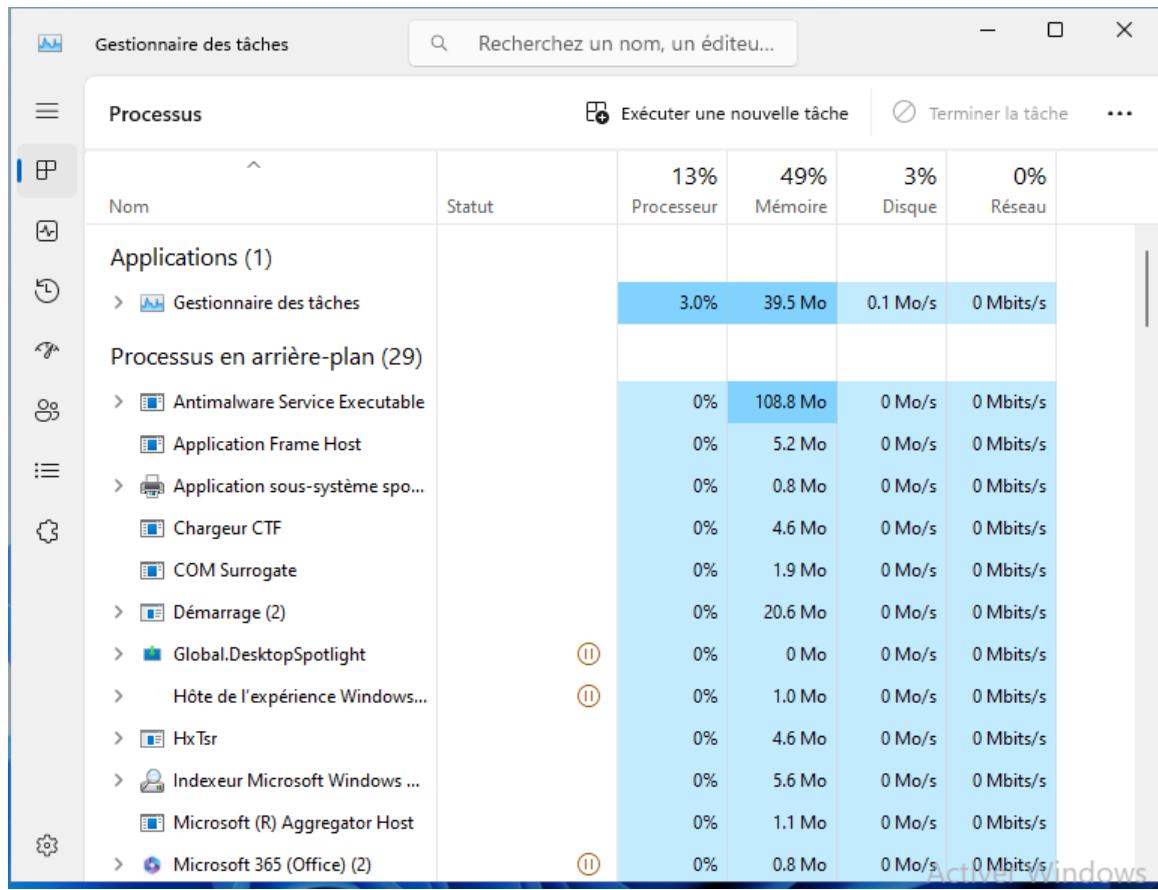
Public network (active)
Firewall is on.

[Allow an app through firewall](#)
[Network and Internet troubleshooter](#)
[Firewall notification settings](#)
[Advanced settings](#)
[Restore firewalls to default](#)

Activer Windows
Accédez aux paramètres pour activer Windows

Gestionnaire des tâches

- Outil système permettant de surveiller les processus et applications en cours d'exécution sur Windows.
- Affiche l'utilisation des ressources système telles que le processeur, la mémoire, le disque, et le réseau.
- Permet de terminer des processus ou applications non répondantes pour libérer des ressources.
- Offre un aperçu des performances du système, incluant l'historique de l'utilisation du CPU, de la mémoire, etc.
- Accessible en faisant un clic droit sur la barre des tâches et en sélectionnant "Gestionnaire des tâches" ou en utilisant le raccourci clavier Ctrl+Shift+Esc.



The screenshot shows the Windows Task Manager window titled "Gestionnaire des tâches". The main area is a table titled "Processus" with columns: Nom, Statut, Processeur, Mémoire, Disque, and Réseau. The "Processeur" column is highlighted in blue. The table lists several processes, including "Gestionnaire des tâches" (using 3.0% CPU), "Antimalware Service Executable" (using 0% CPU, 108.8 Mo memory), and various system services like "Application Frame Host" and "Chargeur CTF" (both using 0% CPU). Some processes have a yellow warning icon next to them.

Nom	Statut	Processeur	Mémoire	Disque	Réseau
Applications (1)		3.0%	39.5 Mo	0.1 Mo/s	0 Mbits/s
Processus en arrière-plan (29)		0%	108.8 Mo	0 Mo/s	0 Mbits/s
> Antimalware Service Executable		0%	5.2 Mo	0 Mo/s	0 Mbits/s
> Application Frame Host		0%	0.8 Mo	0 Mo/s	0 Mbits/s
> Application sous-système spo...		0%	4.6 Mo	0 Mo/s	0 Mbits/s
> Chargeur CTF		0%	1.9 Mo	0 Mo/s	0 Mbits/s
> COM Surrogate		0%	20.6 Mo	0 Mo/s	0 Mbits/s
> Démarrage (2)	(II)	0%	0 Mo	0 Mo/s	0 Mbits/s
> Global/DesktopSpotlight	(II)	0%	1.0 Mo	0 Mo/s	0 Mbits/s
> Hôte de l'expérience Windows...	(II)	0%	4.6 Mo	0 Mo/s	0 Mbits/s
> HxTsr		0%	5.6 Mo	0 Mo/s	0 Mbits/s
> Indexeur Microsoft Windows ...		0%	1.1 Mo	0 Mo/s	0 Mbits/s
> Microsoft (R) Aggregator Host		0%	0.8 Mo	0 Mo/s	0 Mbits/s
> Microsoft 365 (Office) (2)	(II)	0%	0.8 Mo	0 Mo/s	0 Mbits/s

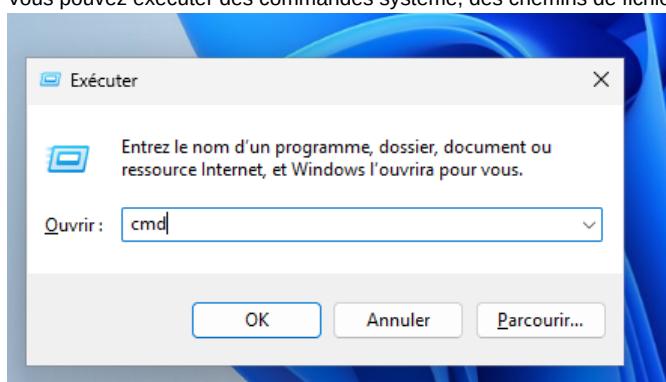
Démo Couper Explorer.exe et le relancer

Applications de démarrage

- Programmes configurés pour se lancer automatiquement au démarrage de Windows.
- Peuvent inclure des utilitaires système, des applications de messagerie, des lanceurs d'applications, etc.
- Affectent le temps de démarrage du système et l'utilisation des ressources dès le démarrage.

Exécuter

- Permet d'exécuter des commandes, des programmes, des fichiers ou d'accéder à certaines fonctionnalités Windows rapidement.
- Utilisez le raccourci clavier "Win + R" pour ouvrir rapidement la fenêtre Exécuter.
- Exemples de commandes courantes :
 - "cmd" : Ouvre l'invite de commande.
 - "msconfig" : Lance l'outil de configuration du système.
 - "appwiz.cpl" : Ouvre la fenêtre "Programmes et fonctionnalités" pour désinstaller des programmes.
 - "control" : Accède au Panneau de configuration.
 - "calc" : Lance la calculatrice Windows.
- Vous pouvez exécuter des commandes système, des chemins de fichiers, et même des URL en utilisant la fenêtre Exécuter

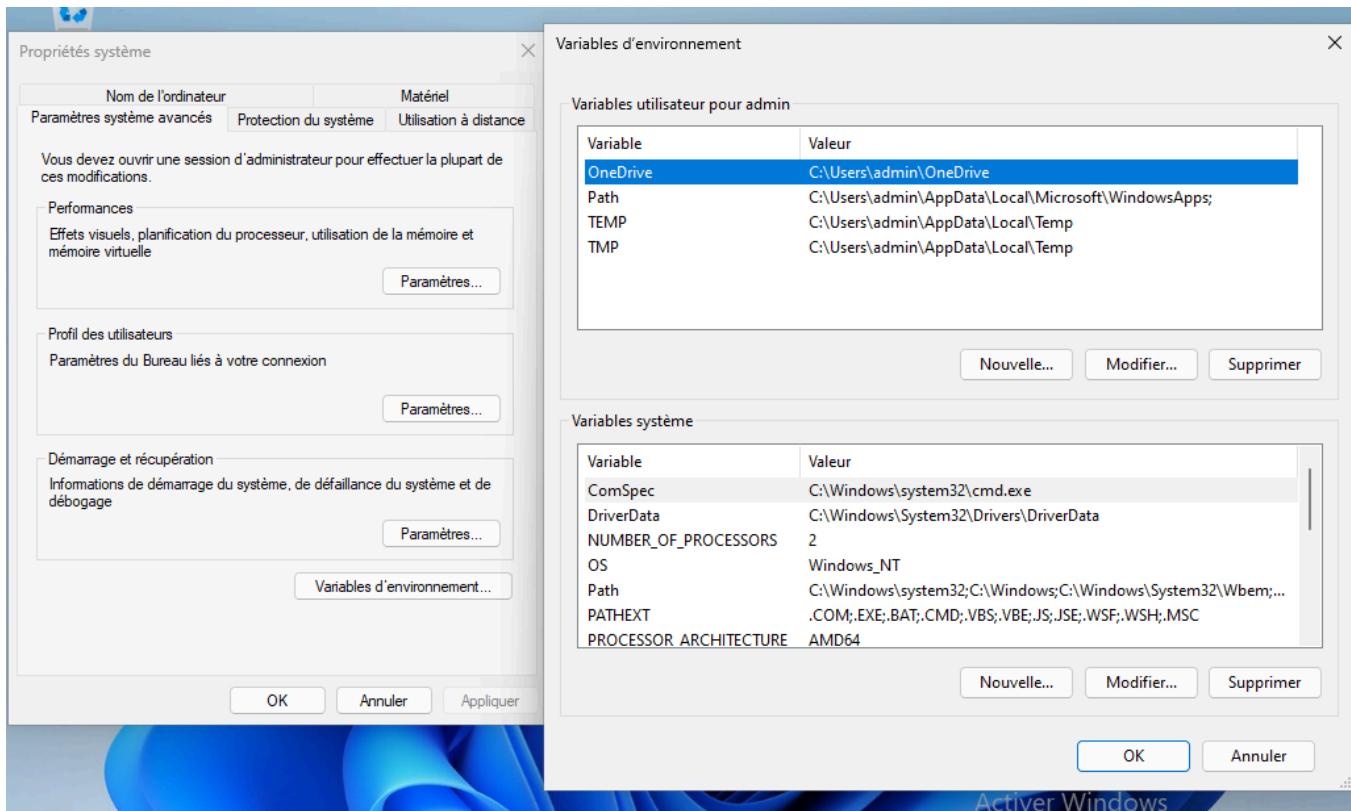


Gestion des Paths

Gestion des PATH :

- Le PATH est une variable d'environnement qui spécifie les répertoires dans lesquels le système d'exploitation recherche les exécutables.

- Permet d'exécuter des fichiers exécutables depuis la ligne de commande sans spécifier le chemin complet.
- Modification du PATH :
- Accessible via les Propriétés Système > Paramètres système avancés > Variables d'environnement.
 - Peut être configuré globalement (pour tous les utilisateurs) ou localement (pour l'utilisateur courant).
- Ajouter au PATH :
- Permet d'ajouter de nouveaux répertoires contenant des exécutables auxquels on souhaite accéder globalement.
 - Utile pour les développeurs ou pour des applications nécessitant un accès rapide depuis n'importe quel répertoire.
- Impact :
- Facilite l'exécution de programmes et de scripts sans naviguer dans leur répertoire.
 - Doit être modifié avec précaution pour éviter de perturber le fonctionnement d'autres programmes.
- Conseils :
- Ajouter de nouveaux chemins à la fin pour éviter de surcharger les entrées existantes.
 - Vérifier et supprimer les entrées obsolètes pour maintenir la variable PATH propre et efficace.



Quelques raccourcis clavier

Raccourcis Windows généraux :

- Win : Ouvre ou ferme le menu Démarrer.
- Win + D : Affiche ou masque le bureau.
- Win + E : Ouvre l'Explorateur de fichiers.
- Win + L : Verrouille l'écran.
- Win + Tab : Ouvre la vue des tâches (Task View) pour gérer les bureaux virtuels.
- Alt + Tab : Permet de basculer entre les applications ouvertes.
- Alt + F4 : Ferme l'application active.
- Win + Flèche gauche/droite : Ancrer une fenêtre à gauche ou à droite de l'écran.
- Alt + Enter : Affiche les propriétés d'un fichier ou d'un dossier sélectionné.

Raccourcis dans le gestionnaire de tâches :

- Ctrl + Shift + Échap : Ouvre le gestionnaire de tâches.
- Ctrl + Alt + Suppr : Affiche un menu avec des options telles que le verrouillage, la déconnexion, le gestionnaire de tâches, etc.

Raccourcis de capture d'écran :

- Win + Shift + S : Ouvre l'outil de capture d'écran pour sélectionner une zone.
- Win + PrtScn : Capture tout l'écran et enregistre l'image dans le dossier "Captures d'écran".
- Alt + PrtScn : Capture la fenêtre active et la copie dans le presse-papiers.

Raccourcis pour la gestion des fenêtres :

- Win + Flèche haut : Maximise la fenêtre active.
- Win + Flèche bas : Réduit la fenêtre active ou la restaure si elle est réduite.
- Win + Flèche gauche/droite : Ancre la fenêtre à gauche ou à droite de l'écran.

- Win + Maj + Flèche gauche/droite : Déplace la fenêtre active vers un autre écran (si plusieurs écrans sont utilisés).
Raccourcis dans l'Explorateur de fichiers :
- Ctrl + C : Copie les fichiers sélectionnés.
- Ctrl + X : Coupe les fichiers sélectionnés.
- Ctrl + V : Colle les fichiers copiés/coupés.
- F2 : Renomme le fichier sélectionné.
- Alt + P : Affiche le volet de prévisualisation.

Important

Le plus IMPORTANT de TOUS! Shift + Ctrl + Win+ Alt + L. Je vous laisse tester!

SInon, Shift + Ctrl + Win+ Alt + O

Sinon, Shift + Ctrl + Win+ Alt + T

Bitlocker

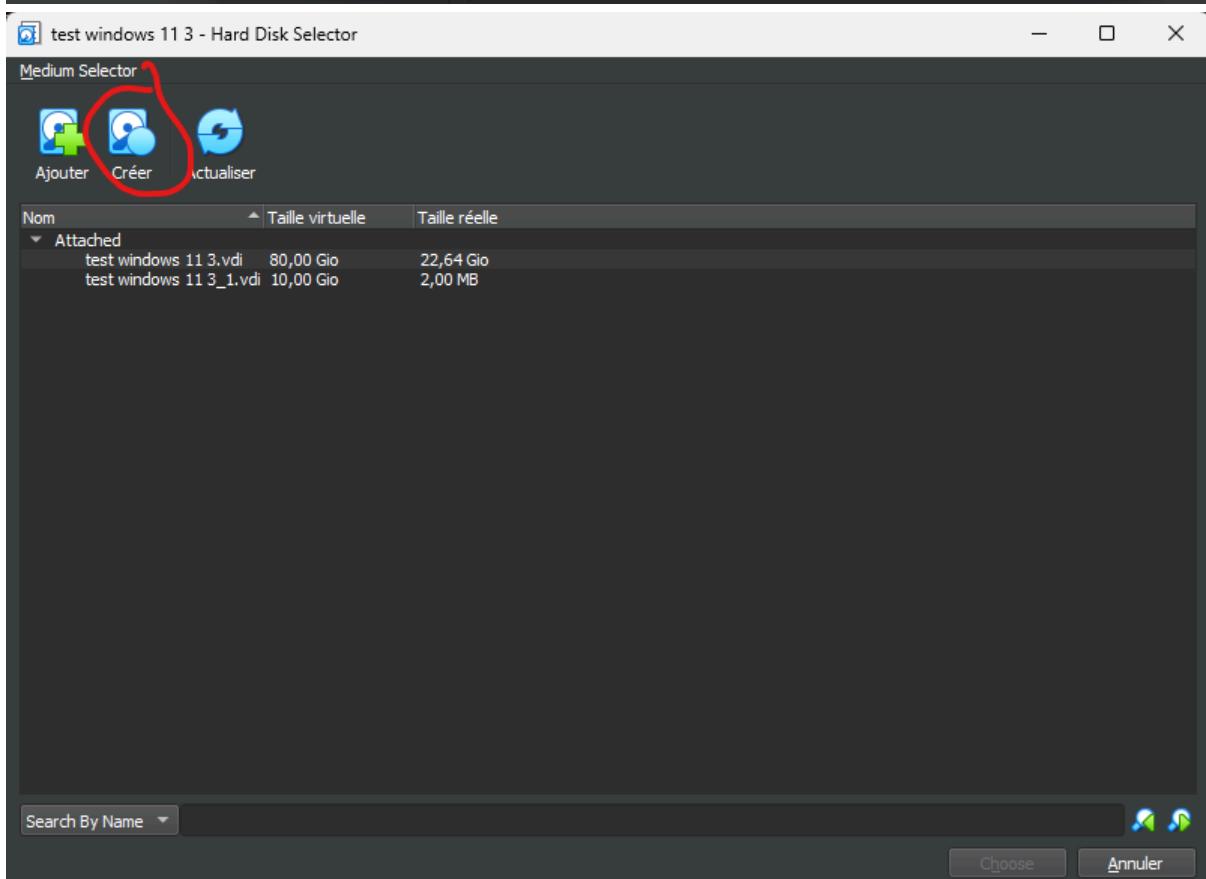
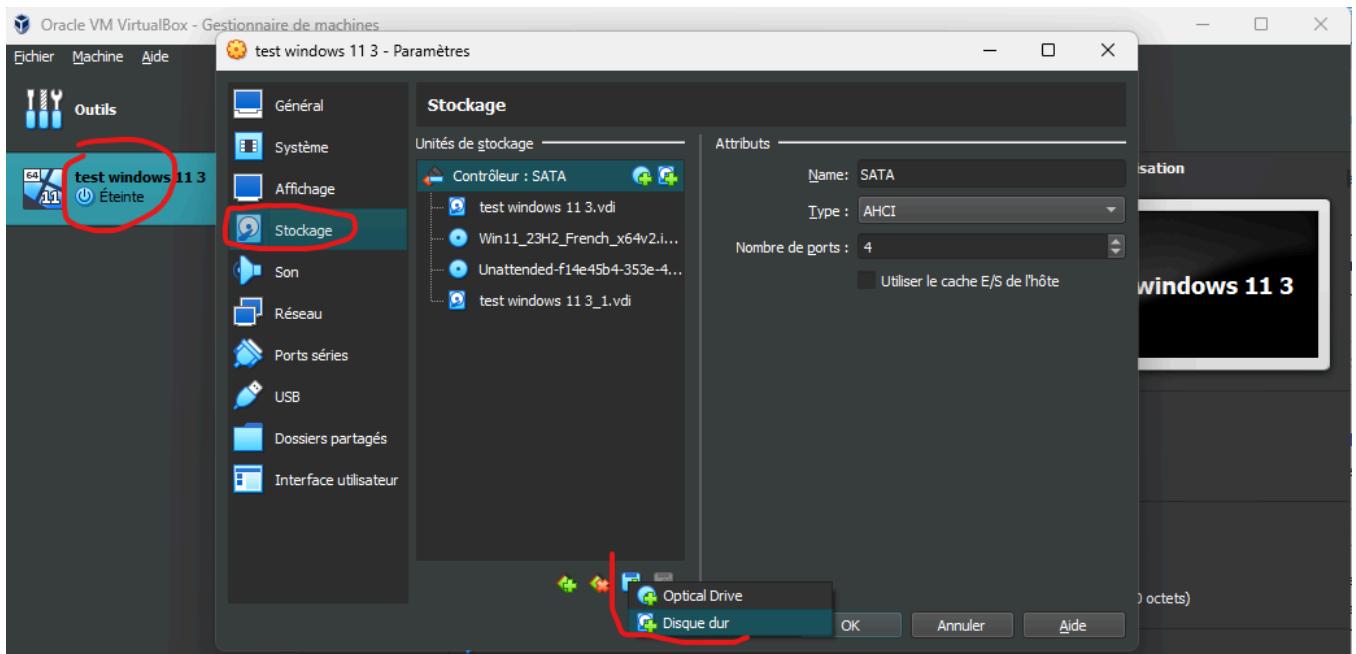
- BitLocker est conçu pour protéger les données stockées sur des disques durs et des lecteurs à l'aide du chiffrement.
- Il chiffre l'intégralité du contenu d'un disque, y compris le système d'exploitation, les fichiers et les données.
- BitLocker peut empêcher l'accès aux données sans une authentification appropriée, comme un mot de passe, un lecteur de carte à puce ou une clé USB.
- Compatibilité matérielle :
 - BitLocker nécessite un module TPM (Trusted Platform Module) pour renforcer la sécurité matérielle.
 - Vous pouvez également utiliser BitLocker sans TPM en utilisant une méthode alternative, comme une clé USB d'authentification.
- Gestion des clés :
 - BitLocker génère des clés de chiffrement qui sont stockées en toute sécurité dans le TPM ou d'autres méthodes d'authentification.
 - Les administrateurs peuvent sauvegarder des clés de récupération pour accéder aux données en cas d'oubli du mot de passe.

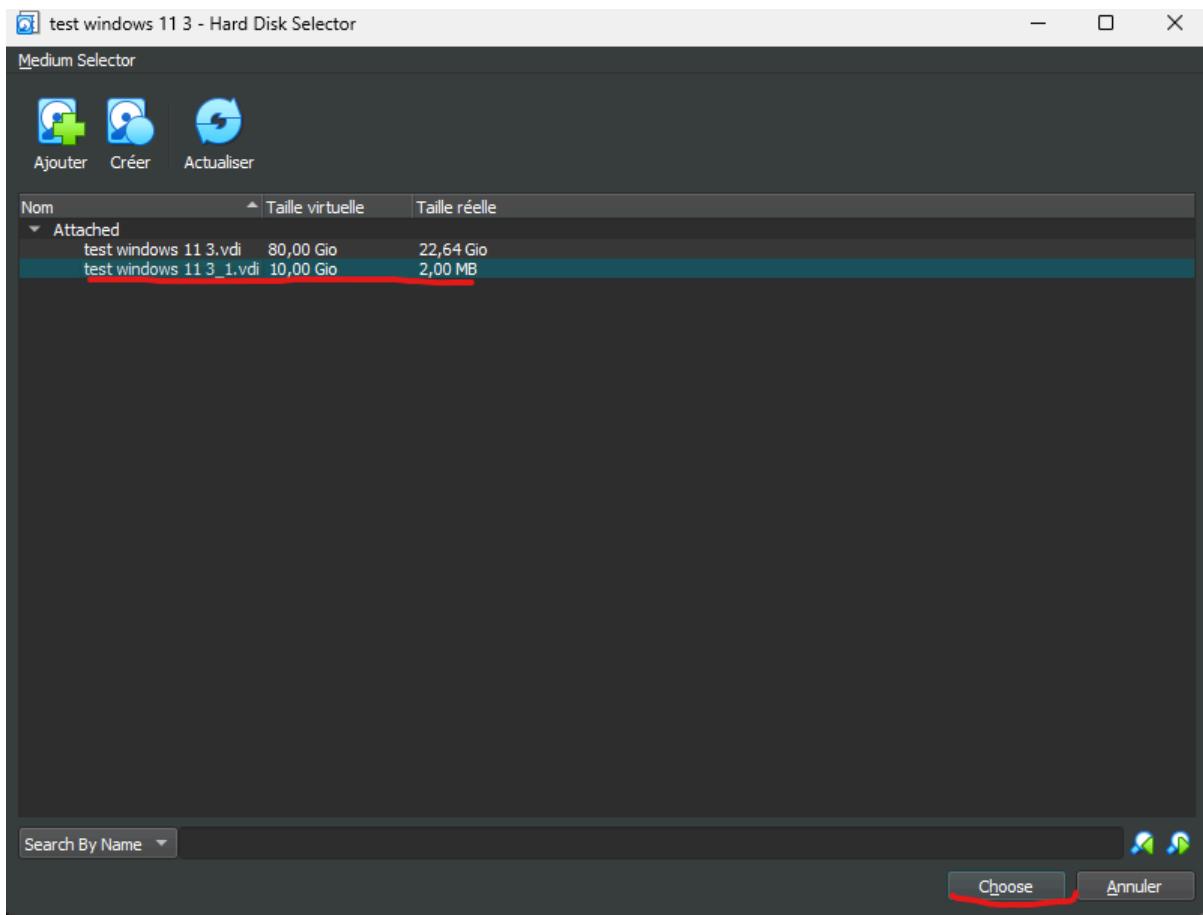
Les backups

Vous devriez consulter le cours [Cours Les bases du backups](#)

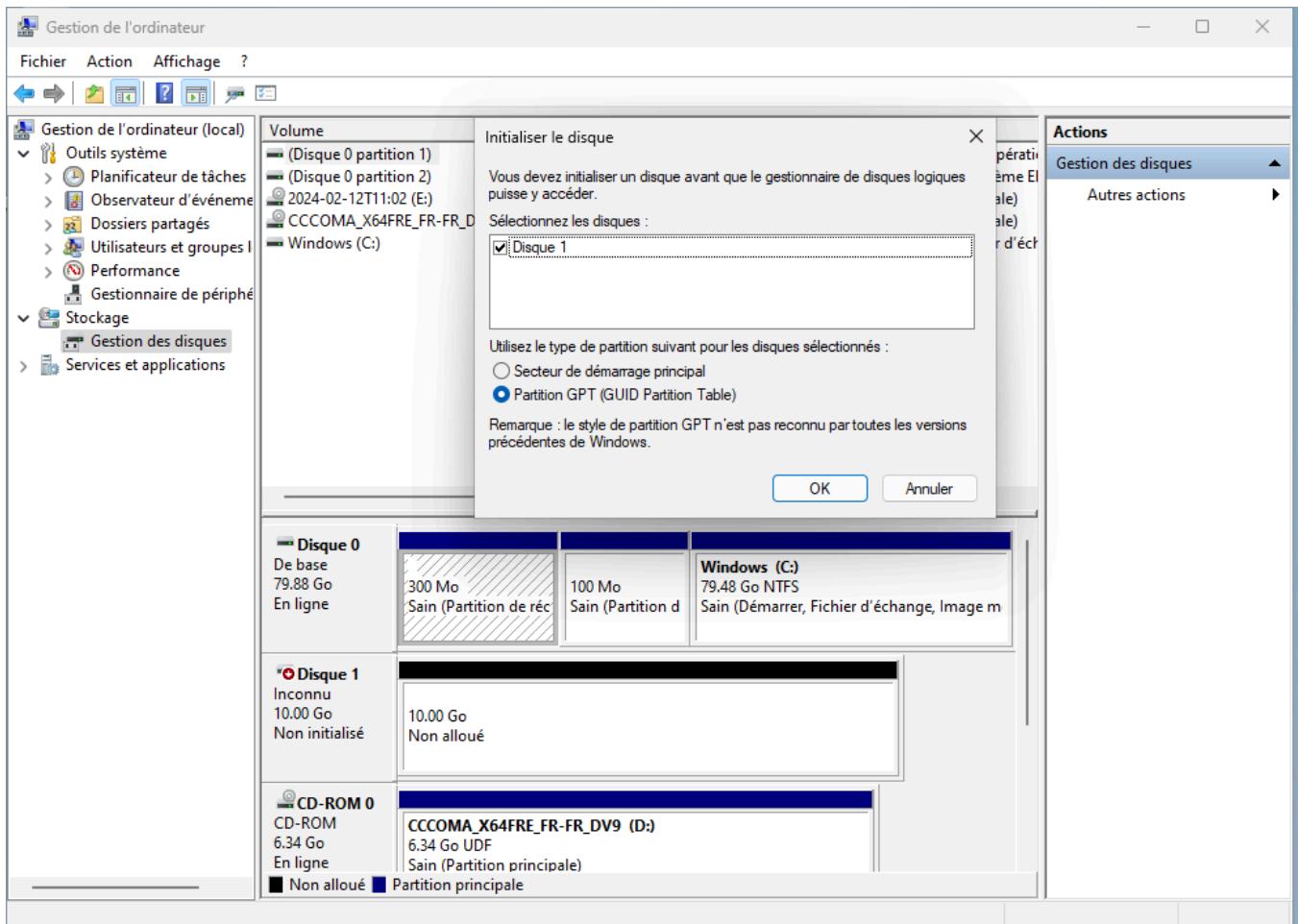
Ajouter un disque dans Win11

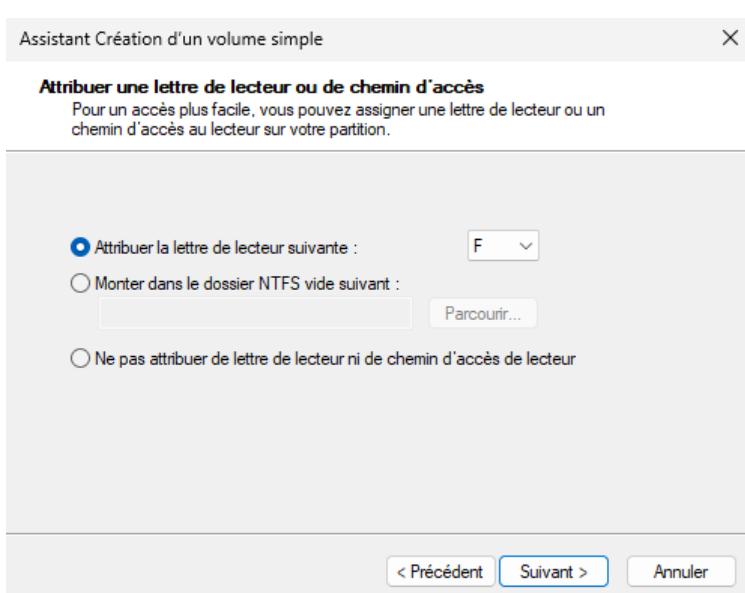
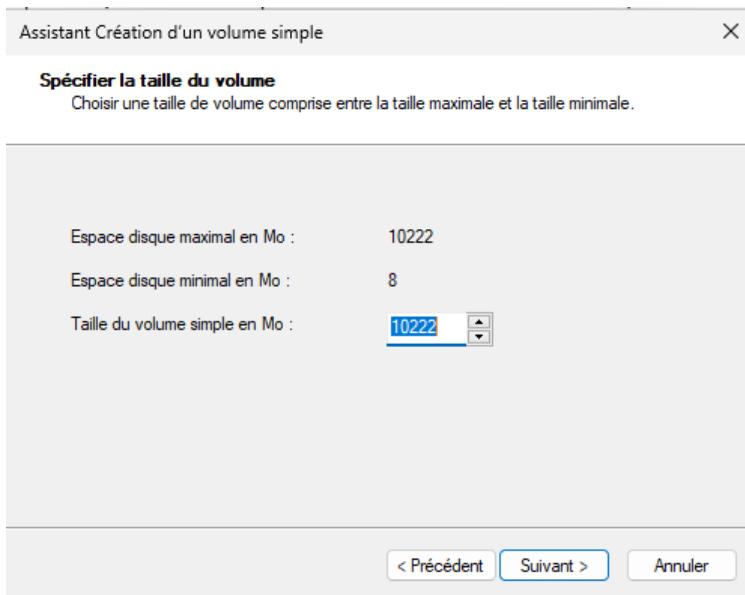
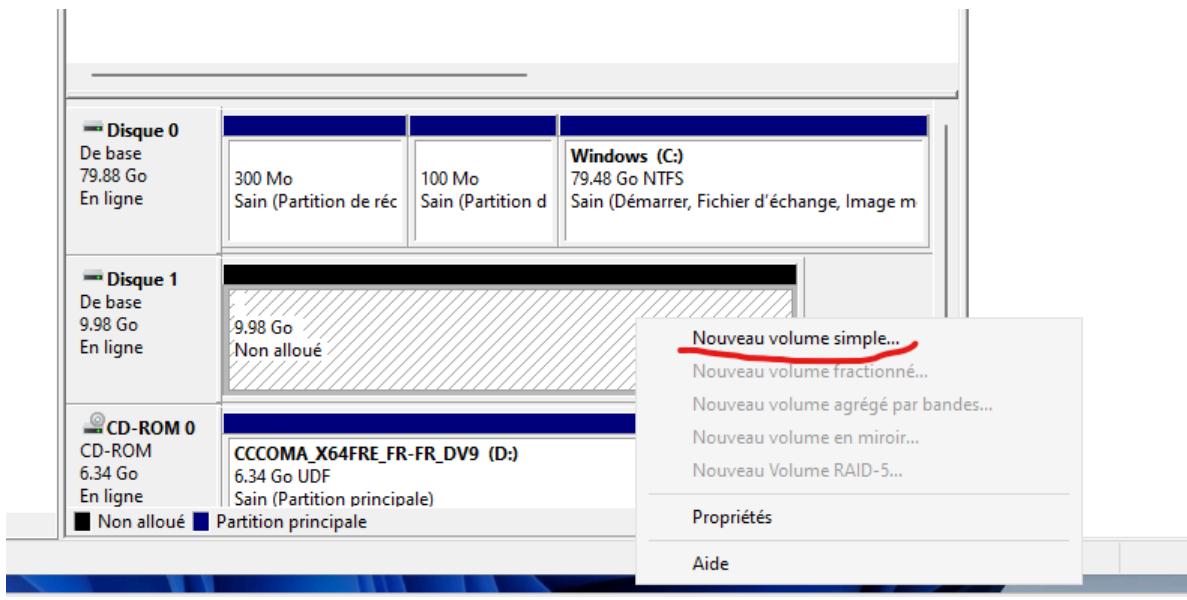
On pourrait le faire pour de vrai... mais on va plutôt continuer sur notre Machine Virtuelle!

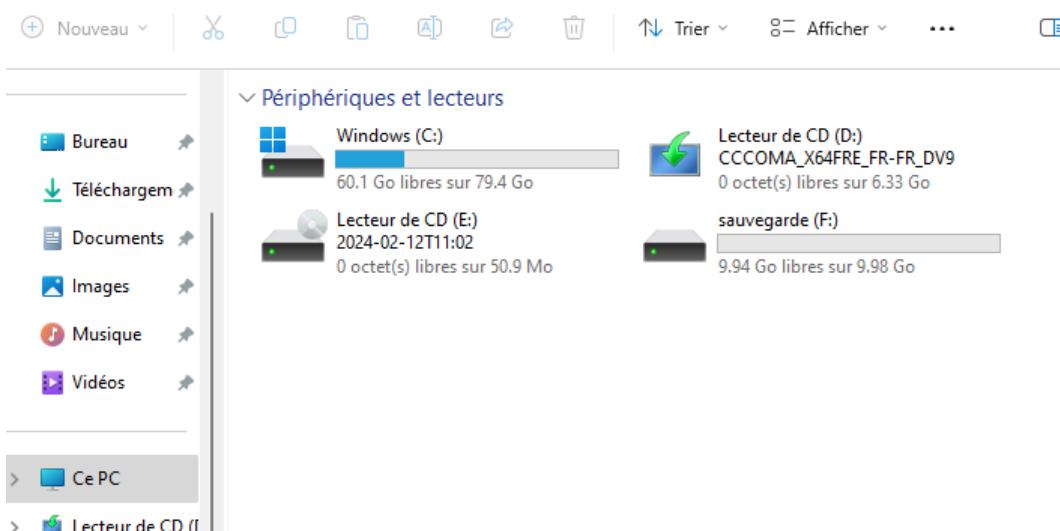
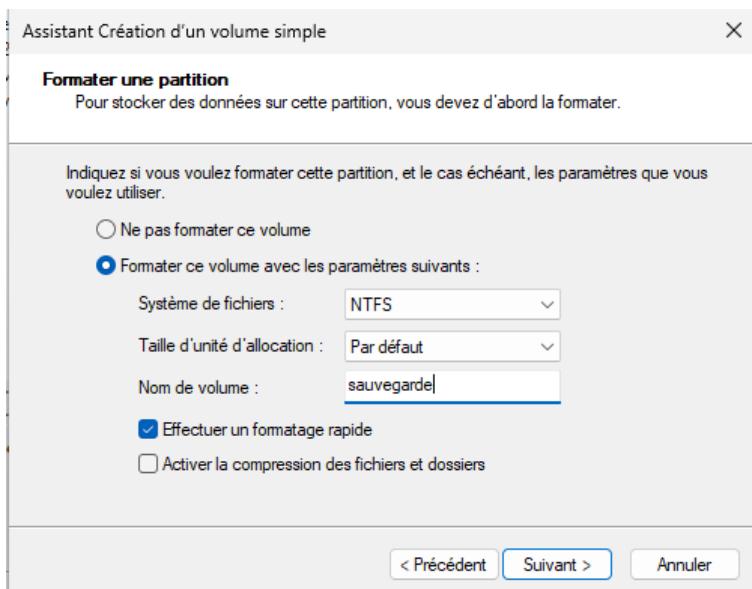




Maintenant on passe dans windows:

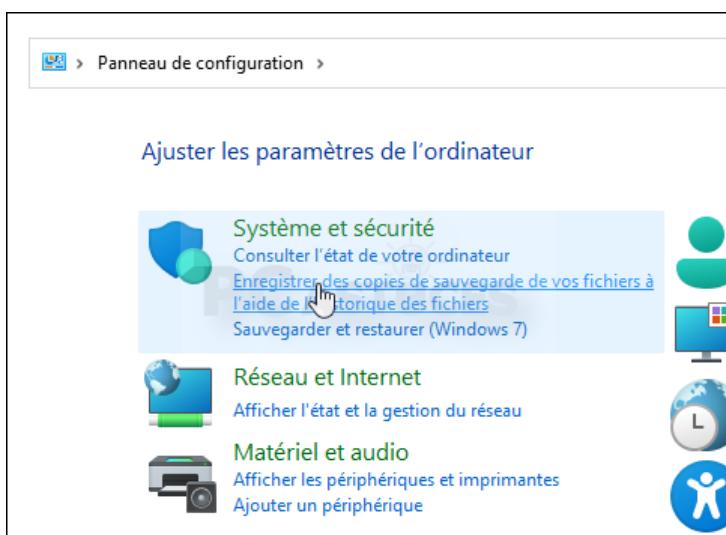






Créer un volume de sauvegarde

Nous allons utiliser le volume précédent pour configurer Windows afin qu'il fasse des sauvegarde automatique sur ce nouveau volume.



Historique des fichiers

Page d'accueil du panneau de configuration

Restaurer des fichiers personnels

Sélectionner un lecteur

Exclure des dossiers

Paramètres avancés

Conservez un historique

L'historique des fichiers

Copier les fichiers à partir de :

Copier les fichiers vers :

Sélectionner un lecteur d'historique des fichiers

Sélectionnez un lecteur dans la liste suivante ou entrez un emplacement réseau.

Lecteurs disponibles	Espace libre	Espace total
sauvegarde (F:)	9.94 Go	9.98 Go

Ajouter un emplacement réseau

Afficher tous les emplacements réseau

Conservez un historique de vos fichiers.

L'historique des fichiers enregistre des copies de vos fichiers afin que vous puissiez les récupérer s'ils sont perdus ou endommagés.

L'historique des fichiers est désactivé.

Copier les fichiers à partir de : Bibliothèques, Bureau, Contacts et Favoris

Copier les fichiers vers :

sauvegarde (F:) 9.94 Go disponible(s) sur 9.98 Go

Activer

Accueil

Galerie

OneDrive

Bureau

Téléchargement

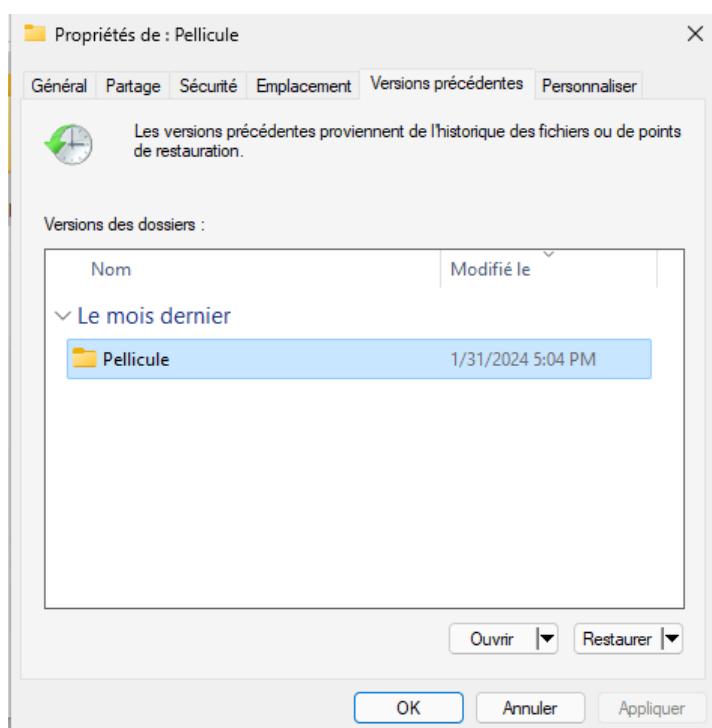
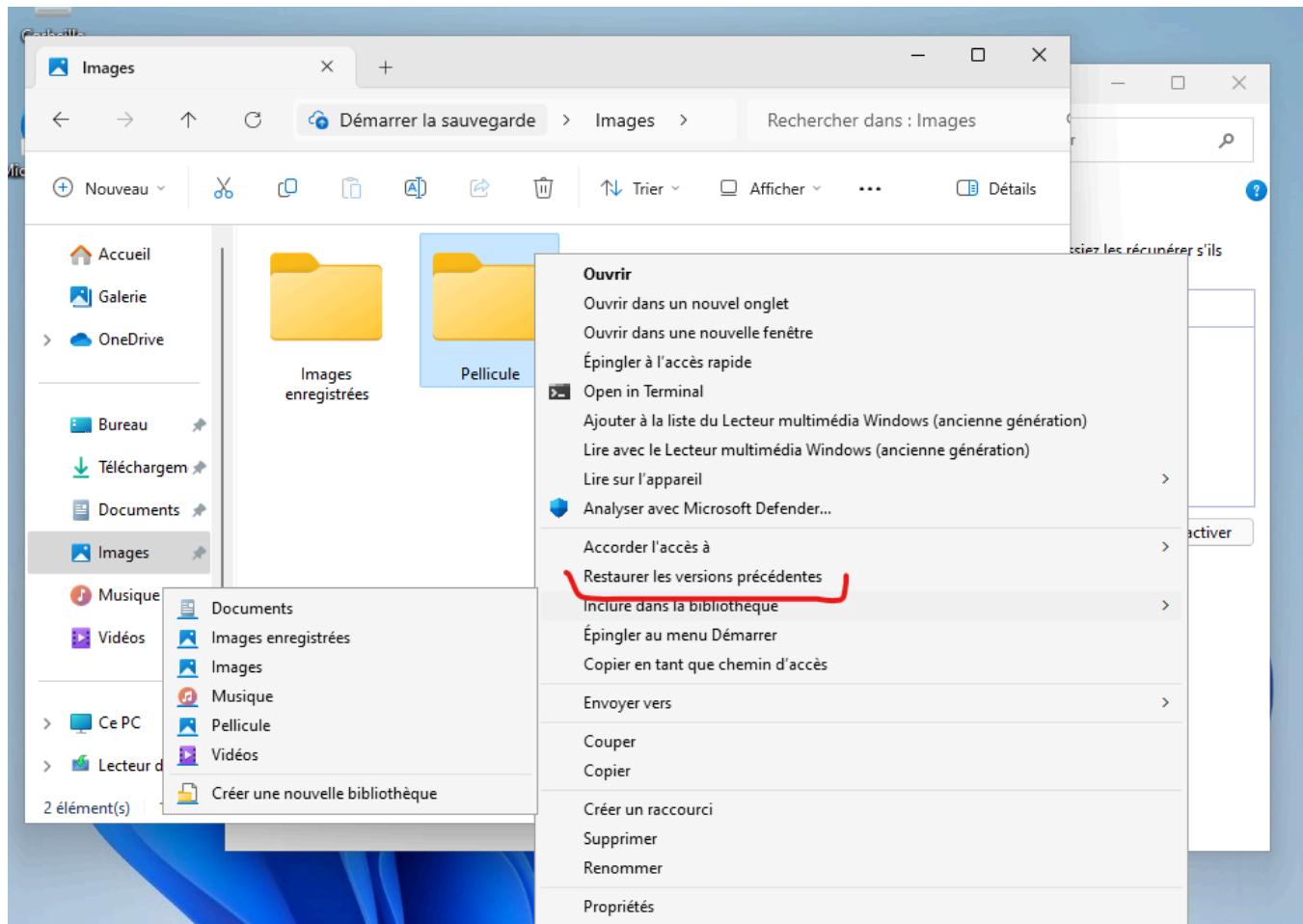
Documents

Images

Musique

Vidéos

Nom	Modifié le	Type	Taille
FileHistory	2/12/2024 12:09 PM	Dossier de fichiers	



D'autres outils de sauvegarde

Orienté poste de travail Perso / Pro :

- Cobian Backup
 - Freefilesync
 - Syncback
 - Etc.
- Orienté serveur :
- Veeam Backup
 - Plein d'autres solutions propre

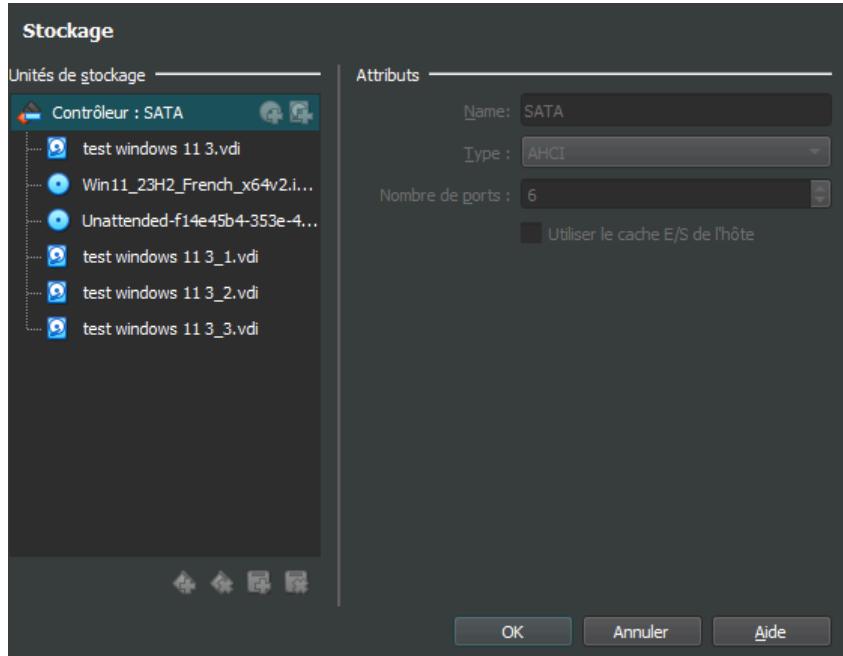
- Scripting
- Etc.

Le Raid

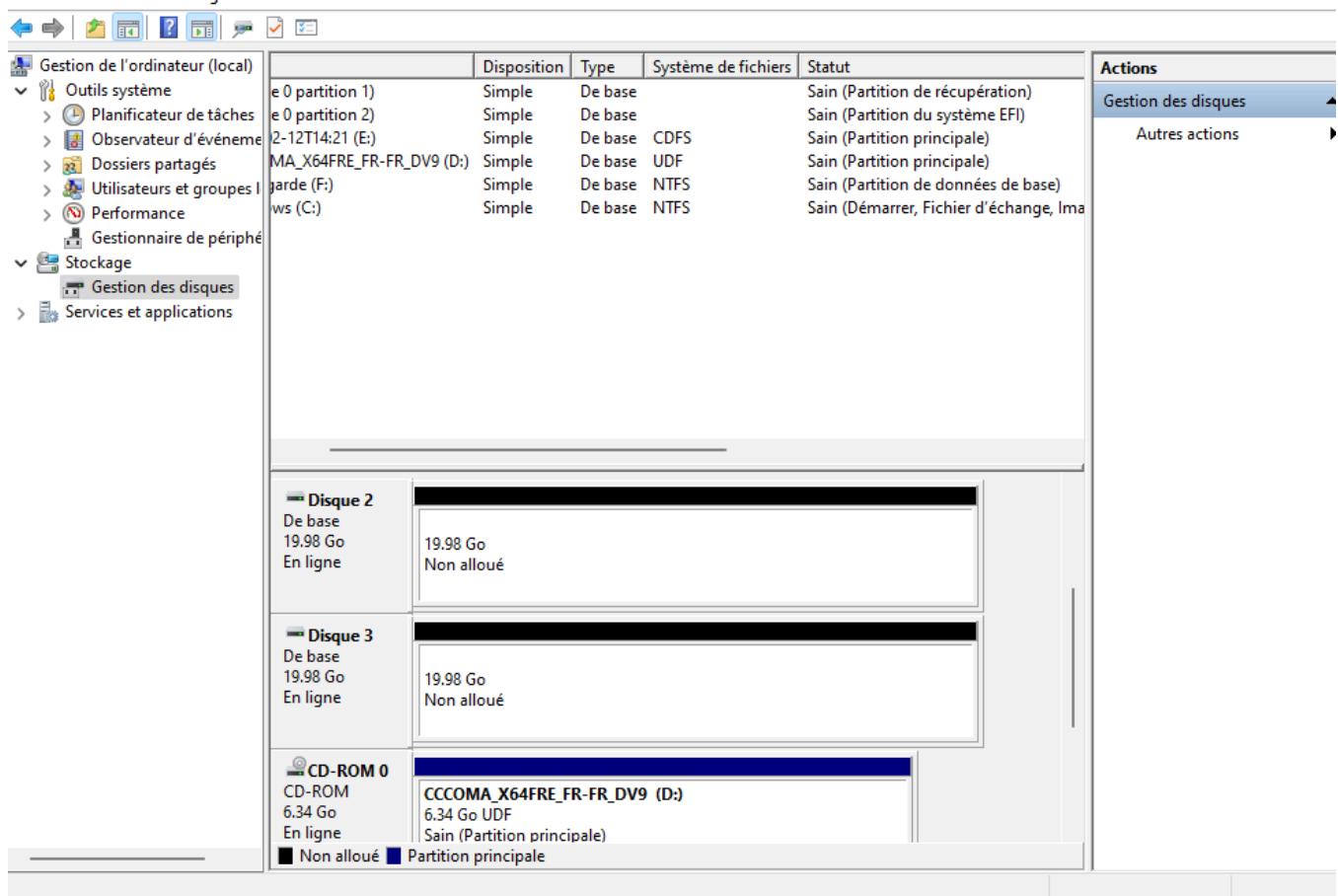
Vous devriez aller voir le cours [Cours Les bases du RAID](#)

Créer un RAID 1 logiciel sous W11

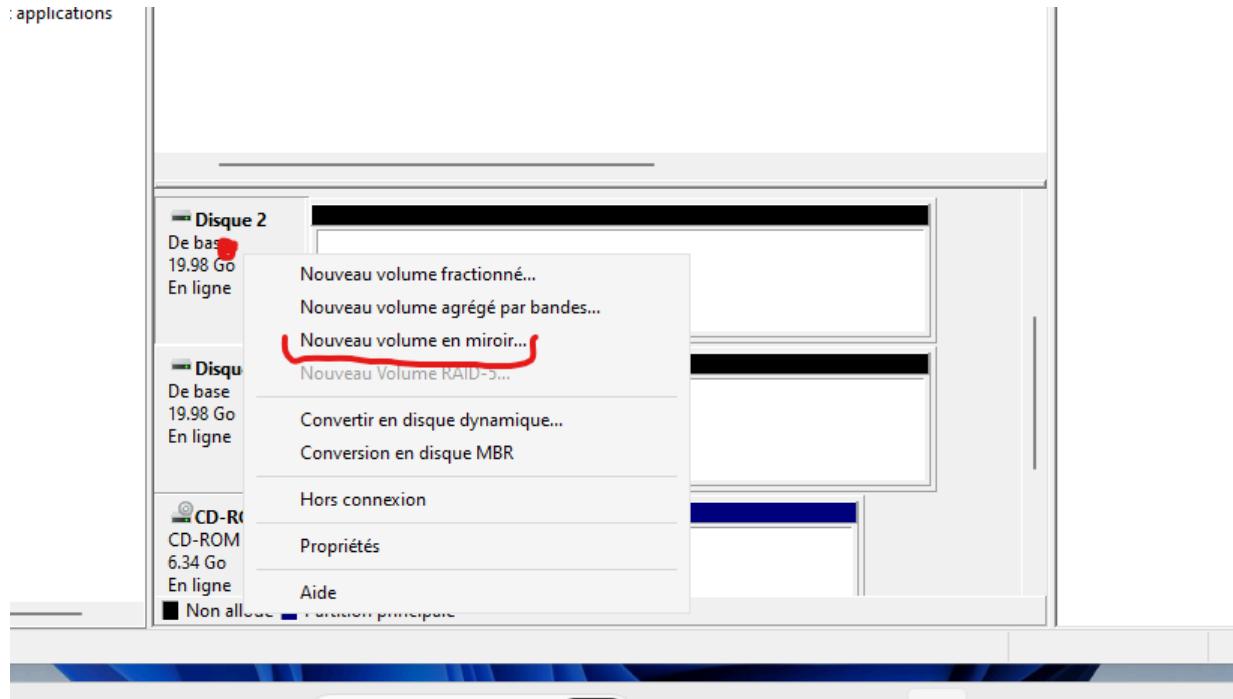
Créer 2 disques dans votre VM



Les disques dans le gestionnaire de disque de W11



Selectionner Nouveau volume en miroir...



Choisissez les disques pour le raid

Sélectionner les disques
Vous pouvez sélectionner les disques et fixer la taille de disque pour ce volume.

Disponible :

- < Supprimer
- < Supprimer tout

Sélectionné :

- Disque 2 20462 Mo
- Disque 3 20462 Mo

Taille totale du volume en mégaoctets (Mo) :

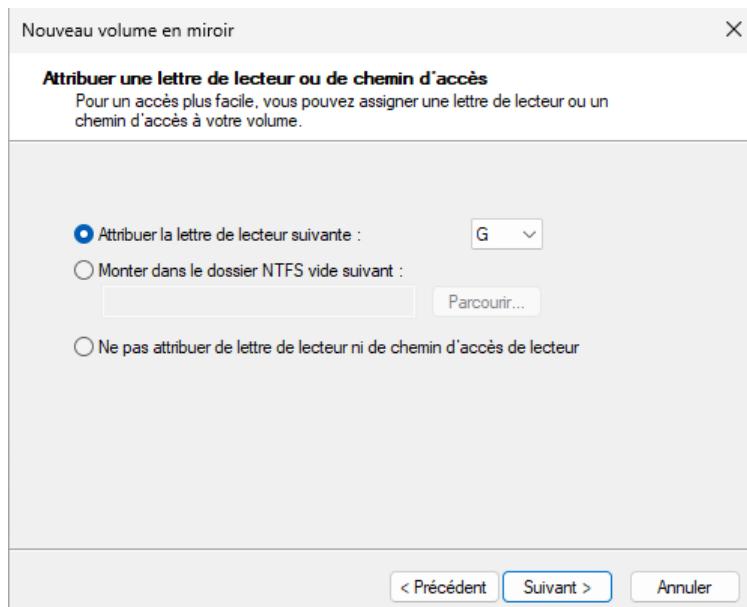
Espace disque disponible maximal en Mo :

Sélectionnez l'espace en Mo : ▲ ▼

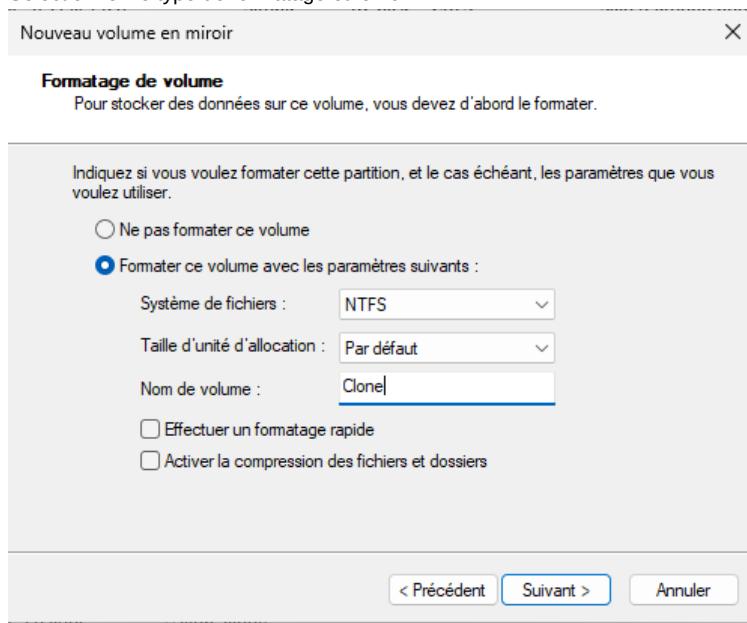
< Précédent Suivant > Annuler

En ligne Non alloué

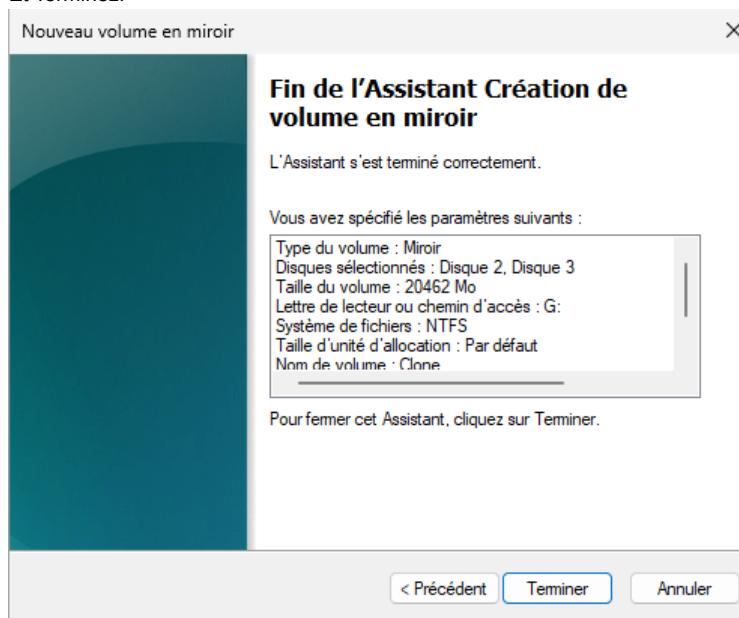
Sélectionnez la lettre du lecteur



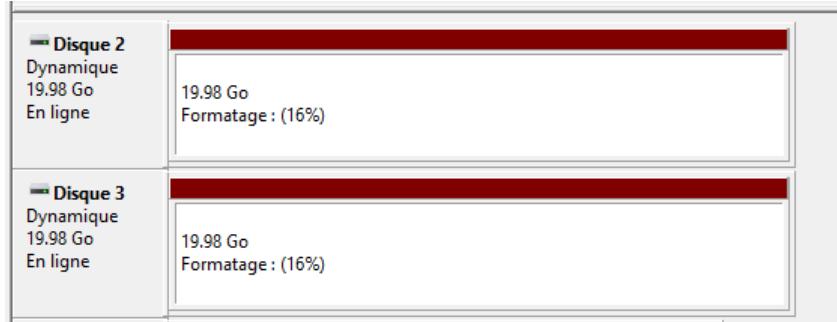
Sélectionnez le type de formatage et le nom



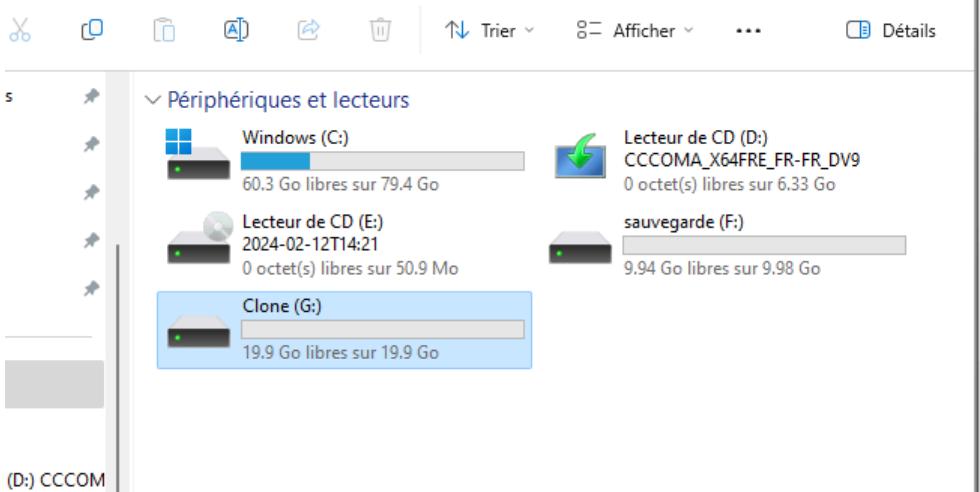
Et Terminez!



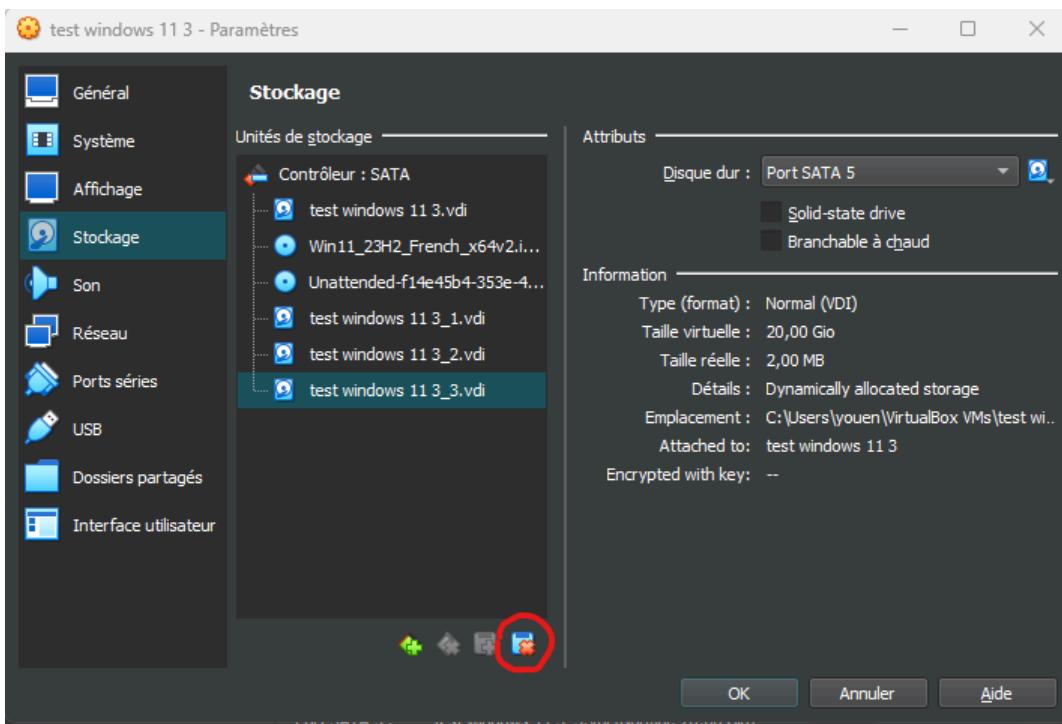
Mise en place des disques:



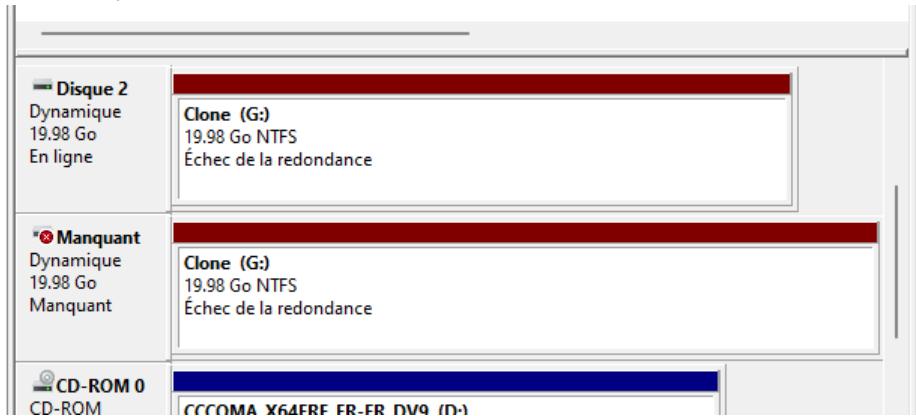
Vous pouvez trouver votre disque:



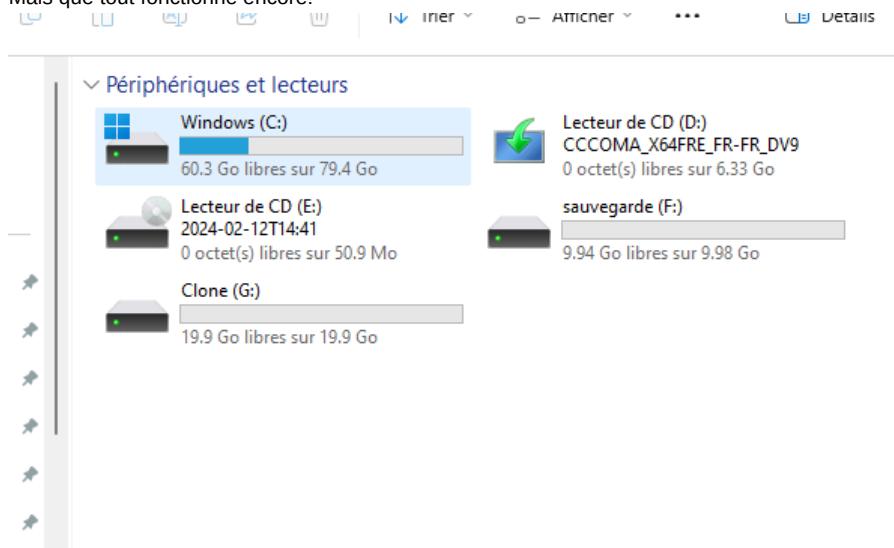
Détruissez un disque!



Constatez sa disparition



Mais que tout fonctionne encore!



Reconstruire le Raid

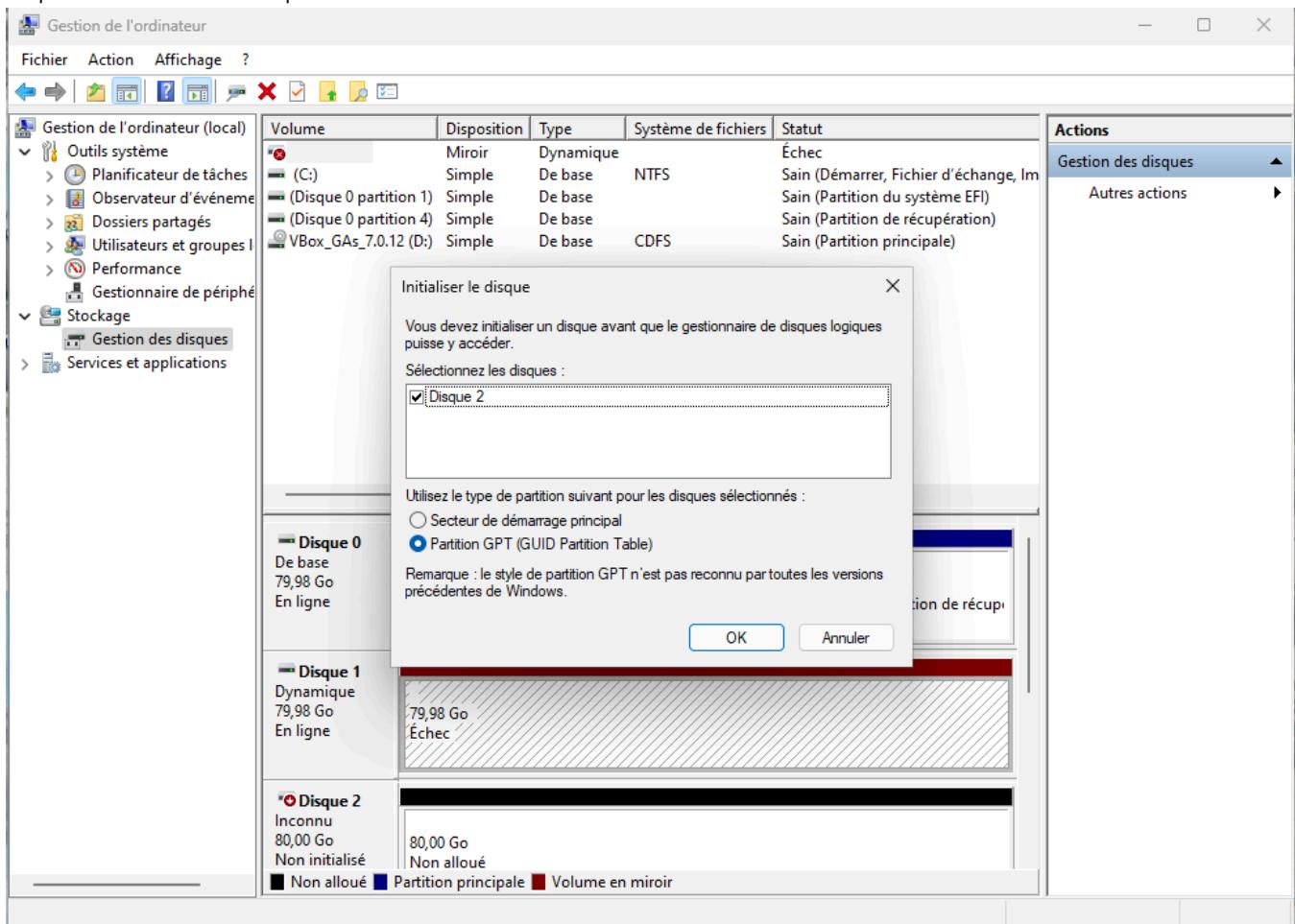
Pour reconstruire le RAID il va falloir que je retourne ajouter un nouveau disque à ma VM. Je ne remet de screen, ce sont les mêmes qu'au dessus.

Une fois le disque rajouter, je rallume ma VM et je vais retourner dans la gestion de l'ordinateur puis des disques.

⚠️ Warning

Attention a bien creer un nouveau disque et ne pas rattacher le disque existant!

On peut activer le nouveau disque

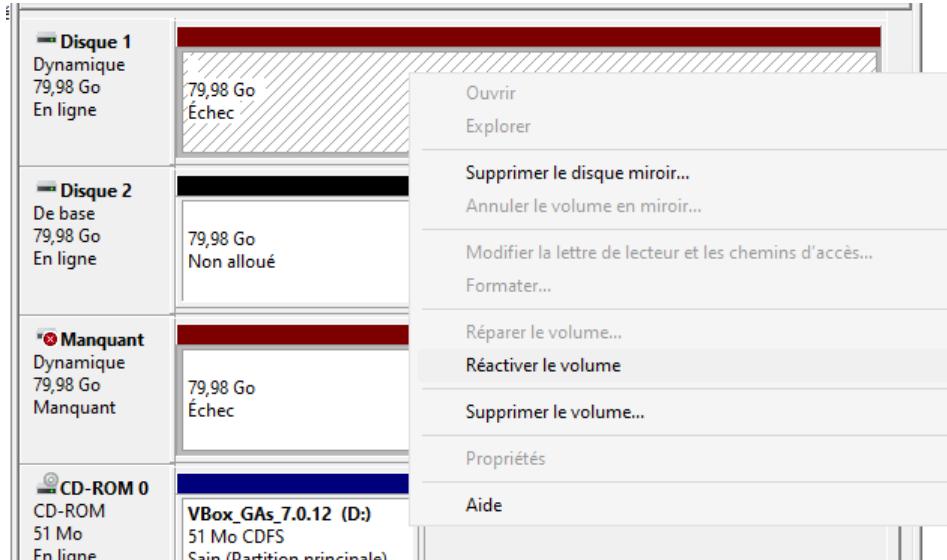


Ici nous voyons que le disque principal est en échec.

Le second est le nouveau disque et est vierge

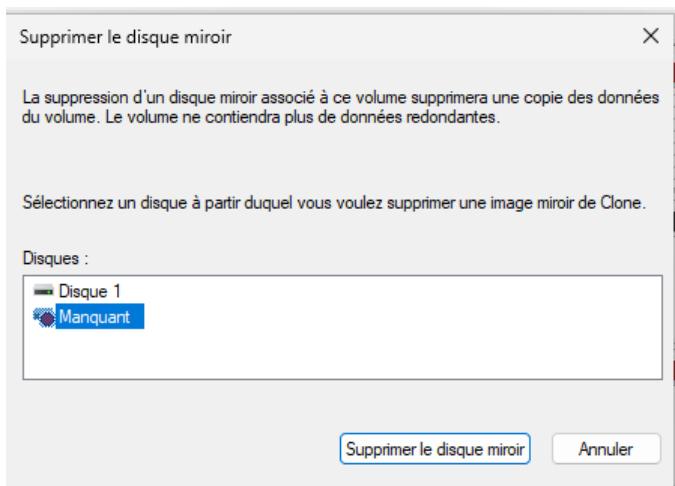
Le troisième est manquant, normal, nous l'avons retiré précédemment.

Le disque principal ne se met pas forcément en échec. Il est cependant réactivable. Click droit sur ce dernier puis Réactiver le volume.



Il se réactive et le G: sera à nouveau accessible. Cependant il nous signifie que la redondance est en échec.

Nous allons ensuite Supprimer le disque miroir manquant du RAID. Pour cela il faut aller dans le même menu qu'au dessus. Click droit sur le disque fonctionnel puis cliquer sur "Supprimer le disque miroir".



On supprime le disque manquant après l'avoir sélectionné.

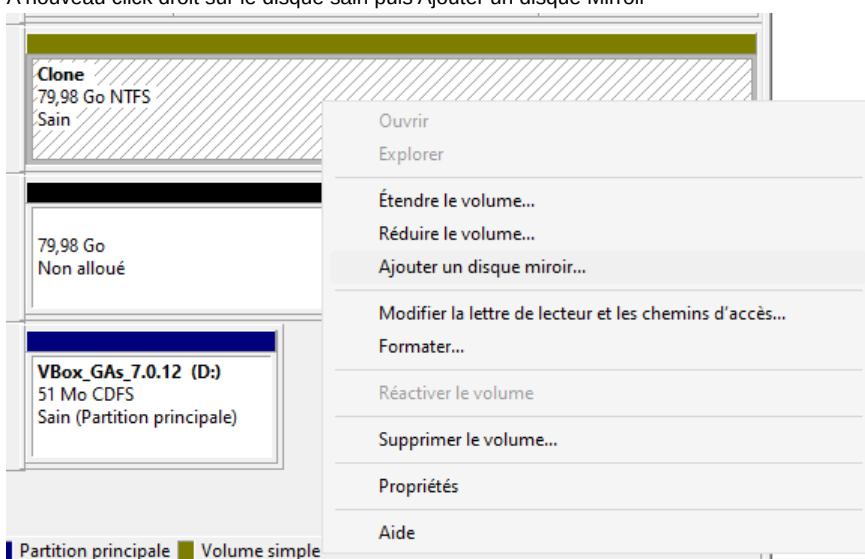
Il change d'état et le disque manquant disparait de la liste.

Disque 0 De base 79,98 Go En ligne	100 Mo Sain (Partition d)	(C) 79,07 Go NTFS Sain (Démarrer, Fichier d'échange, Image miroir)	835 Mo Sain (Partition de récupération)
Disque 1 Dynamique 79,98 Go En ligne	Clone 79,98 Go NTFS Sain		
Disque 2 De base 79,98 Go En ligne	79,98 Go Non alloué		
CD-ROM 0 CD-ROM 51 Mo En ligne	VBox_GAs_7.0.12 (D: 51 Mo CDFS Sain (Partition principale)		

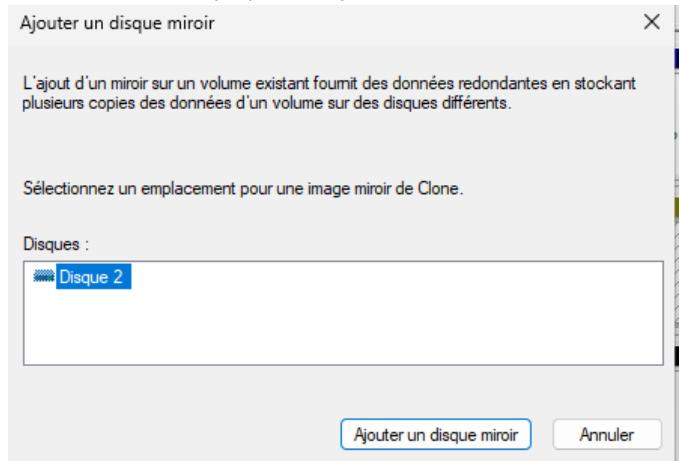
■ Non alloué ■ Partition principale ■ Volume simple

Maintenant on va ajouter le nouveau disque dans le RAID.

A nouveau click droit sur le disque sain puis Ajouter un disque Miroir



On Sélectionne le disque puis on l'ajoute.



La synchronisation se lance.

Disque 0 De base 79,98 Go En ligne	100 Mo Sain (Partition d)	(C) 79,07 Go NTFS Sain (Démarrer, Fichier d'échange, Image n°)	835 Mo Sain (Partition de récupération)
Disque 1 Dynamique 79,98 Go En ligne	Clone 79,98 Go NTFS Resynchronisation en cours		
Disque 2 Dynamique 79,98 Go En ligne	Clone 79,98 Go NTFS Resynchronisation en cours		
CD-ROM 0 CD-ROM 51 Mo En ligne	VBox_GAs_7.0.12 (D: 51 Mo CDFS Sain (Partition principale)		

Les données du disque sain sont copié sur le disque miroir jusqu'à être identique ce qui rendra le RAID à nouveau pleinement fonctionnel.
Pendant cette opération l'accès au disque G: reste opérationnel.

Disque 0 De base 79,98 Go En ligne	100 Mo Sain (Partition d)	(C) 79,07 Go NTFS Sain (Démarrer, Fichier d'échange, Image n°)	835 Mo Sain (Partition de récupération)
Disque 1 Dynamique 79,98 Go En ligne	Clone 79,98 Go NTFS Sain		
Disque 2 Dynamique 79,98 Go En ligne	Clone 79,98 Go NTFS Sain		
CD-ROM 0 CD-ROM 51 Mo En ligne	VBox_GAs_7.0.12 (D: 51 Mo CDFS Sain (Partition principale)		

■ Non alloué ■ Partition principale ■ Volume en miroir

Le RAID est redevenue Sain. Tout est revenue à la normale.

Invite de commande

- Permet d'interagir directement avec l'OS
 - Fonctionne en ligne de commande textuelle
 - Exécuter des commandes et des scripts
 - Effectuer des diagnostics
 - Administration du réseau
 - Console historique qui a peu évolué

Une liste non exhaustive de commandes DOS régulièrement utilisées

- **DIR** : Affiche la liste des fichiers et dossiers dans un répertoire.
 - **CD** : Change de répertoire.
 - **MD** ou **MKDIR** : Crée un nouveau répertoire.
 - **RD** ou **RMDIR** : Supprime un répertoire.
 - **DEL** ou **ERASE** : Supprime un fichier.
 - **COPY** : Copie des fichiers d'un emplacement à un autre.
 - **XCOPY** : Copie des fichiers et répertoires, y compris leur arborescence.
 - **MOVE** : Déplace des fichiers ou des répertoires.
 - **REN** ou **RENAME** : Renomme un fichier ou un répertoire.
 - **CLS** : Efface l'écran.
 - **ATTRIB** : Modifie les attributs d'un fichier (lecture seule, caché, etc.).
 - **FORMAT** : Formate un disque.
 - **CHKDSK** : Vérifie et répare un disque.
 - **PING** : Teste la connectivité réseau.
 - **EXIT** : Ferme l'invite de commandes.

Scripting Bash

Il est possible de créer un fichier dans lequel on écrira une liste de commandes DOS qui seront exécutées les unes à la suite des autres. Ce fichier se nomme généralement un "script". Dans ce cas précis on parle de script Batch. D'ailleurs pour être compris par Windows ce sera un fichier texte avec une extension .bat et non pas .txt.

Il est possible d'écrire des commentaires dans un fichier .bat dans le but d'en faciliter la compréhension. Pour cela il faut commencer la ligne soit par :: soit par REM . Tout ce qui suivra ces mentions sur une même ligne sera ignoré par le système qui exécutera les fichiers.

Exemple d'un script Batch

```

@echo off
:: Script batch pour automatiser quelques tâches

:: Crée un dossier de sauvegarde s'il n'existe pas
if not exist C:\Backup mkdir C:\Backup

:: Copie tous les fichiers .txt du répertoire Documents vers Backup
copy C:\Users\%USERNAME%\Documents\*.txt C:\Backup

:: Affiche un message indiquant la fin de la copie
echo Les fichiers ont été copiés dans le dossier Backup.

:: Attend 5 secondes avant de continuer
timeout /t 5

:: Supprime tous les fichiers .tmp dans le dossier Temp
del C:\Users\%USERNAME%\AppData\Local\Temp\*.tmp /q

:: Affiche un message de confirmation
echo Nettoyage des fichiers temporaires terminé.

:: Fin du script
pause

```

Il est également possible d'interagir avec le script avec des saisies clavier.

Exemple avec ce script qui récupère simplement votre nom

```

@echo off
:: Demande à l'utilisateur d'entrer son nom
set /p nom="Veuillez entrer votre nom : "

:: Affiche un message personnalisé
echo Bonjour, %nom% !

pause

```

Powershell et le terminal

- Un langage de script avancé, conçu pour l'automatisation et la configuration système, basé sur le .NET Framework.
- Une interface de ligne de commande qui permet aux utilisateurs de gérer les systèmes d'exploitation Windows, Linux, et MacOs.
- Une plateforme d'administration qui offre des fonctionnalités complètes pour gérer les réseaux, les serveurs, et les postes de travail à travers des commandes et scripts.
- Extensible, permettant aux utilisateurs d'ajouter leurs propres commandes personnalisées et fonctionnalités grâce à des modules et des scripts.
- Capable d'accéder à une vaste gamme d'interfaces de programmation d'applications (APIs), de services Windows Management Instrumentation (WMI), et de Component Object Model (COM) pour une gestion avancée des tâches.
- Doté d'un système de piping et de redirection sophistiqué, qui permet de traiter et de manipuler les données de manière puissante et flexible.
- Conçu pour interagir avec des services web et des applications basées sur le cloud, facilitant la gestion des environnements informatiques modernes.
- Un langage de script orienté objet
- Langage par défaut dans le nouveau « terminal » de Windows
- De nombreux alias existent pour lier des commandes PowerShell à des commandes linux par exemple

```
Windows PowerShell      X + - □ ×
Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindows
PS C:\Users\admin> ls

Répertoire : C:\Users\admin

Mode                LastWriteTime       Length Name
----                -----          ---- 
d-r---   1/31/2024 4:46 PM           Contacts
d-r---   1/31/2024 4:46 PM           Desktop
d-r---   1/31/2024 4:46 PM           Documents
d-r---   1/31/2024 4:46 PM           Downloads
d-r---   1/31/2024 4:46 PM           Favorites
d-r---   1/31/2024 4:46 PM           Links
d-r---   1/31/2024 4:46 PM           Music
d-r---   1/31/2024 4:48 PM           OneDrive
d-r---   1/31/2024 5:04 PM           Pictures
d-r---   1/31/2024 4:46 PM           Saved Games
d-r---   1/31/2024 4:48 PM           Searches
d-r---   2/1/2024 12:12 AM          Videos

PS C:\Users\admin> |
```

Scripting Powershell

- Possibilité de créer des scripts
- Extension de fichier type *.ps1
- Ne peut être exécuter par défaut sur un OS
- Nécessite que l'OS accepte les scripts non signé
- Possibilité de signer des scripts Powershell

Des commandes utile

- **Get-Help** : Fournit des informations détaillées sur les commandes PowerShell, y compris leur syntaxe et leurs options.
- **Get-Command** : Liste toutes les commandes disponibles dans PowerShell, y compris les fonctions, les cmdlets, et les scripts.
- **Get-Process** : Affiche les processus en cours d'exécution sur le système, permettant de surveiller et de gérer les ressources système.
- **Get-Service** : Permet de récupérer les informations sur les services Windows, y compris leur statut actuel (en cours d'exécution, arrêté, etc.).
- **Set-ExecutionPolicy** : Modifie la politique d'exécution de PowerShell pour déterminer quels scripts peuvent être exécutés sur le système.
- **Import-Module** : Charge un module PowerShell spécifique en mémoire, permettant d'accéder à des commandes supplémentaires.
- **Export-Csv / Import-Csv** : Permet d'exporter et d'importer des données au format CSV, facilitant le travail avec des données structurées.
- **Select-Object** : Sélectionne des propriétés spécifiques d'objets dans les résultats de commande, permettant de personnaliser l'affichage des données.
- **Where-Object** : Filtre les objets en fonction de critères spécifiques, utile pour isoler des éléments dans un ensemble de données.
- **Copy-Item / Remove-Item / Move-Item** : Gèrent les fichiers et les répertoires, permettant de copier, déplacer, et supprimer des éléments dans le système de fichiers.
- **New-Item** : Crée de nouveaux éléments, tels que des fichiers, des dossiers ou des clés de registre.
- **Get-Content / Set-Content** : Lit le contenu d'un fichier ou écrit du contenu dans un fichier, utile pour la manipulation de fichiers.
- **Invoke-WebRequest** : Effectue des requêtes web, permettant de télécharger des pages web ou d'interagir avec des API web.
- **Start-Process** : Lance un processus ou une application, offrant la possibilité d'exécuter des programmes externes.
- **Stop-Process** : Termine un ou plusieurs processus en cours d'exécution, permettant de gérer les applications actives.
- **Get-EventLog** : Récupère les entrées d'un journal des événements Windows, essentiel pour le diagnostic et la surveillance du système.
- **Test-Path** : Vérifie l'existence de fichiers, de dossiers ou d'autres éléments de chemin, utilisé pour les vérifications conditionnelles dans les scripts.
- **Get-ChildItem** : Enumère les fichiers et dossiers dans un chemin spécifié, équivalent à la commande "dir" dans l'invite de commande.
- **Measure-Object** : Calcule les propriétés des objets, telles que la somme ou la moyenne, utile pour analyser des ensembles de données.
- **ConvertTo-Json / ConvertFrom-Json** : Convertit des objets en chaînes JSON et vice versa, facilitant l'interaction avec des formats de données modernes et des API web.

Le piping

- Transmettre la sortie (output) d'une commande comme entrée (input) à une autre commande, créant une chaîne d'opérations.
- Utiliser le caractère pipe "|" pour connecter deux commandes ou plus, permettant l'enchaînement sans stockage temporaire.
- Faciliter le traitement et la manipulation des données en combinant plusieurs commandes en une seule instruction.
- Permettre le filtrage, le tri, ou la transformation des données de manière efficace et concise.
- Augmenter la modularité et la réutilisabilité du code en combinant des commandes simples pour effectuer des tâches complexes.
- Éviter la création de fichiers intermédiaires ou de variables temporaires pour le passage de données entre commandes.
- Être largement utilisé dans des langages de script tels que PowerShell, bash, et zsh pour une programmation plus fluide et dynamique.

Manipulation d'une commande et d'objet Powershell

Utilisons la commande get-process

```
PS C:\Users\youen> test-path .\Video\  
False  
PS C:\Users\youen> get-process
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
387	19	6424	5280	4,02	11256	1	AdobeCollabSync
285	14	4004	2532	0,48	11604	1	AdobeCollabSync
182	12	4480	10704		8784	0	AggregatorHost
148	10	2344	6284		3632	0	amdfendrsr
484	28	18848	34328	0,11	11888	1	ApplicationFrameHost
139	10	1760	6076		6188	0	armsvc
389	18	4848	15144		4120	1	aticlxx
214	11	1876	5908		3640	0	atiesrxx
265	18	7644	13544	45,50	10292	0	audiogd
307	33	17992	1612	0,05	22592	1	backgroundTaskHost
183	11	2680	12756	0,00	30312	1	backgroundTaskHost
207	14	1932	19288	0,02	21496	1	BrLogRw
255	18	5736	16980	1,75	23376	1	BrStMonW
2307	33	19884	26904		23444	0	BrYNsVC
158	10	5756	7304		5380	0	conhost
92	7	5240	3948		6824	0	conhost
158	10	5768	7272		9576	0	conhost
139	10	5876	6916	0,00	16776	1	conhost
755	30	2260	4444		1016	0	csrss
995	45	5176	5660		1140	1	csrss
590	23	30616	42104	1,28	12784	1	ctfmon
492	22	7428	17776		3408	0	dashHost
112	7	1128	4672		4808	0	dasHost
345	24	19308	41216	0,61	11248	1	Discord

- La commande `get-process` liste la totalité des processus en cours d'exécution
- Les colonnes représentent des propriétés
- Chaque ligne est un objet
- C'est donc une liste d'objets manipulable

Comprendre get-process get-help get-process

- `Get-help` permet de lire la documentation d'une commande
- Liste les différentes syntaxes
- Liste les différents alias
- Peut donner le lien de vers de la documentation externe

Rajoutons des paramètres get-process explorer

```
PS C:\Users\youen> get-process explorer
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
6683	279	397568	299060	67,75	2724	1	explorer

Piping et changement de format get-process explorer | format-list -Property *

- Le caractère « | » indique un pipe.
- La sortie de la commande `get-process` est envoyé directement en entrée de la commande `format-list`
- `format-list` est une commande qui permet de changer le formatage de sortie

- On indique à format-list d'afficher toutes les propriétés et leurs résultats grâce à -property *

```
PS C:\Users\youen> get-process explorer | format-list -Property *
```

Name	:	explorer
Id	:	2724
PriorityClass	:	Normal
FileVersion	:	10.0.22621.2428 (WinBuild.160101.0800)
HandleCount	:	7104
WorkingSet	:	310071296
PagedMemorySize	:	408768512
PrivateMemorySize	:	408768512
VirtualMemorySize	:	1511659456
TotalProcessorTime	:	00:01:09.0468750
SI	:	1
Handles	:	7104
VM	:	2204829282304
WS	:	310071296
PM	:	408768512
NPM	:	294256
Path	:	C:\Windows\Explorer.EXE
Company	:	Microsoft Corporation
CPU	:	69,046875
ProductVersion	:	10.0.22621.2428
Description	:	Explorateur Windows
Product	:	Système d'exploitation Microsoft® Windows®
__NounName	:	Process
BasePriority	:	8
ExitCode	:	
HasExited	:	False
ExitTime	:	
Handle	:	3380
SafeHandle	:	Microsoft.Win32.SafeHandles.SafeProcessHandle

Piping et Tri d'objets Get-Process | Sort-Object -Property CPU -Descending

```
PS C:\Users\youen> Get-Process | Sort-Object -Property CPU -Descending
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
1353	50	4554000	4567468	1 287,48	15608	1	VirtualBoxVM
1411	174	1011252	335148	654,08	22320	1	firefox
1103	133	213616	224476	504,53	20256	1	Discord
575	82	141868	68376	310,11	23460	1	steamwebhelper
477	37	121956	176720	270,53	23056	1	firefox
442	121	600460	607880	233,63	27440	1	firefox
1560	100	161544	101392	184,88	13824	1	Overwolf
2769	170	470356	456876	178,47	8448	1	firefox
392	105	371964	298560	125,75	12124	1	firefox
1392	133	2081632	665928	90,83	25492	1	soffice.bin
778	79	263824	262444	83,59	21680	1	KillerIntelligenceCenter
6769	281	403204	303644	71,03	2724	1	explorer
278	19	7740	13636	56,50	10292	0	audiogd
376	99	301512	233272	52,16	17740	1	firefox
542	18	8344	20760	42,28	20828	1	OverwolfHelper64
600	24	10328	22772	39,92	21464	1	OverwolfHelper
1079	54	325564	53916	35,02	7340	1	steamwebhelper
1019	97	66564	82708	28,19	12964	1	steam
365	57	270880	296528	23,91	28352	1	firefox
317	22	24928	22776	23,20	18548	1	SteelSeriesPrism
1374	115	243860	284392	15,81	25084	1	thunderbird
334	51	131896	149940	14,86	14000	1	firefox
206	14	22282	15126	12,05	22820	1	firefox

- On pipe la sortie vers sort-object qui permet de trier les résultats
- On trie en fonction de la propriété CPU et par ordre décroissant.

On rajoute un filtre pour ne voir que les 5 premiers objets Get-Process | Sort-Object -Property CPU -Descending | Select-Object -First 5 -Property ID, ProcessName

- Ajout d'un pipe vers une commande qui permet de filtrer, select-object
- first X permet d'afficher uniquement les X premiers objets de la liste

- property id, processname permet de filtrer les propriétés affichés

```
PS C:\Users\youen> Get-Process | Sort-Object -Property CPU -Descending | Select-Object -First 5 -Property ID, ProcessName
Id ProcessName
-- -----
15608 VirtualBoxVM
22320 firefox
20256 Discord
23460 steamwebhelper
23056 firefox

PS C:\Users\youen> |
```

On transforme cette commande en script

```
echo "Get-Process | Sort-Object -Property CPU -Descending | Select-Object -First 5 -Property ID, ProcessName" > test.ps1
```

- Echo permet d'afficher en sortie un texte, ici la commande précédente.
- Le cible > indique que la sortie de cette commande est envoyé vers un fichier
- test.ps1 est le nom du fichier visé
- Si le fichier existe le contenu est écrasé sinon le fichier est créé.

Le contenu du fichier

```
test.ps1
Fichier    Modifier    Affichage
Get-Process | Sort-Object -Property CPU -Descending | Select-Object -First 5 -Property ID, ProcessName
```

Tester le script .\test.ps1

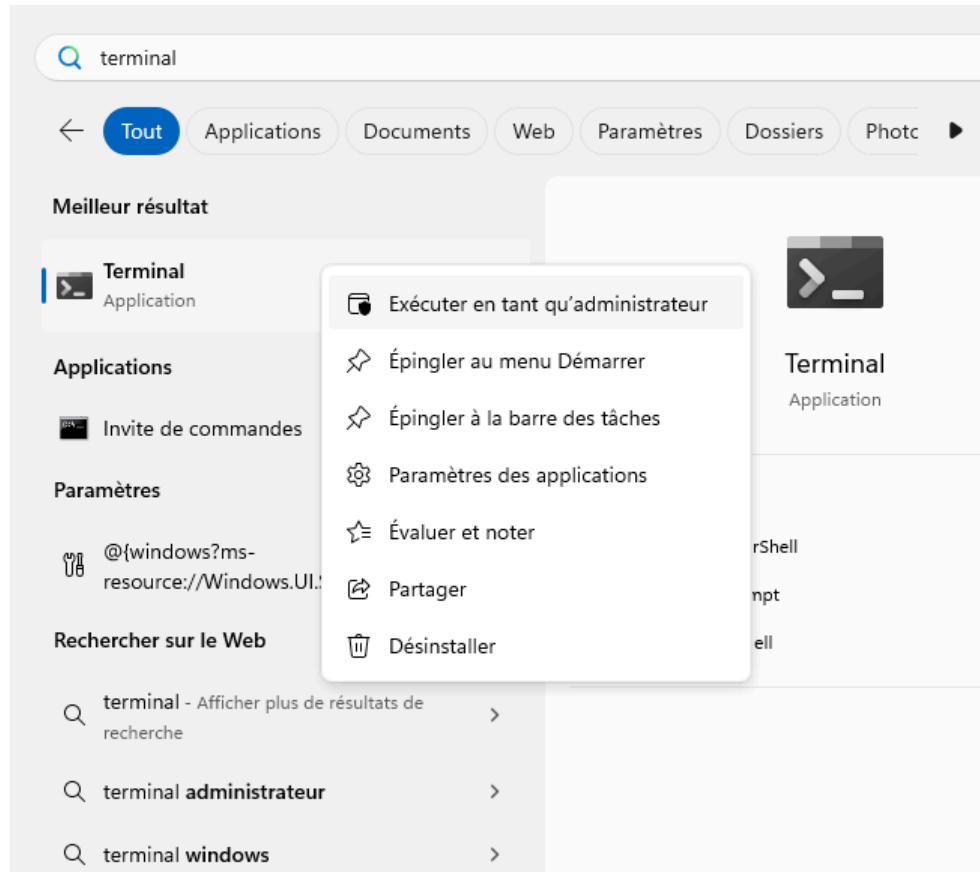
```
Windows PowerShell
PS C:\Users\youen> .\test.ps1
.\test.ps1 : Impossible de charger le fichier C:\Users\youen\test.ps1, car l'exécution de scripts est désactivée sur ce système. Pour plus d'informations, consultez about_Execution_Policies à l'adresse
https://go.microsoft.com/fwlink/?LinkId=135170.
Au caractère Ligne:1 : 1
+ .\test.ps1
+ ~~~~~
+ CategoryInfo          : Erreur de sécurité : () [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess
PS C:\Users\youen>
```

- Exécute le script
- Une erreur est levé
- L'OS refuse l'exécution de script non signé!

Autoriser l'exécution de script non signé

- Par défaut Windows refuse d'exécuter des scripts non signés
- Utiliser la commande Set-ExecutionPolicy RemoteSigned RemoteSigned
- Cette commande devra être exécuté dans un terminal ouvert avec des droits administrateurs

Ouvrir un terminal avec les droits d'administrateur



Lancer la commande Set-ExecutionPolicy RemoteSigned RemoteSigned

```
Sélection Administrateur : Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindows

PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned

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:\Windows\system32>
```

On reteste le script:

```
Windows PowerShell      X + 
PS C:\Users\youen> .\test.ps1
Id ProcessName
-- -----
15608 VirtualBoxVM
22320 firefox
20256 Discord
23056 firefox
27440 firefox

PS C:\Users\youen>
```

Exemple de Script plus complet

Ce script liste l'ensemble d'un dossier et leur taille

```
# Spécifier le chemin du dossier à analyser
$cheminDossier = "C:\Users\youen\Downloads"

# Lister tous les fichiers et dossiers dans le chemin spécifié
$elements = Get-ChildItem -Path $cheminDossier

# Afficher les noms et la taille de chaque élément
foreach ($element in $elements) {
    if ($element -is [System.IO.DirectoryInfo]) {
        # C'est un dossier
        Write-Host "$($element.Name) - Dossier"
    } else {
        # C'est un fichier
        Write-Host "$($element.Name) - Taille: $($element.Length) octets"
    }
}
```

Exercice Script Powershell

Suivez un tutoriel fournis par Microsoft:

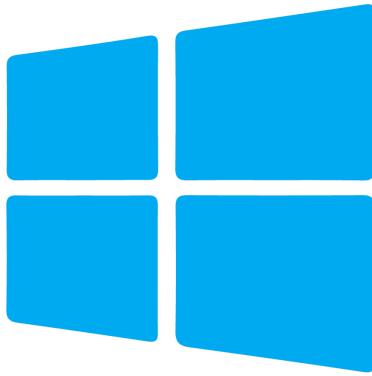
<https://learn.microsoft.com/fr-fr/training/modules/script-with-powershell/>

Windows en milieu Professionnel

Les problématique d'une entreprise

- Administrer plusieurs centaines voir millier de machines utilisateur
- Administrer des dizaines voir centaines de serveurs
- Déployer des outils et logiciels sur poste client comme serveur
- Gérer les stockages partagés
- Gérer des droits d'accès
- Etc.

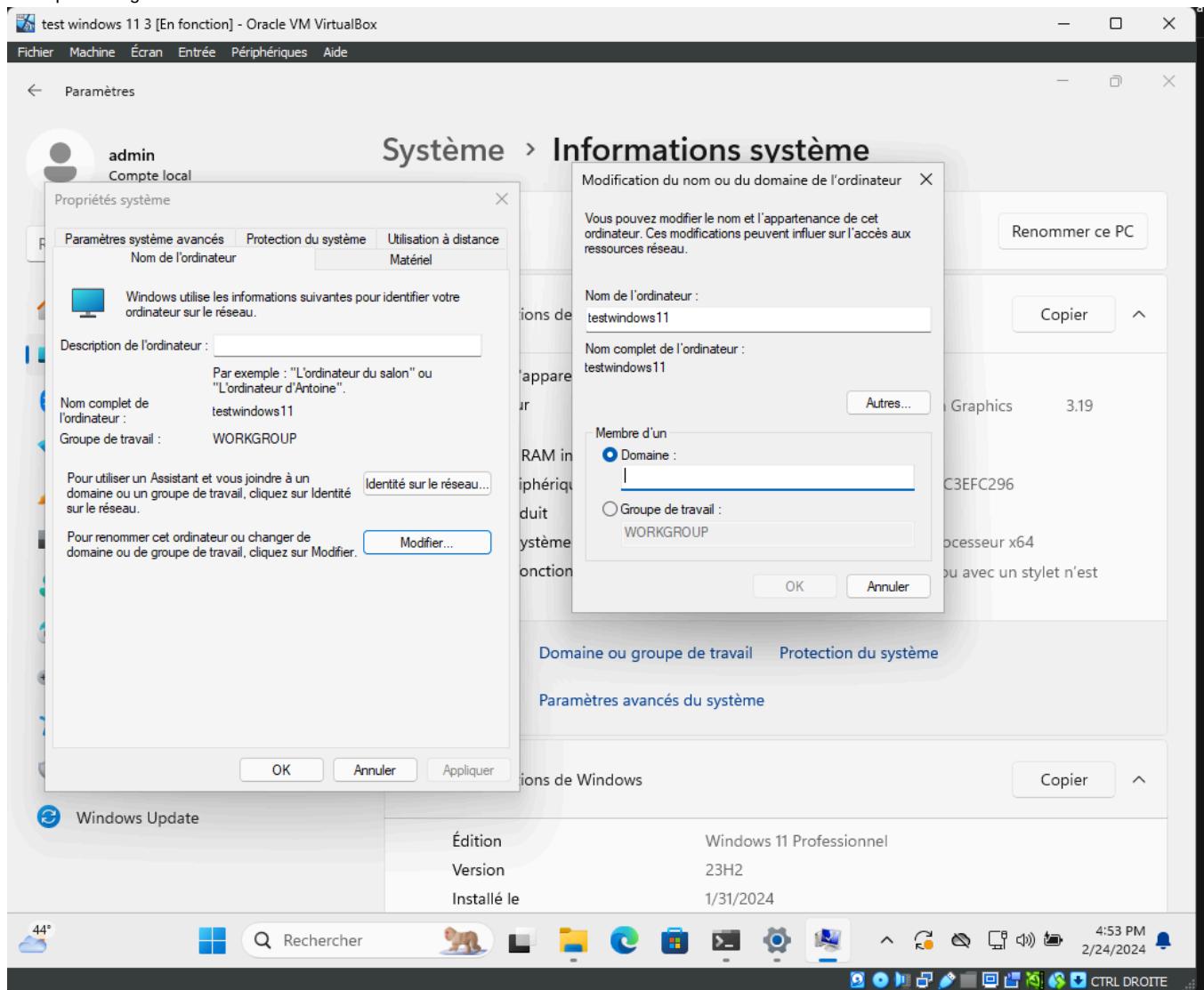
Active Directory



Microsoft Active Directory

- **Un réseau d'ordinateurs** : Il permet de connecter un ensemble d'ordinateurs sous un même réseau administratif.
- **Géré par Active Directory** : Utilise Active Directory pour centraliser l'administration et la sécurité des comptes utilisateurs et des ordinateurs.
- **Contrôle d'accès et de politiques** : Permet aux administrateurs de définir des politiques de sécurité, d'installer des logiciels, et de gérer les mises à jour sur tous les ordinateurs du domaine.
- **Authentification unique (Single Sign-On, SSO)** : Les utilisateurs peuvent accéder à plusieurs ressources sur le réseau avec un seul ensemble d'identifiants.
- **Gestion centralisée des ressources** : Facilite la gestion des ressources partagées comme les fichiers, les imprimantes, et les applications.
- **Sécurité améliorée** : Offre des outils avancés pour sécuriser le réseau, comme le chiffrement, la gestion des mots de passe, et les audits de sécurité.
- **Simplification de l'administration IT** : Réduit la complexité de la gestion des nombreux utilisateurs et ordinateurs au sein d'une organisation.
- **Hiérarchie et délégation** : Permet de créer une structure hiérarchique avec des niveaux de privilèges différents, délégant certaines tâches administratives.

Exemple d'intégration à un domaine Windows



Les avantages

- Authentification centralisée : Le poste doit s'authentifier via le domaine, permettant l'utilisation de comptes utilisateurs gérés de manière centralisée.
- Application des politiques de groupe (GPO) : Le poste reçoit et applique des politiques de sécurité et de configuration définies par les administrateurs du domaine.
- Accès aux ressources partagées : Le poste obtient l'accès à des ressources réseau partagées, comme les fichiers, les imprimantes, et les applications, selon les permissions attribuées.
- Gestion centralisée des mises à jour : Les mises à jour de logiciels et de sécurité peuvent être gérées et déployées de manière centralisée par les administrateurs du domaine.
- Contrôle d'accès basé sur les rôles : Les droits et permissions de l'utilisateur sur le poste client peuvent être ajustés selon les rôles attribués dans le domaine.
- Synchronisation de l'heure : Le poste client synchronise son horloge avec le serveur de domaine pour assurer la cohérence au sein du réseau.
- Changement des pratiques de connexion : Les utilisateurs doivent utiliser des identifiants de domaine pour se connecter, plutôt que des comptes locaux.
- Possibilité de restrictions supplémentaires : Selon les politiques du domaine, certaines fonctionnalités et applications peuvent être restreintes ou désactivées sur le poste client.
- Audit et conformité : Les activités sur le poste client peuvent être surveillées et enregistrées pour des besoins d'audit et de conformité.
- Assistance et maintenance à distance : Permet aux administrateurs de fournir une assistance à distance, de déployer des logiciels, et de résoudre des problèmes à distance.

Et beaucoup d'autres points...



quickmeme.com